The attached DRAFT document (provided here for historical purposes) has been superseded by the following publication:

Publication Number:	NIST Special Publication (SP) 800-161
Title:	Supply Chain Risk Management Practices for Federal Information Systems and Organizations

Publication Date: April 2015

- Final Publication: <u>http://dx.doi.org/10.6028/NIST.SP.800-161</u> (which links to http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf).
- Related Information on CSRC: http://csrc.nist.gov/publications/PubsSPs.html#800-161 http://csrc.nist.gov/scrm/
- Information on other NIST Computer Security Division publications and programs can be found at: http://csrc.nist.gov/



The following information was posted with the attached DRAFT document:

Jun. 3, 2014

SP 800-161

DRAFT Supply Chain Risk Management Practices for Federal Information Systems and Organizations (Second Draft)

This document provides guidance to federal departments and agencies on identifying, assessing, and mitigating Information and Communications Technology (ICT) supply chain risks at all levels in their organizations. It integrates ICT supply chain risk management (SCRM) into federal agency enterprise risk management activities by applying a multi-tiered SCRM-specific approach, including supply chain risk assessments and supply chain risk mitigation activities and guidance.

NIST requests comments on Draft NIST SP 800-161 by **July 18, 2014**. Please submit comments to scrm-nist_@nist.gov using this public comment template (MS Word – see link below) with "Comments NIST SP 800-161" in the subject line.



	(Second Draft) NIST Special Publication 800-161
_	Supply Chain Risk Management Practices for Federal Information Systems and Organizations
	Les De sere
	Jon Boyens Celia Paulsen
	Rama Moorthy
	Nadya Bartol
	http://dy.doi.org/10.6028/NIST SP.800-XXX
	http://dx.doi.org/10.0020/10151.51.000-XXX
	COMPUTER SECURITY
	NST
	National Institute of Standards and Technology
	U.S. Department of Commerce

32 33	NIST Special Publication 800-16 Second Public Draf		
34			
35	Supply Chain Risk Management		
36	Practices for Federal Information		
37	Systems and Organizations		
38			
39	Jon Boyens		
40	Celia Paulsen		
41	Computer Security Division		
4Z 42	Information Technology Laboratory		
43 44	Rama Moorthy		
45	Hatha Systems		
46	Washington DC		
47			
48	Nadva Bartol		
49	Utilities Telecom Council		
50	Washington, D.C.		
51			
52	http://dx.doi.org/10.6028/NIST.SP.800-XXX		
53			
54	June 2014		
55	NENT OF COM		
50 57	and the second sec		
58			
59			
60			
61	TO ANT		
62	TATES OF		
63	U.S. Department of Commerce		
64 65	Penny Pritzker, Secretary		
66	National Institute of Standards and Technology		
67	Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director		
68			

Authority

70 This publication has been developed by NIST in accordance with its statutory responsibilities 71 under the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541 et 72 seq., Public Law 107-347. NIST is responsible for developing information security standards and 73 guidelines, including minimum requirements for federal information systems, but such standards 74 and guidelines shall not apply to national security systems without the express approval of 75 appropriate federal officials exercising policy authority over such systems. This guideline is 76 consistent with the requirements of the Office of Management and Budget (OMB) Circular A-77 130, Section 8b(3), Securing Agency Information Systems, as analyzed in Circular A-130, 78 Appendix IV: Analysis of Key Sections. Supplemental information is provided in Circular A-130, 79 Appendix III, Security of Federal Automated Information Resources. 80 Nothing in this publication should be taken to contradict the standards and guidelines made 81 mandatory and binding on federal agencies by the Secretary of Commerce under statutory 82 authority. Nor should these guidelines be interpreted as altering or superseding the existing 83 authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. 84 This publication may be used by nongovernmental organizations on a voluntary basis and is not 85 subject to copyright in the United States. Attribution would, however, be appreciated by NIST. 86 National Institute of Standards and Technology Special Publication 800-161 87 Natl. Inst. Stand. Technol. Spec. Publ. 800-161, 298 pages (June 2014) 88 http://dx.doi.org/10.6028/NIST.SP.800-ÝÝÝ 89 CODEN: NSPUE2 90 91 Certain commercial entities, equipment, or materials may be identified in this document in order to 92 93 describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or 94 95 96 equipment are necessarily the best available for the purpose. There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including 97 concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, 98 and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST. 99 Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones 100 noted above, are available at http://csrc.nist.gov/publications. 101 102 103 104 Public comment period: June 3, 2014 through July 18, 2014 105 National Institute of Standards and Technology 106 Attn: Computer Security Division, Information Technology Laboratory 107 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930 108 Email: scrm-nist@nist.gov 109

Reports on Computer Systems Technology

110 111

112 The Information Technology Laboratory (ITL) at the National Institute of Standards and 113 Technology (NIST) promotes the U.S. economy and public welfare by providing technical

114 leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test

115 methods, reference data, proof of concept implementations, and technical analyses to advance the

- 116 development and productive use of information technology. ITL's responsibilities include the
- 117 development of management, administrative, technical, and physical standards and guidelines for
- 118 the cost-effective security and privacy of other than national security-related information in
- federal information systems. The Special Publication 800-series reports on ITL's research, and outreach afforts in information system security, and its collaboration activities
- 120 guidelines, and outreach efforts in information system security, and its collaborative activities
- 121 with industry, government, and academic organizations.

122 123

138 139

140

144 145

146

Abstract

Federal agencies are concerned about the risks associated with information and communications technology (ICT) products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the ICT supply chain. These risks are associated with the federal agencies decreased visibility into, understanding of, and control over how the technology that they acquire is developed, integrated and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services.

This publication provides guidance to federal agencies on identifying, assessing, and mitigating
 ICT supply chain risks at all levels of their organizations. This publication integrates ICT supply
 chain risk management (SCRM) into federal agency risk management activities by applying a
 multitiered, SCRM-specific approach, including guidance on supply chain risk assessment and
 mitigation activities.

Keywords

Acquire; Information and Communication Technology Supply Chain Risk Management; ICT
 SCRM; risk management; supplier; supply chain; supply chain risk; supply chain risk assessment;
 supply chain assurance; supply chain security

Acknowledgements

147 The authors, Jon Boyens, National Institute of Standards and Technology (NIST), Celia Paulsen 148 (NIST), Rama Moorthy (Hatha Systems), and Nadya Bartol (Utilities Telecom Council), would 149 like to acknowledge and thank the information and communication technology (ICT) supply 150 chain risk management (SCRM) community, which has provided the authors invaluable insight 151 and diverse perspectives to managing the ICT supply chain. We would especially like to thank 152 Kelly Dempsey (NIST), Dr. Ron Ross (NIST), and Stephanie Shankles (Booz Allen Hamilton) 153 for their contribution to the content during the document development and review. We would also 154 like to thank numerous reviewers within the information technology community who took the 155 time to provide valuable feedback and comments to the first public draft. Finally, we would like 156 to thank the participants of NIST's October 2012 ICT SCRM Workshop for providing the guiding 157 foundation to the approach this publication has taken.

158

161 Notes to Reviewers 162 163 NIST Special Publication 800-161 represents the evolution of a six-year public-private initiative 164 to develop guidance for ICT SCRM. The publication is written for use by those federal agencies 165 that acquire and use ICT products and services. The publication is consistent with the Joint Task 166 Force Transformation Initiative Unified Information Security Framework and integrates concepts 167 described in a number of NIST publications to facilitate integration with the agencies' operational 168 activities. This second public draft resulted from an extensive review and comment process to 169 implement numerous comments from the information technology community. 170 171 The following new content was added to this second public draft: 172 173 • Expanded Scope statement in Section 1 174 Extensive Background in Section 1 • 175 Explanation of how the publication builds on NIST SP 800-39, Managing Information • 176 • Security Risk, and NIST SP 800-53 Revision 4 in Section 1 177 Explanation of the overlay and enhanced overlay concepts in Section 1 and Section 3 • 178 Increased emphasis on balancing the risks and costs of ICT SCRM processes and controls • 179 throughout the publication 180 ICT SCRM controls summary table that provides an ICT SCRM baseline and maps ICT • 181 SCRM controls to NIST SP 800-53 Revision 4 High baseline controls in Appendix D 182 Increased ICT SCRM Supplemental Guidance, including the relevance of each listed • 183 control and enhancement in Section 3 184 Annotated ICT SCRM Plan Template in Appendix H • 185 186 In addition, the controls and enhancements in Section 3 were reviewed for applicability and some 187 controls/enhancements were removed or added. 188 189 We would also welcome your input to determine if the guidance and controls in this document are 190 relevant and useful for managing industrial control systems. 191 192 Your feedback to us during the public review period is invaluable as we attempt to provide useful 193 and practical ICT SCRM guidance to federal agencies. 194

195		Table of Contents					
196	INTE	RODUCTION	1				
197	1.1	PURPOSE	2				
198	1.2	SCOPE	2				
199	1.3	TARGET AUDIENCE	3				
200	1.4	BACKGROUND	3				
201		1.4.1 Federal Agencies ICT Supply Chain					
202		1.4.2 ICT Supply Chain Risk					
203		1.4.3 Federal Agency Relationships with System Integrators, Suppliers, and External Service					
204		Providers	7				
205	1.5	FOUNDATIONAL PRACTICES	9				
206	1.6	RELATIONSHIP TO OTHER PROGRAMS AND PUBLICATIONS					
207 208	1.7	METHODOLOGY FOR BUILDING ICT SCRM GUIDANCE USING SP 800-39 AND NIST SP 800-53 REVISION 4					
209		1 7 1 Integration into Risk Management Process	13				
210		17.1 Integration into hisk Management Process information in the second se	13				
211	18	ORGANIZATION OF THIS SPECIAL PUBLICATION	13				
212	INTE	GRATION OF ICT SCRM INTO ORGANIZATION-WIDE RISK MANAGEMENT	15				
213	21	MULTITIERED RISK MANAGEMENT	16				
214	2.1	2.1.1 TIER 1 – ORGANIZATION	18				
215		2 1 2 TIER 2 – MISSION/BLISINESS PROCESS	10				
216		2.1.3 TIER 3 – INFORMATION SYSTEMS	20				
217	2.2	ICT SCRM ACTIVITIES IN RISK MANAGEMENT PROCESS	21				
218		2.2.1 FRAME	23				
219		2.2.2 ASSESS	33				
220		2.2.3 RESPOND	40				
221		2.2.4 MONITOR	45				
222	ICT S	SCRM CONTROLS	48				
223	3.1	ICT SCRM CONTROLS SUMMARY	49				
224	3.2	ICT SCRM CONTROLS THROUGHOUT ORGANIZATIONAL HIERARCHY	50				
225	3.3	APPLYING ICT SCRM CONTROLS TO ACQUIRING ICT PRODUCTS AND SERVICES	50				
226		3.3.1 System Integrators	50				
227		3.3.2 Suppliers	51				
228		3.3.3 External Providers of Information System Services	51				
229	3.4	SELECTING AND TAILORING IMPLEMENTING ICT SCRM SECURITY CONTROLS	51				
230		3.4.1 ICT SCRM Control Format	52				
231		3.4.2 Using ICT SCRM Controls in This Publication	53				
232	3.3	ICT SCRM SECURITY CONTROLS	55				
233		FAMILY: ACCESS CONTROL	55				
234		FAMILY: AWARENESS AND TRAINING	60				
235		FAMILY: AUDIT AND ACCOUNTABILITY	62				
236		FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION	65				
237		FAMILY: CONFIGURATION MANAGEMENT	68				
238		FAMILY: CONTINGENCY PLANNING	75				
239		FAMILY: INCIDENT RESPONSE	79				
240		FAMILY: MAINTENANCE	81				
241		FAMILY: MEDIA PROTECTION	84				
242		FAMILY: PLANNING	87				
243		FAMILY: PROGRAM MANAGEMENT	89				

244	FAMILY: PERSONNEL SECURITY	
245	FAMILY: PROVENANCE	
246	FAMILY: RISK ASSESSMENT	
247	FAMILY: SYSTEM AND COMMUNICATION PROTECTION	108
248	FAMILY: SYSTEM AND INFORMATION INTEGRITY	
249	GLOSSABY	
250		1
250		ـــــــــــــــــــــــــــــــــــــ
251		I
252		1
253	NIST SP 800-53 ICT SCRM-RELEVANT CONTROLS	1
254	FAMILY: ACCESS CONTROL	1
255	FAMILY: AWARENESS AND TRAINING	13
256	FAMILY: AUDIT AND ACCOUNTABILITY	15
257	FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION	21
258	FAMILY: CONFIGURATION MANAGEMENT	28
259	FAMILY: CONTINGENCY PLANNING	40
260	FAMILY: IDENTIFICATION AND AUTHENTICATION	45
261	FAMILY: INCIDENT RESPONSE	50
262	FAMILY: MAINTENANCE	53
263	FAMILY: MEDIA PROTECTION	58
264	FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION	61
265	FAMILY: PERSONNEL SECURITY	66
266	FAMILY: RISK ASSESSMENT	68
267	FAMILY: SYSTEM AND SERVICES ACQUISITION	71
268	FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION	
269	FAMILY: PLANNING	106
270	FAMILY: PROGRAM MANAGEMENT	110
271	ICT SUPPLY CHAIN THREAT EVENTS	1
272	SUPPLY CHAIN THREAT SCENARIOS AND ANALYSIS FRAMEWORK	1
273	DEVELOPING AND ANALYZING THREAT SCENARIOS & IDENTIFYING APPLICABLE CONTROLS	2
274	SAMPLE SCENARIOS	4
275	SCENARIO 1: Telco Counterfeits	5
276	SCENARIO 2: Industrial Espionage	9
277	SCENARIO 3: Malicious Code Insertion	13
278	SCENARIO 4: Unintentional Compromise	16
279	ICT SCRM PLAN TEMPLATE	1
280	1 INTRODUCTION	4
281	1.1 Purpose and Scope	
282	1.2 Authority	
283	1.3 Audience	
284	2 ROLES AND RESPONSIBILITIES	
285	2.1 Responsibility for the Plan	
286	2.2 Key Contributors	5
287	3 ICT SCRM CONTROLS	
288	4 USING AND REVISING ICT SCRM PLAN	
289	4.1 Communicating ICT SCRM Plan	

290	4.2 Revision and Improvement	6
291	4.3 Implementing and Assessing Effectiveness of ICT SCRM Plans	6
292	4.4 Use of ICT SCRM Plan during Contingencies and Emergencies	9
293	ATTACHMENTS	9
294		

List of Tables and Figures

298		
299	Figure 1-1: Four Aspects of ICT SCRM	4
300	Figure 1-2: Federal Agency Relationships with System Integrators, Suppliers, and External Service	
301	Providers with Respect to the Scope of NIST SP 800-161, Supply Chain Risk Management	
302	Practices for Federal Information Systems and Organizations	5
303	Figure 1-3: ICT Supply Chain Risk	7
304	Figure 1-4: Federal Agency Visibility, Understanding and Control of its ICT Supply Chains	8
305	Figure 1-5: ICT SCRM Security Controls in NIST SP 800-161, Supply Chain Risk Management Practices	or
306	Federal Information Systems and Organizations, Section 3.5	13
307	Figure 2-1: Risk Management Process	15
308	Figure 2-2: Multitiered Organization-wide Risk Management	17
309	Table 2-1: Supply Chain Risk Management Stakeholders	18
310	Figure 2-3: ICT SCRM Risk Assessment	21
311	Figure 2-4: ICT SCRM Activities in Risk Management Process	22
312	Figure 2-5: ICT SCRM in the Frame Step	24
313	Table 2-2: Example ICT Supply Chain Threat Agents	26
314	Table 2-3: Supply Chain Threat Considerations	27
315	Table 2-4: Supply Chain Vulnerabilities Considerations	28
316	Table 2-5: Supply Chain Constraints	30
317	Figure 2-6: ICT SCRM in the Assess Step	33
318	Table 2-6: Examples of ICT Supply Chain Vulnerabilities Mapped to the Organizational Tiers	37
319	Figure 2-7: ICT SCRM in the Respond Step	41
320	Table 2-7: ICT SCRM Plan Controls at Tiers 1, 2, and 3	43
321	Figure 2-8: ICT SCRM in the Assess Step	46
322	Figure 3-1: ICT SCRM Security Controls in NIST SP 800-161, Supply Chain Risk Management Practices f	or
323	Federal Information Systems and Organizations, Section 3.5	48
324	Table 3-2: ICT SCRM Control Format	52
325	Table D-1: ICT SCRM Control Summary	.D-1
326	Table F-1: Adversarial ICT Supply Chain Threat Events	. F-1
327	Table F-2: Non-Adversarial ICT Supply Chain Threat Events	. F-7
328	Figure G-1: Sample Threat Scenario Analysis Framework	.G-4
329	Figure H-1: ISO/IEC 15288 Life Cycle Processes	.H-1
330	Figure H-2: ICT SCRM Plan and Life Cycles	.H-2
331	Figure H-3: Agency Implementation of ICT SCRM Plan	.H-7
332	Figure H-4: Agency Implementation of ICT SCRM Plan with Life Cycles	.H-8
222		

333

334 CHAPTER ONE

335 INTRODUCTION

336

THE information and communications technology (ICT) supply chain is a complex, globally 367 338 distributed, and interconnected ecosystem that is long, has geographically diverse routes, 339 and consists of multiple tiers of outsourcing. This ecosystem includes public and private 340 sector entities that depend upon each other to develop, integrate, and use ICT products and 341 services. The ecosystem has evolved to provide a set of highly refined, cost-effective, reusable 342 ICT solutions, either commercially licensable, open source, or delivered as services. Federal 343 government information systems have rapidly adopted this ecosystem of solution options, which 344 increased their reliance on commercially available (commercial off-the-shelf [COTS] or open 345 source) products, system integrator support for custom-built systems, and external service 346 providers. This resulted in increased complexity, diversity, and scale of the federal government's 347 ICT supply chains.

348

349 COTS products are developed by a globalized ecosystem of vendors for a global base of public 350 and private sector customers. This globalized ecosystem of vendors affords significant benefits to 351 its customers, including low cost, interoperability, rapid innovation, a variety of product features, 352 and choice among competing vendors. However, the same globalization that creates these 353 benefits enables increased opportunities for adversaries (individuals, organizations, or nation-354 states) to directly or indirectly affect the management or operations of companies, in a manner 355 that may result in risks to the end user. For example, an adversary may have the power to coerce a 356 manufacturer to hand over the manufacturing specifications of a sensitive U.S. system or to insert 357 malicious capability into a product. Similarly, the rapid adoption of open source software, most 358 commonly in binary form, extends these risk scenarios to the libraries, frameworks, and toolkits 359 on which so much of modern software relies. Threats and vulnerabilities created in this way are 360 often extremely sophisticated and difficult to detect and thus provide a significant risk to federal 361 agencies. It should be noted that, ICT products or services manufactured anywhere (domestically 362 or abroad) may contain vulnerabilities that can present opportunities for ICT supply chain-related 363 compromises,¹ including most of the same sophisticated threats that are posed by foreign entities. 364

365 Federal agencies are concerned about ICT supply chain risks when acquiring ICT products and

366 services. These ICT supply chain risks may include insertion of counterfeits, unauthorized

367 production, tampering, theft, insertion of malicious software, as well as poor manufacturing and

development practices in the ICT supply chain. These risks are associated with the federal

369 agency's decreased visibility into, and understanding of, how the technology that they acquire is

¹ This document defines an ICT Supply Chain Compromise as:

An occurrence within the ICT supply chain whereby an adversary jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits. An ICT supply chain compromise can occur anywhere within the system development life cycle of the product or service.

developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services.²

372

Currently, federal agencies, and many private sector integrators and suppliers use varied and
nonstandard practices, which makes it difficult to consistently measure and manage ICT supply
chain risks across different organizations. ICT Supply Chain Risk Management (SCRM) is the
process of identifying, assessing, and mitigating the risks associated with the global and
distributed nature of ICT product and service supply chains.

379 **1.1 PURPOSE**

380

381 Due to the growing sophistication and complexity of ICT and the globalization of ICT supply 382 chains, federal agency information systems are increasingly at risk of compromise, and agencies 383 need guidance to help manage ICT supply chain risks. The purpose of this publication is to 384 provide guidance to federal agencies on identifying, assessing, selecting, and implementing risk 385 management processes and mitigating controls throughout their organizations to help manage 386 ICT supply chain risks.

387

As a result of implementing the guidance in this publication, organizations will be able to establish appropriate policies, processes, and controls to manage ICT supply chain risks. This publication empowers organizations to develop ICT SCRM solutions that are tailored to their particular mission/business needs, threats, and operational environments. This publication does not provide contract language or a complete list of ICT SCRM methods and techniques that mitigate specific supply chain threats.

394 395

1.2 SCOPE

397

This publication provides guidance to federal agencies on managing risks to and through their ICT supply chains. The processes and controls described in this publication build on federal agency guidance and are for the federal agencies to consider and implement. While entities outside of the federal government may decide to consult this publication as a source of good practices, this publication does not contain any specific guidance for those entities.

403

404 The guidance and controls in this publication are recommended for use with high-impact systems

405 according to Federal Information Processing Standard (FIPS) 199, *Standards for Security*

406 Categorization of Federal Information and Information Systems. However, because of

² This document adapts the definition of risk from Federal Information Processing Standard (FIPS) 200 to establish a definition for ICT supply chain risk as follows:

Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

- 407 interdependencies and individual needs, agencies may choose to apply the guidance to systems at
- 408 a lower impact level or to specific system components.
- 409
- 410 In applying the processes and controls, organizations may decide to include requirements that
- 411 they include in their policies, acquisition guidelines, and procurement documents.
- 412

In this document the word *organization* refers to the *federal agency*. In the context of this document, the *acquirer* is the federal agency.

Federal agencies are a diverse set of organizations with different missions, structures, and sizes. The guidance in this publication applies across the federal sector, and therefore this publication does not differentiate between the terms federal agency and uses those terms interchangeably.

416

417 **1.3 TARGET AUDIENCE**

418

419 ICT SCRM is an organization-wide activity that should be directed under the overall agency 420 governance, regardless of the specific organizational structure. At the organization level, ICT 421 SCRM activities should be led by the risk executive function, described in NIST SP 800-39, and 422 implemented throughout the organization by a variety of individuals in different roles. The 423 audience for this publication is federal agency personnel involved in engineering/developing, 424 testing, deploying, acquiring, maintaining, and retiring ICT components and systems. These 425 functions may include, but are not limited to, information technology, information security, 426 contracting, risk executive, program management, legal, supply chain and logistics, acquisition 427 and procurement, other related functions, and end users. Other personnel or entities are free to 428 make use of the guidance as appropriate to their situation. 429

430 **1.4 BACKGROUND**

431

ICT SCRM encompasses activities in the system development life cycle, including research and
development (R&D), design, manufacturing, acquisition, delivery, integration, operations, and
disposal/retirement of an organization's ICT products (i.e., hardware and software) and services.
ICT SCRM lies at the intersection of security, integrity, resilience, and quality, as depicted in
Figure 1-1.

- 437
 Security provides the confidentiality, integrity, and availability of information that (a) describes the ICT supply chain (e.g., information about the paths of ICT products and services, both logical and physical); or (b) traverses the ICT supply chain (e.g., intellectual property contained in ICT products and services), as well as information about the parties participating in the ICT supply chain (anyone who touches an ICT product or service throughout its life cycle);
- Integrity is focused on ensuring that the ICT products or services in the ICT supply chain are genuine and authentic and do not contain any unwanted (and potentially dangerous) functionality, as well as that the ICT products and services will perform according to expectations;
- Resiliency is focused on ensuring that ICT supply chain will provide required ICT
 products and services under stress; and
- 449
 Quality is focused on reducing unintentional vulnerabilities that may provide opportunities for exploitation.
- 451

- 452 This publication addresses the overlap between security, integrity, resilience, and quality depicted
- 453 in Figure 1-1 by the overlapping circles. The publication does not address the entire body of
- 454 knowledge of these disciplines that is depicted by the non-overlapping areas of the circles in
- 455 Figure 1-1.
- 456
- 457



461462 1.4.1 Federal Agencies ICT Supply Chain

463

Federal agencies run complex information systems and networks to support their missions. These
information systems and networks are composed of ICT products and components made available
by ICT *suppliers*. Federal agencies also acquire and deploy an array of IT services,³ including
those that:

 Integrate or provide operations, maintenance, and disposal support for federal information systems and networks within and outside of the federal agency authorization boundaries, made available by *system integrators;* and

³ NIST SP 800-53 Rev. 4 defines Authorization Boundary as "All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected."

- 472 Provide external services to support federal agency operations that are provided from • 473 both within or outside of the federal agency authorization boundaries, made available by 474 external service providers.
- 475

476 In addition to operating information systems and networks internally, federal agencies also host 477 system development and integration activities within their authorization boundaries. Those

478 activities may be performed by the agency themselves or by system integrators. The ICT Supply

479 Chain Infrastructure is the integrated set of components (hardware, software and processes)

480 within the federal agency's organizational boundary that composes the environment in which a

- 481 system is developed or manufactured, tested, deployed, maintained, and retired/decommissioned.
- 482 Figure 1-2 depicts a federal agency ICT supply chain that consists of multiple layers of system
- 483 integrators, external service providers, and suppliers with respect to the scope of this publication 484 and the drivers that influence activities described herein.
- 485



486 487

488

489

Figure 1-2: Federal Agency Relationships with System Integrators, Suppliers, and External Service Providers with Respect to the Scope of NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations.

Supplier and system integrator are included under the definition of "developer" by NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations:

A general term that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; and (iv) product resellers. Development of systems, components, or services can occur internally within organizations (i.e., in-house development) or through external entities.

NIST SP 800-161 uses NIST SP 800-53 Revision 4 *developer* definition items (i), (iii), and (iv) to define *supplier* and item (ii) to define *system integrator*.

NIST SP 800-53 Revision 4 describes external service provider as follows:

External services can be provided by: (i) entities within the organization but outside of the security authorization boundaries established for organizational information systems; (ii) entities outside of the organization either in the public sector (e.g., federal agencies) or private sector (e.g., commercial service providers); or (iii) some combination of the public and private sector options. External information system services include, for example, the use of service-oriented architectures (SOAs), cloud-based services (infrastructure, platform, software), or data center operations. External information system services may be used by, but are typically not part of, organizational information systems. In some situations, external information system services may completely replace or heavily augment the routine functionality of internal organizational information systems.

Additionally, NIST SP 800-53 Revision 4 describes organizational users as follows:

An organizational employee or an individual the organization deems to have equivalent status of an employee including, for example, contractor, guest researcher, or individual detailed from another organization.

490

491

492 **1.4.2** ICT Supply Chain Risk

493 ICT supply chain risks include insertion of counterfeits, unauthorized production, tampering,
494 theft, insertion of malicious software, as well as poor manufacturing and development practices in
495 the ICT supply chain. These risks are realized when threats in the ICT supply chain exploit
496 existing vulnerabilities.

497

498 Figure 1-3 depicts ICT supply chain risk resulting from the likelihood and impact of the

499 applicable threats exploiting applicable vulnerabilities.

ICT Supply Chain Risk

Threats

Vulnerabilities

Adversarial: e.g., insertion of counterfeits, tampering, theft, and insertion of malicious software.

Non-adversarial: e.g., natural disaster, poor quality products/services and poor practices (engineering, manufacturing, acquisition, management, etc). External: e.g., weaknesses to the supply chain, weaknesses within entities in the supply chain, dependencies (power, comms, etc.)

Internal: e.g., information systems and components, organizational policy/processes (governance, procedures, etc.)

Likelihood (probability of a threat exploiting a vulnerability(s))

Adversarial: capability and intent

Non-adversarial: occurrence based on statistics/history

Impact - degree of harm

To: mission/business function From: data loss, modification or exfiltration

From: unanticipated failures or loss of system availability

From: reduced availability of components

- 500
- 501
- 502
- 503

Figure 1-3: ICT Supply Chain Risk

It should be noted that it might take years for a vulnerability stemming from the ICT supply chain to be exploited or discovered. In addition, it may be difficult to determine whether an event was the direct result of a supply chain vulnerability. This may result in a persistent negative impact on federal agencies' missions that could range from reduction in service levels leading to customer dissatisfaction to theft of intellectual property, or degradation of mission-critical federal agency functions.

510

5111.4.3Federal Agency Relationships with System Integrators, Suppliers, and512External Service Providers

513 ICT supply chain risks are associated with the federal agency's decreased visibility into, and 514 understanding of, how the technology that they acquire is developed, integrated and deployed, as 515 well as the processes, procedures, and practices used to assure the integrity, security, resilience, 516 and quality of the products and services. Federal agencies have a variety of relationships with 517 their system integrators, suppliers, and external service providers. Figure 1-4 depicts how the 518 diverse types of these relationships affect the federal agency's visibility and control of the supply 519 chain.



Reduced Visibility, Understanding and Control

Figure 1-4: Federal Agency Visibility, Understanding and Control of its ICT Supply Chains

523 524

521 522

525

526 Some supply chain relationships are tightly integrated, such as when a system integrator develops 527 a complex information system to be operated within the federal agency's authorization boundary 528 or when an external service provider manages federal agency information systems and resources 529 on behalf of the department. These relationships are usually guided by an agreement (e.g., 530 contract) that establishes detailed functional and security requirements and may provide for 531 custom development or significant customization of ICT products and services. For these 532 relationships, system integrators and external service providers are likely to be able to work with 533 the federal agency to implement those processes and controls listed in NIST SP 800-161, Supply 534 Chain Risk Management Practices for Federal Information Systems and Organizations, that are 535 deemed appropriate based on the results of a risk assessment and cost/benefit analysis. This may 536 include floating requirements upstream in the supply chain that can significantly impact costs to 537 the supplier. The cost of requiring system integrators and external service providers to implement 538 ICT SCRM processes and controls should be weighed against the benefits of improved ICT 539 supply chain security afforded by adhering to those additional requirements. Often, working 540 directly with the system integrators and external service providers to identify appropriate 541 mitigation processes and controls will help create a more cost-effective strategy. 542

543 Procuring ICT products directly from ICT suppliers establishes a direct relationship between 544 those suppliers and the federal agencies. This relationship is also usually guided by an agreement

545 between the acquirer and ICT supplier. However, ICT products created by suppliers are created

546 for general purposes for a global market and typically are not tailored to any individual

547 customer's specific requirements. It is suggested that acquirers establish a dialog with the ICT

548 suppliers regarding the possibility of implementing ICT SCRM processes and controls in this

- 549 publication. However, acquirers should recognize that ICT suppliers might not be able to offer
- significant tailoring or choose not to modify their processes or product to support federal agency
- security and ICT SCRM requirements. Acquirers may want to establish a dialog with the ICT
- suppliers regarding the possibility of implementing ICT SCRM processes and controls in this
- 553 publication. As with system integrators and external service providers, ICT products that support
- 554 ICT SCRM may be more costly than products that do not. Acquirers should weigh those costs
- against the benefits afforded by these products to make their final acquisition decision.
- 556

Requiring a greater level of testing, documentation, or security features from system integrators, suppliers, and external service providers may increase the price of a product or service. Additional costs may include the development or testing of products, or the collection, analysis, storage and protection of data. This is especially true for those products and services developed for general-purpose application and not tailored to the specific federal agency security or ICT SCRM requirements. Acquirers should evaluate the costs and benefits of adding ICT SCRM requirements into agreements.

557 558

559 **1.5 FOUNDATIONAL PRACTICES**

560

561 ICT supply chain risk management builds on existing standardized practices in multiple 562 disciplines. Federal agencies should consider reaching a base level of maturity in foundational 563 practices prior to specifically focusing on ICT SCRM practices that are more advanced. Those 564 foundational practices are described in NIST standards and guidelines as well as other applicable 565 national and international standards and best practices. They include: ensuring that organizations 566 understand the cost and scheduling constraints of implementing ICT SCRM; integrating 567 information security requirements into the acquisition process; using applicable baseline security 568 controls as one of the sources for security requirements; ensuring a robust software quality 569 control process; and establishing multiple delivery routes for critical system elements. A formal 570 program and process, including dedicated resources, may be used to reaching a base level of 571 maturity. FIPS 199 "high-impact" systems should already have these foundational practices 572 established. 573

Having foundational practices in place is critical to successfully and productively interacting with
mature system integrators and suppliers who may have such practices standardized and in place.
The following are specific examples of the multidisciplinary foundational practices that can be
implemented incrementally to improve an organization's ability to develop and implement more
advanced ICT SCRM practices:

- Implement a risk management hierarchy and risk management process (in accordance with NIST SP 800-39) including an organization-wide risk assessment process (in accordance with NIST SP 800-30);
 Establish an organization governance structure that integrates ICT SCRM requirement
 - Establish an organization governance structure that integrates ICT SCRM requirements and incorporates these requirements into the organizational policies;
 - Establish consistent, well-documented, repeatable processes for determining FIPS 199 impact levels;
 - Use risk assessment processes after the FIPS 199 impact level has been defined, including criticality analysis, threat analysis, and vulnerability analysis;
- 589 Implement a quality and reliability program that includes quality assurance and quality control process and practices;
- Establish a set of roles and responsibilities for ICT SCRM that ensures that the broad set of right individuals are involved in decision making, including who has the required

584

585

586

587

593		authority to take action, who has accountability for an action or result, and who should be			
594		consulted and/or informed (e.g., Legal, Risk Executive, HR, Finance, Enterprise IT,			
595		Program Management/System Engineering, Information Security,			
596		Acquisition/procurement, supply chain logistics, etc.);			
597	•	Ensure adequate resources are allocated to information security and ICT SCRM to ensure			
598		proper implementation of guidance and controls;			
599	•	• Implement consistent, well-documented, repeatable processes for system engineering,			
600		ICT security practices, and acquisition;			
601	•	Implement an appropriate and tailored set of baseline information security controls in			
602		NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information			
603		Systems and Organizations;			
604	•	Establish internal checks and balances to assure compliance with security and quality			
605		requirements;			
606	•	Establish supplier management program including, for example, guidelines for			
607		purchasing directly from qualified original equipment manufacturers (OEMs) or their			
608		authorized distributors and resellers;			
609	•	Implement a tested and repeatable contingency plan that integrates ICT supply chain risk			
610		considerations to ensure the integrity and reliability of the supply chain including during			
611		adverse events (e.g., natural disasters such as hurricanes or economic disruptions such as			
612		labor strikes); and			
613	•	Implement a robust incident management program to successfully identify, respond to,			
614		and mitigate security incidents. This program should be capable of identifying causes of			
615		security incidents, including those originating from the ICT supply chain.			
616					
617	The gu	idance and controls contained in this publication are built on existing practices from			
618	multip	le disciplines and are intended to increase the ability of federal agencies to strategically			
619	manag	e ICT supply chain risks over the entire life cycle of systems, products, and services.			
620					

622 623

1.6 RELATIONSHIP TO OTHER PROGRAMS AND PUBLICATIONS

This publication builds on the Joint Task Force Transformation Initiative Unified Information
 Security Framework⁴ and uses concepts described in a number of NIST publications to facilitate
 integration with the agencies' existing organization-wide activities. These publications are
 complementary and work together to help organizations build risk-based information security

⁴ The Unified Information Security Framework is a comprehensive, flexible, risk-based information security framework developed by the Joint Task Force, a partnership among the National Institute of Standards and Technology, the Department of Defense, the U.S. Intelligence Community, and the Committee on National Security Systems. The Unified Information Security Framework consists of five core publications including: NIST Special Publication 800-39 (Managing Information Security Risk: Organization, Mission, and Information System View); NIST Special Publication 800-30 (Guide for Conducting Risk Assessments); NIST Special Publication 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations); NIST Special Publication 800-53A (Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans); and NIST Special Publication 800-37 (Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach).

628 programs to help protect their operations and assets against a range of diverse and increasingly 629 sophisticated threats. This publication will be revised to remain consistent with the NIST SP 800-

630 53 security controls catalog, using an iterative process as the ICT SCRM discipline matures.

631

633

639

640

641

632 NIST SP 800-161 builds on the fundamental concepts described in:

- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and
 Information System View, to integrate ICT SCRM into the risk management tiers and risk
 management process;
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments* (NIST SP 800-30
 Revision 1), to integrate ICT SCRM into the risk assessment process;
 - NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, to conduct criticality analysis to scoping ICT SCRM activities to high-impact components or systems;
- NIST 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, to provide information security controls for enhancing and tailoring to ICT SCRM context; and
- NIST SP 800-53A Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, to
 enable the assessment techniques to be applicable to ICT SCRM controls in this
 publication.
- 649

NIST SP 800-161 refines the multitiered risk management approach of NIST SP 800-39,

651 *Managing Information Security Risk: Organization, Mission, and Information System View*, by 652 providing ICT SCRM guidance at Organization, Mission, and Information System Tiers. It also

653 contains an enhanced overlay⁵ of specific ICT SCRM controls, building on NIST SP 800-53

654 Revision 4. Finally, NIST SP 800-161 describes the development and implementation of an ICT

- 655 SCRM plan to be developed at all levels of an organization. An ICT SCRM plan is an output of
- 656 ICT supply chain risk assessment and should contain ICT SCRM controls tailored to specific 657 agency mission/business needs, operational environments, and/or implementing technologies.
- 658

For specific guidance on system security engineering, the readers of NIST SP 800-161 should
consult NIST SP 800-160, *Systems Security Engineering*. Both publications build on NIST SP
800-53 Revision 4. They complement each other: NIST SP 800-161 addresses the security

- 662 engineering aspects of ICT SCRM while NIST SP 800-160 addresses system security engineering
- 663 more broadly throughout System Development Life Cycle (SDLC) processes.
- 664

⁵ An overlay is "a set of security controls, control enhancements, supplemental guidance, and other supporting information, that is intended to complement (and further refine) security control baselines to provide greater ability to appropriately tailor security requirements for specific technologies or product groups, circumstances and conditions, and/or operational environments. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems." – NIST SP 800-53 Rev 4 (adapted). An enhanced overlay is an overlay which adds controls or enhancements to security control baselines in order to highlight or address needs specific to the purpose of the overlay.

665 NIST SP 800-161 draws from a collaborative ICT SCRM community workshop hosted in 666 October 2012 and NISTIR 7622, Notional Supply Chain Risk Management Practices for Federal 667 Information Systems, which resulted from several years of rigorous study of the ICT SCRM discipline and provided NIST the insight required to scope and develop this special publication. 668 669 NISTIR 7622 can be used by the reader for background materials in support of applying the 670 special publication to their specific acquisition processes. 671 672 673 NIST SP 800-161 also draws from several external publications, including: 674 National Defense University, Software Assurance in Acquisition: Mitigating Risks to the 675 Enterprise: 676 • National Defense Industrial Association (NDIA), Engineering for System Assurance; 677 International Organization for Standardization/International Electrotechnical Commission 678 (ISO/IEC) 15288 - System Life Cycle Processes; 679 • Draft ISO/IEC 27036 – Information Technology – Security Techniques – Information 680 Security for Supplier Relationships; 681 Open Trusted Technology Provider Standard (O-TTPS)TM, Version 1.0, Mitigating 682 Maliciously Tainted and Counterfeit Products; and 683 • Software Assurance Forum for Excellence in Code (SAFECode) Software Integrity 684 Framework and Software Integrity Best Practices. 685 686 This publication does not replace guidance provided with respect to federal agency assessment of 687 cloud service providers' security. The external service providers discussed in this publication 688 include cloud service providers. When applying this publication to cloud service providers, 689 federal agencies should first use Federal Risk and Authorization Program (FedRAMP) cloud 690 services security guidelines and then apply NIST SP 800-161 for those processes and controls 691 that are not addressed by FEDRAMP. 692 693 694 1.7 METHODOLOGY FOR BUILDING ICT SCRM GUIDANCE USING SP 800-695 **39 AND NIST SP 800-53 REVISION 4** 696 697 This publication applies the multitiered risk management approach of NIST SP 800-39, 698 Managing Information Security Risk: Organization, Mission, and Information System View, by 699 providing ICT SCRM guidance at Organization, Mission, and System Tiers. It also contains an 700 enhanced overlay of specific ICT SCRM controls, building on NIST SP 800-53 Revision 4. 701 702 The guidance/controls contained in this publication are built on existing practices from multiple 703 disciplines and are intended to increase the ability of federal agencies to strategically manage the

- associated ICT supply chain risks over the entire life cycle of systems, products, and services. It should be noted that this publication gives federal agencies the flexibility to either develop stand-
- alone documentation (e.g. policies, assessment and authorization (A&A) plan and ICT SCRM
- 707 plan) for ICT SCRM or to integrate it into existing agency documentation.
- 708
- 709 The processes and controls in this publication should be integrated into agencies' existing system
- 710 development life cycles (SDLCs) and organizational environments at all levels of the risk
- 711 management hierarchy (organization, mission, system). For individual systems, this guidance is
- 712 recommended for use for those information systems that are categorized as high-impact systems
- according to the Federal Information Processing Standard (FIPS) 199, *Standards for Security*
- 714 Categorization of Federal Information and Information Systems. The agencies may choose to

apply this guidance to systems at a lower impact level or to specific system components. Finally,

716 NIST SP 800-161 describes the development and implementation of an ICT SCRM plan to be

developed at all levels of an organization. An ICT SCRM plan is an output of ICT supply chain

risk assessment and should contain ICT SCRM controls tailored to specific agency
 mission/business needs, operational environments, and/or implementing technologies.

719 720

721 1.7.1 Integration into Risk Management Process

722

723 The processes in this publication are integrated into the Risk Management Process described in 724 NIST SP 800-39 to facilitate integration of ICT SCRM into the overall federal agency risk 725 management activities. Section 2 provides an overview of the NIST SP 800-39 risk management 726 hierarchy and approach, and identifies ICT SCRM activities in the risk management process. The 727 structure of Section 2.2 mirrors NIST SP 800-39. Chapter 3 builds on NIST SP 800-39 Chapter 3, 728 providing descriptions and explanations of ICT SCRM activities. The processes and controls in 729 this publication should be integrated into agencies' existing system development life cycles and 730 organizational environments at all levels of the risk management hierarchy (organization, 731 mission, system).

732

733 1.7.2 Enhanced ICT SCRM Overlay

734 This publication contains an enhanced overlay of NIST SP 800-53 Rev. 4. It identifies, refines, 735 and expands ICT SCRM-related controls from NIST SP 800-53 Revision 4, adds new controls 736 that address specific ICT SCRM concerns, and offers ICT SCRM-specific supplemental guidance 737 where appropriate. Figure 1-5 illustrates the process that was used to create the enhanced overlay. 738 The individual controls and enhancements from NIST SP 800-53 Revision 4 that were relevant 739 and especially relevant to ICT SCRM were extracted. These controls were then analyzed to 740 determine how they apply to ICT SCRM. Additional supplemental guidance was then developed 741 and included for each control and control enhancement. The resulting set of controls and 742 enhancements were then evaluated to determine whether all ICT SCRM concerns were addressed. 743 A new control family, Provenance, and some additional controls and control enhancements were 744 created to address specific remaining ICT SCRM concerns. 745

745



Federal Information Systems and Organizations, Section 3.5

- 747 748 749
- 750
- 751

Managing Cost and Resources

Federal agencies should be aware that implementing these controls will require financial and human resources. Any requirements that result from federal agencies implementing these controls may also require financial and human resources from their system integrators, suppliers, and external service providers potentially resulting in increased costs to the federal acquirers. The acquirers should be cognizant of the costs and weight them against the benefits when selecting ICT SCRM controls. When appropriate, allow system integrators, suppliers, and external services providers the opportunity to reuse any existing data and documentation that may provide evidence to support ICT SCRM. The challenge of balancing ICT supply chain risks with benefits and costs of mitigating controls should be a key component of the federal agency acquirer's overall approach to ICT SCRM.

752 753 754

755

756

1.8 ORGANIZATION OF THIS SPECIAL PUBLICATION

757 This publication is organized as follows:

758 • Chapter 1 provides the purpose, scope, and applicability of the publication and describes 759 foundational concepts and practices. 760 Chapter 2 discusses ICT SCRM processes and how to integrate them into the • 761 organizational risk management hierarchy and risk management process, based on NIST 762 SP 800-39. 763 Chapter 3 provides a comprehensive set of baseline controls for organizations to choose • 764 from and the guidance required for customization/tailoring for their organization and ICT 765 needs. 766 • Appendix A provides a glossary of terms used in this publication. 767 Appendix B provides the acronyms and abbreviations used in this publication. • 768 Appendix C lists references used in the development of this publication. 769 Appendix D maps the ICT SCRM controls in this publication to their associated NIST SP 770 800-53 Revision 4 controls. 771 Appendix E provides NIST SP 800-53 Revision 4 controls relevant to ICT SCRM that • 772 are listed or expanded in Chapter 3. 773 Appendix F provides a listing of threats from NIST SP 800-30 Revision 1 Appendix E • 774 relevant to ICT SCRM. 775 Appendix G provides a Supply Chain Threat Analysis Framework and illustrative threat • 776 scenarios. 777 Appendix H provides an annotated ICT SCRM Plan Template. • 778

779 CHAPTER TWO

780 INTEGRATION OF ICT SCRM INTO 781 ORGANIZATION-WIDE RISK MANAGEMENT

782

787

788

789

790

ICT Supply Chain risk management should be integrated into the organization-wide risk
management process described in NIST SP 800-39 and depicted in Figure 2-1. This process
includes the following continuous and iterative steps:
(i) Frame risk – establish the context for risk-based decisions and the current state of th

- (i) Frame risk establish the context for risk-based decisions and the current state of the system or ICT supply chain infrastructure;
- (ii) Assess risk review and interpret criticality, threat, vulnerability, likelihood, impact, and related information;
- (iii) Respond to risk once determined select, tailor, and implement mitigation controls; and
- (iv) Monitor risk on an ongoing basis, including changes to an information system or ICT
 supply chain infrastructure, using effective organizational communications and a
- feedback loop for continuous improvement.
- 794



795 796

Figure 2-1: Risk Management Process

797

798 Managing ICT supply chain risks is a complex, multifaceted undertaking that requires a 799 coordinated effort across an organization and building trust relationships and communicating with 800 external and internal partners and stakeholders. This includes: engaging multiple disciplines in 801 identifying priorities and developing solutions; ensuring that ICT SCRM activities are performed 802 throughout the SDLC; and incorporating ICT SCRM into overall risk management decisions. ICT 803 SCRM activities should involve identifying and assessing applicable risks, determining 804 appropriate mitigating actions, developing ICT SCRM Plans to document selected mitigating 805 actions, and monitoring performance against ICT SCRM Plans. Because ICT supply chains differ 806 across and within organizations, ICT SCRM plans should be tailored to individual organizational, 807 program, and operational contexts. Tailored ICT SCRM plans will help organizations to focus

appropriate resources on the most critical functions and components based on organizational

809 mission/business requirements and their risk environment.

Organizations should ensure that tailored ICT SCRM Plans are designed to:

- Manage, rather than eliminate risk;
- Ensure that operations are able to adapt to constantly evolving threats;
- Be responsive to changes within their own organization, programs, and systems; and
- Adjust to the rapidly evolving practices of the private sector's global ICT supply chain.

810 811

812 Section 2.1 describes the three-tier risk management approach in terms of ICT SCRM. Generally, 813 senior leaders provide the strategic direction, mid-level leaders plan and manage projects, and 814 individuals on the front lines develop, implement, and operate the ICT supply chain 815 infrastructure. The activities performed in each tier can be integrated into an organization's 816 overall risk management process in order to ensure that the ICT SCRM program appropriately 817 supports the organization's mission and goals.⁶ Section 2.2 describes the Risk Management 818 Framework as it applies to ICT SCRM. The foundational concepts are described in greater detail 819 in NIST SP 800-39.

820

821 **2.1 MULTITIERED RISK MANAGEMENT** 822

To integrate risk management throughout an organization, NIST SP 800-39 describes three organizational tiers, depicted in Figure 2-2, that address risk at the: (i) organization level; (ii) mission/business process level; and (iii) information system level. ICT SCRM requires the

826 involvement of all three tiers.

⁶ This document uses the word "mission" to mean the organization's required tasks as determined by the organization's purpose and enterprise-level goals and priorities.





Figure 2-2: Multitiered Organization-wide Risk Management⁷

In general, Tier 1 is engaged in the development of the overall ICT SCRM strategy,

832 determination of organization-level ICT SCRM risks, and setting of the organization-wide ICT

833 SCRM policies to guide the federal agency activities in establishing and maintaining

organization-wide ICT SCRM capability. Tier 2 is engaged in prioritizing the federal agency
 mission and business functions, conducting mission/business-level risk assessment, implementing

836 Tier 1 strategy and guidance to establish the overall federal agency organizational capability to

manage ICT supply chain risks, and guiding organization-wide ICT acquisitions and their

corresponding SDLCs. Tier 3 is involved in specific ICT SCRM activities to be applied to
 individual information systems and information technology acquisitions, including integration of
 ICT SCRM into these systems' SDLCs.

841

The ICT SCRM activities can be performed by a variety of individuals or groups within a federal
agency ranging from a single individual to committees, divisions, programs, or any other
organizational structures. ICT SCRM activities will be distinct for different organizations

depending on their organizations structure, culture, mission, and many other factors. It should be

846 noted that this publication gives federal agencies the flexibility to either develop stand-alone

847 documentation (e.g. policies, assessment and authorization (A&A) plan and ICT SCRM Plan) for

848 ICT SCRM, or to integrate it into existing agency documentation.

⁷ Further information about the concepts depicted in Figure 2-2 can be found in NIST SP 800-39.

Table 2-1 shows generic ICT SCRM stakeholders for each tier with the specific ICT SCRM

activities performed within the corresponding tier. These activities are either direct ICT SCRM
 activities or have a direct impact on ICT SCRM.

- 853
- 854
- 855

Table 2-1: Supply Chain Risk Management Stakeholders

Tiers	Tier Name	Generic Stakeholder	Activities
1	Organization	Executive Leadership (CEO, CIO, COO, CFO, CISO, CTO, etc.) - Risk executive	Define corporate strategy, policy, goals and objectives
2	Mission	Business Management (includes program management (PM), research and development (R&D), Engineering [SDLC oversight], Acquisitions / Procurement, Cost Accounting, - "ility" management [reliability, safety, security, quality], etc.)	Develop actionable policies and procedures, guidance and constraints
3	Information Systems	Systems Management (architect, developers, system owner, QA/QC, test, contracting personnel (approving selection, payment and approach for obtaining, maintenance engineering, disposal personnel, etc.)	Policy implementation, requirements, constraints, implementations

856

857 The ICT SCRM process should be carried out across the three risk management tiers with the

858 overall objective of continuous improvement in the organization's risk-related activities and

859 effective inter-tier and intra-tier communication, thus integrating both strategic and tactical activities among all stakeholders with a shared interest in the mission/business success of the

organization. Whether addressing a component, a system, a process, a mission function, or a
 policy, it is important to engage the relevant ICT SCRM stakeholders at each tier to ensure that
 risk management activities are as informed as possible.

864

865 The next few sections provide example activities in each tier. However, because each

organization is different, there may be activities that are performed in different tiers than listed as

- 867 individual organizational context requires.
- 868

Chapter 3 provides a number of mission/business ICT SCRM controls that organizations can tailor for their use to help guide Tier 1, Tier 2, and Tier 3 ICT SCRM activities. It should be noted the tailoring should be scoped to the organization's risk management needs and take into consideration the costs associated with implementing ICT SCRM.

- 869
- 870
- 871

872 873

874

2.1.1 TIER 1 – ORGANIZATION

875

876 Tier 1 (Organization) provides strategic ICT SCRM direction for an organization using

877 organizational-level mission/business requirements and policies, governance structures such as

the risk executive (function), and organization-wide resource allocation strategies for ICT

879 SCRM. Tier 1 activities help to ensure that ICT SCRM solutions are cost-effective, efficient, and

880 consistent with the strategic goals and objectives of the organization. It is critical that, as

881 organizations define and implement organization-wide strategies, policies, and processes in this 882 tier, they include ICT SCRM considerations.

883

884 ICT SCRM activities at this tier include:

- 885 Establish ICT SCRM policies based on external and organizational requirements and 886 constraints (e.g., applicable laws and regulations). Policies should include the purpose 887 and applicability, as well as investment and funding requirements, of the ICT SCRM 888 program; 889 Based on the ICT SCRM policy, identify: • 890 Mission/business requirements that will influence ICT SCRM, such as cost, 0 891 schedule, performance, security, privacy, quality, and safety; 892 Information security requirements, including ICT SCRM-specific requirements; 0 893 Organization-wide mission/business functions and how ICT SCRM will be 0 894 integrated into their processes; 895 Establish risk tolerance level for ICT supply chain risks; • 896 Establish a group of individuals across the organization who will address ICT SCRM • 897 throughout the organization, known as the ICT SCRM Team; and 898 Ensure ICT SCRM is appropriately integrated into the organization risk management • 899 activities. 900 901 Implementing ICT SCRM requires that federal agencies establish a coordinated team-based 902 approach to assess ICT supply chain risk and manage this risk by using technical and 903 programmatic mitigation techniques. The coordinated team approach, either ad hoc or formal, 904 will enable agencies to conduct a comprehensive analysis of their ICT supply chain, communicate 905 with external partners/stakeholders, and gain broad consensus regarding appropriate resources for 906 ICT SCRM. 907 908 The ICT SCRM Team should consist of members with diverse roles and responsibilities for 909 leading and supporting ICT SCRM activities including information technology, information 910 security, contracting, risk executive, mission/business, legal, supply chain and logistics, 911 acquisition and procurement, and other relevant functions. These individuals may include 912 government personnel or prime contractors hired to provide acquisition services to a government 913 client. 914 915 Members of the ICT SCRM team should be a diverse group of people who are involved in the 916 various aspects of the SDLC. Collectively, to aid in ICT supply chain risk management, these 917 individuals should have an awareness of, and provide expertise in organizational acquisition 918 processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding 919 of the technical aspects and dependencies of systems. 920 921 2.1.2 TIER 2 – MISSION/BUSINESS PROCESS
- 922

925 requirements are defined and managed – including ICT SCRM as well as cost, schedule, 926 performance, and a variety of critical nonfunctional requirements. These nonfunctional 927 requirements are also known as "ilities" and include concepts such as reliability, dependability. 928 safety, security, and quality. Many threats to and through the supply chain are addressed at this 929 level in the management of trust relationships with system integrators, suppliers, and external 930 service providers of ICT products and services. Because ICT SCRM can both directly and 931 indirectly impact mission/business processes, understanding, integrating and coordinating ICT 932 SCRM activities at this tier are critical for ensuring successful federal agency mission and 933 business operations. 934 935 ICT SCRM activities at this tier include: 936 • Defining the risk response strategy, including ICT SCRM considerations, for critical 937 processes: 938 • Establishing ICT SCRM processes to support mission/business processes; 939 Determining the ICT SCRM requirements of the mission/business systems needed to • 940 execute the mission/business processes; 941 • Incorporating ICT SCRM requirements into the mission/business processes; 942 Integrating ICT SCRM requirements into an enterprise architecture to facilitate the • 943 allocation of ICT SCRM controls to organizational information systems and the 944 environments in which those systems operate; and 945 Establishing a mission/business-specific ICT SCRM team that coordinates and • 946 collaborates with the organizational ICT SCRM team. 947 948 949 2.1.3 TIER 3 – INFORMATION SYSTEMS 950

Tier 2 (Mission/Business Process) addresses risk from a *mission/business process* perspective and

is informed by the risk context, risk decisions, and risk activities at Tier 1.⁸ In this tier, program

951 Tier 3 (Information Systems) is where ICT SCRM activities are integrated into the SDLC of 952 organizational information systems and system components. Many threats *through* the supply 953 chain are addressed at this level with the use of ICT SCRM-related information security 954 requirements. Risk management activities at Tier 3 reflect the organization's risk management 955 strategy defined in Tier 1 (per NIST SP 800-39), as well as cost, schedule, and performance 956 requirements for individual information systems as defined in Tier 2. ICT SCRM activities at this 957 tier include:

958 959

960

923

924

• Applying ICT SCRM controls in the development and sustainment of systems supporting mission/business processes; and

⁸ For more information, see National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, Section 2.2, *Multitiered Risk Management*.

963

964

• Applying ICT SCRM controls to the SDLC and the environment in which the SDLC is conducted (e.g., ICT supply chain infrastructure) used to develop and integrate mission/business systems.

At Tier 3, ICT SCRM significantly intersects with the SDLC, which includes acquisition (both
 custom and off-the-shelf), requirements, architectural design, development, delivery, installation,
 integration, maintenance, and disposal/retirement of information systems, including ICT products
 and services.

970 2.2 ICT SCRM ACTIVITIES IN RISK MANAGEMENT PROCESS 971

972 Risk management is a comprehensive process that requires organizations to: (i) frame risk (i.e., 973 establish the context for risk-based decisions); (ii) assess risk; (iii) respond to risk once 974 determined; and (iv) monitor risk on an ongoing basis using effective organizational 975 communications and a feedback loop for continuous improvement in the risk-related activities of 976 organizations. Figure 2-3 depicts interrelationships among the risk management process steps, 977 including the order in which each analysis may be executed and the interactions required to 978 ensure that the analysis is inclusive of the various inputs at the organization, mission, and 979 operations levels. 980

980 981



982 983 984

Figure 2-3: ICT SCRM Risk Assessment

985 The steps in the risk management process – Frame, Assess, Respond, and Monitor - are iterative 986 and not inherently sequential in nature. Different individuals can perform the steps at the same 987 time depending on a particular need or situation. Organizations have significant flexibility in how 988 the risk management steps are performed (e.g., sequence, degree of rigor, formality, and 989 thoroughness of application) and in how the results of each step are captured and shared—both 990 internally and externally. The outputs from a particular risk management step will directly impact 981 one or more of the other risk management steps in the risk management process.

Figure 2-4 summarizes ICT SCRM activities throughout the risk management process as they are
performed within the three organizational tiers. The arrows between different steps of the risk
management process depict simultaneous flow of information and guidance among the steps.
Together the arrows indicate that the inputs, activities, and outputs are continuously interacting
and influencing one another. More details are provided in the following subsections.

- 998
- 999

terprise	 Frame Develop ICT SCRM Policy Conduct Baseline Criticality Determination Integrate ICT SCRM 	 Assess Integrate ICT SCRM considerations into enterprise risk management 	 Respond Make enterprise risk decisions to avoid, mitigate, share, or transfer risk Select, tailor, and implement appropriate enterprise ICT 	 Monitor Integrate ICT SCRM into agency Continuous Monitoring program Monitor and evaluate enterprise-level constraints and
E	considerations into enterprise risk management		SCRM controls • Document controls in Enterprise ICT SCRM Plan	 risks for change and impact Monitor effectiveness of enterprise-level risk response
Mission/Business Process	 Define ICT SCRM Mission/business requirements Incorporate these requirements into mission/ business processes and enterprise architecture Establish ICT SCRM Risk Assessment Methodology Establish FIPS 199 impact levels Conduct Mission Function Baseline Criticality Determination Determine ICT SCRM risk assessment methodology 	 Conduct Risk Assessment including Criticality Analysis for mission threads Determine current risk posture 	 Make mission/business-level risk decisions to avoid, mitigate, share, or transfer risk Select, tailor , and implement appropriate mission/ business- level controls Document controls in Mission- level ICT SCRM Plan 	 Identify which mission functions need to be monitored for ICT supply chain change and assessed for impact Integrate ICT SCRM into Continuous Monitoring processes and systems Monitor and evaluate mission- level risks and constraints for change and impact Monitor effectiveness of mission-level risk response
System	• Define system-level ICT SCRM requirements	 Conduct ICT SCRM Risk Assessment including Criticality Analysis for individual systems Determine current risk posture 	 Make mission/business-level risk decisions to avoid, mitigate, share, or transfer risk Select, tailor, and implement appropriate system-level controls Document ICT SCRM controls in System Security Plan 	 Monitor and evaluate system-level requirements and risks for change and impact Monitor effectiveness of system-level risk response

1000

- 1001
- 1002

1003

Figure 2-4: ICT SCRM Activities in Risk Management Process

Figure 2-4 depicts interrelationships among the risk management process steps including the
 order in which each analysis is executed and the interactions required to ensure that the analysis is
 inclusive of the various inputs at the organization, mission, and operations levels.

The remainder of this section provides a detailed description of ICT SCRM activities within the
 Frame, Assess, Respond, and Monitor steps of the Risk Management Process. The structure of

- 1010 subsections 2.2.1 through 2.2.4 mirrors the structure of NIST SP 800-39, Sections 3.1-3.4. For
- 1011 each step of the Risk Management Process (i.e., Frame, Assess, Respond, Monitor), the structure
- 1012 includes Inputs and Preconditions, Activities, and Outputs and Post-Conditions. Activities are
- 1013 further organized into Tasks according to NIST SP 800-39. NIST SP 800-161 cites the steps and 1014
- tasks of the risk management process but rather than repeating any other content of NIST SP 800-1015
- 39, it provides ICT SCRM-specific guidance for each step with its Inputs and Preconditions, 1016 Activities with corresponding Tasks, and Outputs and Post-Conditions. NIST SP 800-161 adds
- 1017 one task to the tasks provided in NIST SP 800-39, under the Assess step: Task 2-0, Criticality Analvsis.
- 1018
- 1019 1020

1021 2.2.1 FRAME

1022 **Inputs and Preconditions** 1023

1024 *Frame* is the step that establishes context for ICT SCRM in all three tiers. The scope and structure 1025 of the organizational ICT supply chain landscape, the overall risk management strategy, as well 1026 as specific program/project or individual information system needs, are defined in this step. The 1027 data and information collected during Frame provides inputs for scoping and fine-tuning ICT 1028 SCRM activities in other risk management process steps throughout the three tiers.

1029

1030 NIST SP 800-39 defines risk framing as "the set of assumptions, constraints, risk tolerances, and 1031 priorities/trade-offs that shape an organization's approach for managing risk." ICT SCRM risk 1032 framing should be integrated into the overall organization risk framing process. Outputs of the 1033 organization's risk framing and the overall risk management process should serve as inputs into 1034 the ICT SCRM risk framing, including but not limited to:

- 1035 1036
- Organization policies, strategies, and governance; •
- Applicable laws and regulations; 1037 •
- Mission functions and business goals; 1038 •
- 1039 Organization processes (security, quality, etc.); •
- 1040 Organization threats, vulnerabilities, risks, and risk tolerance; •
 - Criticality of mission functions;
 - Enterprise Architecture; •
 - Mission-level security policies; •
 - Functional requirements; and
 - Security requirements. •
- 1045 1046

1041

1042

1043

1044

1047 ICT SCRM risk framing is an iterative process that also uses inputs from the other steps of the 1048 risk management process (Assess, Respond, and Monitor) as inputs. Figure 2-5 depicts the Frame 1049 Step with its inputs and outputs along the three organizational tiers.

- 1050
- 1051
- 1052
- 1053



1057

Figure 2-5: ICT SCRM in the Frame Step

1058 Figure 2-5 depicts inputs, activities, and outputs of the Frame Step distributed along the three 1059 organizational tiers. The large arrows on the left and right sides of the activities depict the inputs 1060 and outputs to and from other steps of the Risk Management Process, with the arrow on the left 1061 depicting that the steps are in constant interaction. Inputs into the Frame Step include inputs from 1062 other steps as well as inputs from the organization risk management process that are shaping the 1063 ICT SCRM process. Up-down arrows between the tiers depict flow of information and guidance 1064 from the upper tiers to the lower tiers and the flow of information and feedback from the lower 1065 tiers to the upper tiers. Together the arrows indicate that the inputs, activities, and outputs are 1066 continuously interacting and influencing one another.

1067 1068 *Activities*

1069 RISK ASSUMPTIONS

1070 TASK 1-1: Identify assumptions that affect how risk is assessed, responded to, and monitored1071 within the organization.

1072

1073 Supplemental Guidance:

- 1074 1075 As a part of identifying ICT supply chain Risk Assumptions within the broader Risk Management
- 1076 process (described in NIST SP 800-39), agencies should do the following:

ical to the organization, ality; reat sources, ions related to ICT ies, depending on /business functions; and ntegrated into the overall
ality; reat sources, ions related to ICT ies, depending on /business functions; and ntegrated into the overall
reat sources, ions related to ICT ies, depending on /business functions; and ntegrated into the overall
ions related to ICT ies, depending on /business functions; and ntegrated into the overall
ies, depending on /business functions; and ntegrated into the overall
ies, depending on /business functions; and ntegrated into the overall
ies, depending on /business functions; and ntegrated into the overall
ies, depending on /business functions; and ntegrated into the overall
/business functions; and ntegrated into the overall
ntegrated into the overall
C
likely to regult in
inkery to result in
on their supporting
Iware, software, and
sed to implement the
e functions (e.g., access
ower supply) may also
d by which mission-
prioritized.
ritical components and
quirements, architecture,
m operation. Baseline
at support mission
uirements. This analysis
al agencies should
ed to specific context in
ed to specific context in
are during both Frame
ers during bour Frame
periorined at a night
Sugn additional iterations
lowing:
ons, policies,
al functions, systems,
al functions, systems,
al functions, systems, vers;
al functions, systems, vers; idual systems: and
al functions, systems, vers; idual systems; and the systems/
al functions, systems, vers; idual systems; and / the systems/
al functions, systems, vers; idual systems; and v the systems/ at are critical to the twork
al functions, systems, vers; idual systems; and / the systems/ nat are critical to the twork.
al functions, systems, vers; idual systems; and / the systems/ hat are critical to the twork.
al functions, systems, vers; idual systems; and / the systems/ nat are critical to the twork.
al functions, systems, vers; idual systems; and y the systems/ hat are critical to the twork. as or for future system ive activity that should
- 1128 1129 Threat Sources:
- 1130

1131 For ICT SCRM, threat sources include: (i) hostile cyber/physical attacks either to the supply 1132 chain or to an information system component(s) traversing the supply chain; (ii) human errors; or 1133 (iii) geopolitical disruptions, economic upheavals, natural, or man-made disasters. NIST SP 800-1134 39 states that organizations provide a succinct characterization of the types of tactics, techniques, 1135 and procedures employed by adversaries that are to be addressed by safeguards and 1136 countermeasures (i.e., security controls) deployed at Tier 1 (organization level), at Tier 2 1137 (mission/business process level), and at Tier 3 (information system level)—making explicit the 1138 types of threat sources that are to be addressed as well as making explicit those not being addressed by the safeguards/countermeasures. 1139

1140

1141 Threat information includes historical threat data, factual threat data, or validated technology-1142 specific threat information. Threat information may come from multiple information sources, 1143 including the U.S. Intelligence Community (for federal agencies), as well as open source

reporting such as news and trade publications, partners, suppliers, and customers.

1145

Information about ICT supply chain (such as from supply chain maps) provides the context for
identifying possible locations or access points for threat agents to enter the ICT supply chain. The
ICT supply chain threat agents are similar to the information security threat agents, such as
attackers or industrial spies. Table 22 lists examples of ICT supply chain threat agents. Appendix
G provides Supply Chain Threat Scenarios listed in Table 2-2.

1151

- 1152
- 1153 1154

Table 2-2: Example ICT Supply Chain Threat Agents

Threat Agent	Scenario	Examples
Counterfeiters	Counterfeits inserted into ICT supply chain (see Appendix G Scenario 1)	Criminal groups seek to acquire and sell counterfeit ICT components for monetary gain. Specifically, organized crime groups seek disposed units, purchase overstock items, and acquire blueprints to obtain ICT components that they can sell through various gray market resellers to acquirers. ⁹
Insiders	Intellectual property loss	Disgruntled insiders sell or transfer intellectual property to competitors or foreign intelligence agencies for a variety of reasons including monetary gain. Intellectual property includes software code, blueprints, or documentation.
Foreign Intelligence Services	Malicious code insertion (see Appendix G	Foreign intelligence services seek to penetrate ICT supply chain and implant unwanted functionality (by inserting new or modifying existing functionality) to be

⁹ "Defense Industrial Base Assessment: Counterfeit Electronics," U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, http://www.bis.doc.gov/, January 2010.

Threat Agent	Scenario	Examples
	Scenario 3)	used when the system is operational to gather
		information or subvert ¹⁰ system or mission operations.
Terrorists	Unauthorized	Terrorists seek to penetrate ICT supply chain and may
	access	implant unwanted functionality (by inserting new or
		modifying existing functionality) or subvert system or
		mission operations.
Industrial	Industrial	Industrial spies seek to penetrate ICT supply chain to
Espionage	Espionage (see	gather information or subvert system or mission
	Appendix G	operations.
	Scenario 2)	

1156

1157Agencies can identify and refine ICT SCRM-specific threats in all three tiers. Table 2-3 provides1158examples of threat considerations and different methods that can be used to characterize ICT

1159 supply chain threats at different tiers.

1160

1161

1162

Table 2-3: Supply Chain Threat Considerations

Tier	Threat Consideration	Methods
Tier 1	 Organization's business and mission Strategic supplier relationships Geographical considerations related to the extent of the organization's ICT supply chain 	 Establish common starting points for identifying ICT supply chain threat. Establish procedures for countering organization-wide threats such as insertion of counterfeits into critical systems and components.
Tier 2	 Mission functions Geographic locations Types of suppliers (COTS, external service providers, or custom, etc.) Technologies used organization-wide 	 Identify additional sources of threat information specific to organizational mission functions. Identify potential threat sources based on the locations and suppliers identified through examining available agency ICT supply chain information (e.g., from supply chain map.) Scope identified threat sources to the specific mission functions, using the agency the ICT supply chain information. Establish mission-specific preparatory

¹⁰ Examples of subverting operations include gaining unauthorized control to ICT supply chain or flooding it with unauthorized service requests to reduce or deny legitimate access to ICT supply chain.

	Tier	Threat Consideration	Methods
			procedures for countering threat
			adversaries/natural disasters.
	Tier 3	• SDLC	 Base the level of detail with which threats should be considered on the SDLC phase. Identify and refine threat sources based on the potential for threat insertion within individual SDLC processes.
1163 1164	T 7 J J	1	
1165	vuinerabi	ittes	
1167	A vulnera	bility is a weakness in an information system	m, system security procedures, internal
1168	controls, o	or implementation that could be exploited or	r triggered by a threat source. ¹¹ Within the
1169	ICT SCRI	M context, it is any weakness in the system/	component design, development,
1170	manufactu	iring, production, shipping and receiving, d	elivery, operation, and component end-of
11/1	life that ca	an be exploited by a threat agent to significate hoth the	antiy degrade performance of a system that
11/2 1172	supports t	the mission. This demittion applies to both t	augustic and a second s
11/3	and megr	aled (i.e., within the SDLC) and to the ICT	suppry chain infrastructure, including any

1174 security mitigations and techniques, such as identity management or access control systems.

1175

1177

1178

1179

1180

1181

1176 ICT supply chain vulnerabilities may be found in:

- The systems/components within the SDLC (i.e., being developed and integrated);
- The development and operational environment directly impacting the SDLC; and •
- The logistics/delivery environment that transports ICT systems and components (logically or physically).

1182 Organizations should identify approaches used to characterize ICT supply chain vulnerabilities, 1183 consistent with the characterization of threat sources and events and with the overall approach 1184 used by the organization for characterizing vulnerabilities. Appendix F provides examples of ICT 1185 supply chain threat events, based on NIST SP 800-30 Revision 1 Appendix E. 1186

1187 All three organizational tiers should contribute to determining the organization's approaches to 1188 characterize vulnerabilities, with progressively more detail identified and documented in the 1189 lower tiers. Table 2-4 provides examples of considerations and different methods that could be 1190 used to characterize ICT supply chain vulnerabilities at different tiers.

- 1191 1192
- 1193

Table 2-4: Supply Chain Vulnerabilities Considerations

¹¹ NIST SP 800-53: 800-53A: 800-37: 800-60: 800-115: FIPS 200

1	1	94

Tier	Vulnerability Consideration	Methods
Tier 1	 Organization's mission/business Supplier relationships (e.g., system integrators, COTS, external services) Geographical considerations related to the extent of the organization's ICT supply chain Enterprise/Security Architecture Criticality Baseline 	 Examine agency ICT supply chain information including that from supply chain maps to identify especially vulnerable locations or organizations. Analyze agency mission for susceptibility to potential supply chain vulnerabilities. Examine system integrator and supplier relationships for susceptibility to potential supply chain vulnerabilities. Review enterprise architecture and criticality baseline to identify areas of weakness requiring more robust ICT supply chain considerations.
Tier 2	 Mission functions Geographic locations Types of suppliers (COTS, custom, etc.) Technologies used 	 Refine analysis from Tier 1 based on specific mission functions and applicable threat and supply chain information. Consider using National Vulnerability Database (NVD), including Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS), to characterize, categorize, and score vulnerabilities. Consider using scoring guidance to prioritize vulnerabilities for remediation.
Tier 3	• Individual technologies, solutions, and suppliers should be considered.	 Use CVEs where available to characterize and categorize vulnerabilities. Identify weaknesses.

1196 Consequences and Impact

1197

Impact is the effect on organizational operations, organizational assets, individuals, other
organizations, or the Nation (including the national security interests of the United States) of a
loss of confidentiality, integrity, or availability of information or an information system (NIST SP
800-53 Revision 4).

1202

For ICT SCRM, impact should be considered for the systems or components traversing the ICT
supply chain, the supply chain itself, the ICT supply chain infrastructure, and the organization- or
mission-level activities. All three tiers in the risk management hierarchy may be impacted.
Potential impacts can be gathered through reviewing historical data for the agency, similar peer
organizations, or applicable industry surveys. In this publication, impact is always in relation to
the organization's mission and includes the systems or components traversing the supply chain as

1209 well as the supply chain itself.

1212

1213

1214

1215

1216

1217

1225

1235

1236

1237

1243 1244

1245

- 1211 The following are examples of ICT supply chain consequences and impact:
 - An earthquake in Malaysia reduced the amount of commodity Dynamic Random Access Memory (DRAM) to 60% of the world's supply, creating a shortage for hardware maintenance and new design.
 - Accidental procurement of a counterfeit part resulted in premature component failure, thereby impacting the organization's mission performance.

1218 Likelihood 1219

In an information security risk analysis, likelihood is a weighted factor based on a subjective
analysis of the probability that a given threat is capable of exploiting a given vulnerability.¹²
Agencies should determine which approach(es) they will use to determine the likelihood of an
ICT supply chain compromise, consistent with the overall approach used by the agency's risk
management function.

1226 RISK CONSTRAINTS

TASK 1-2: Identify constraints¹³ on the conduct of risk assessment, risk response, and risk
 monitoring activities within the organization.

1230 Supplemental Guidance:1231

1232 Identify the following two types of constraints to ensure that the ICT supply chain is integrated
1233 into the agency risk management process:
1234

- 1. Agency constraints; and
- 2. ICT supply chain-specific constraints.

Agency constraints serve as an overall input into framing the ICT supply chain policy at Tier 1,
mission requirements at Tier 2, and system-specific requirements at Tier 3. Table 2-5 lists the
specific agency and ICT supply chain constraints. ICT supply chain constraints, such as ICT
SCRM policy and ICT SCRM requirements, may need to be developed if they do not exist.

Table 2-5: Supply Chain Constraints

Tier	Agency Constraints	ICT Supply Chain Constraints
Tier 1	 Organization policies, strategies, governance Applicable laws and regulations Mission functions 	• Organization ICT SCRM policy based on the existing agency policies, strategies, and governance; applicable laws and regulations; mission

¹² CNSSI-4009

¹³ Refer to NIST SP 800-39, Section 3.1, Task 1-2 for a description of constraints in the risk management context.

	• Organization processes (security, quality, etc.)	functions; and organization processes.
Tier 2	 Mission functions Criticality of functions Enterprise Architecture Mission-level security policies 	• ICT SCRM Mission/business requirements that are incorporated into mission/business processes and enterprise architecture.
Tier 3	Functional requirementsSecurity requirements	System-level ICT SCRM requirements.

1247

1262 1263

1264

1265

1266

1267

1268

1269

1270

1271

1272

1273

1274

1275

1276

An organization ICT SCRM policy is a critical vehicle for guiding ICT SCRM activities. Driven by applicable laws and regulations, this policy should support applicable organization policies including acquisition and procurement, information security, quality, and supply chain and logistics. It should address goals and objectives articulated in the overall agency strategic plan, as well as specific mission functions and business goals, along with the internal and external customer requirements. It should also define the integration points for ICT SCRM with the agency's Risk Management Process and SDLC.

ICT SCRM policy should define ICT SCRM-related roles and responsibilities of the agency ICT
 SCRM team, any dependencies among those roles, and the interaction among the roles. ICT
 SCRM-related roles will articulate responsibilities for conducting the risk assessment, identifying
 and implementing risk-based mitigations, and performing monitoring functions. Identifying and
 validating roles will help to specify the amount of effort that will be required to implement the
 ICT SCRM Plan. Examples of ICT SCRM-related roles include:

- Risk executive function that provides overarching ICT supply chain risk guidance to engineering decisions that specify and select ICT products as the system design is finalized;
 - Procurement officer and maintenance engineering responsible for identifying and replacing the hardware when defective;
 - Delivery organization and acceptance engineers who verify that the part is acceptable to receive into the acquiring organization;
 - System integrator responsible for system maintenance and upgrades, whose staff resides in the acquirer facility and uses system integrator development infrastructure and the acquirer operational infrastructure;
- System Security Engineer/Systems Engineer responsible for ensuring that information system security concerns are properly identified and addressed; and
 - The end user of ICT systems/components/services.

1277 ICT SCRM requirements should be guided by the ICT SCRM policy, as well as by the mission
1278 functions and their criticality at Tier 2 and by known functional and security requirements at Tier
1279 3.

- 1280
- 1281 RISK TOLERANCE

TASK 1-3: Identify the level of risk tolerance for the organization.

1283

1284 Supplemental Guidance:

1286 Risk tolerance is the level of risk that organizations are willing to accept in pursuit of strategic

- goals and objectives (NIST SP 800-39). Organizations should take into account ICT supply chain
 threats, vulnerabilities, constraints, and baseline criticality, when identifying the overall level of
 risk tolerance. ¹⁴
- 1200
- 1291 PRIORITIES AND TRADE-OFFS
- **TASK 1-4:** Identify priorities and trade-offs considered by the organization in managing risk.

1294 Supplemental Guidance

1295

As a part of identifying priorities and trade-offs, organizations should consider ICT supply chain
 threats, vulnerabilities, constraints, and baseline criticality.

12981299 Outputs and Post Conditions

Within the scope of NIST SP 800-39, the output of the risk framing step is the *risk management strategy* that identifies how organizations intend to assess, respond to, and monitor risk over time.
This strategy should clearly include ICT SCRM considerations that were identified and result in
the establishment of ICT SCRM-specific processes throughout the agency. These processes
should be documented in one of three ways:

1305 1306

1307 1308

1309

- 1. Integrated into existing agency documentation;
- 2. A separate set of documents addressing ICT SCRM; or
- 3. A mix of separate and integrated documents, based on agency needs and operations.
- 1310 The following information should be provided as an output of the risk framing step, regardless of1311 how the outputs are documented:
- 1312 1313

1314

1315

1316

1317

1318

1319

1320

1321

1322

- ICT SCRM Policy;
- Baseline Criticality including prioritized mission functions and FIPS 199 criticality;
- ICT supply chain risk assessment methodology and guidance;
- ICT supply chain risk response guidance;
 - ICT supply chain risk monitoring guidance;
 - ICT SCRM mission/business requirements;
 - Revised mission/business processes and enterprise architecture with ICT SCRM considerations integrated; and
 - System-level ICT SCRM requirements.

Outputs from the risk framing step serve as inputs to the risk assessment, risk response, and riskmonitoring steps.

¹⁴ Federal Departments' and Agencies' governance structures vary widely (see NIST SP 800-100, Section 2.2.2). Regardless of the governance structure, individual agency risk decisions should apply to the agency and any subordinate organizations, but not in the reverse direction.

1326 **2.2.2 ASSESS**

1327 Inputs and Preconditions

1328

Assess is the step where all the collected data is used to conduct a risk assessment. A number of
inputs are combined and analyzed to identify the likelihood and the impact of an ICT supply
chain compromise, including criticality, threat, and vulnerability analysis results; stakeholder
knowledge; and policy, constraints, and requirements.

An ICT supply chain risk assessment should be integrated into the overall organization risk assessment processes. ICT SCRM risk assessment results should be used and aggregated as

appropriate to communicate ICT supply chain risks at each tier of the organizational hierarchy.

1337 Figure 2-6 depicts the Assess Step with its inputs and outputs along the three organizational tiers.

- 1338
- 1339



1340 1341

1342

1343 Similar to Figure 2-5, Figure 2-6 depicts inputs, activities, and outputs of the Assess Step 1344 distributed along the three organizational tiers. The large arrows on the left and right sides of the 1345 activities depict the inputs from other steps of the Risk Management Process, with the arrow on 1346 the left depicting that the steps are in constant interaction. Inputs into the Assess Step include 1347 inputs from the other steps. Up-down arrows between the tiers depict flow of information and 1348 guidance from the upper tiers to the lower tiers and the flow of information and feedback from 1349 the lower tiers to the upper tiers. Together the arrows indicate that the inputs, activities, and 1350 outputs are continuously interacting and influencing one another.

1352 Criticality, vulnerability, and threat analyses are essential to the supply chain risk assessment 1353 process. As depicted in Figure 2-4, vulnerability and threat analyses can be performed in any 1354 order and may be performed iteratively to ensure that all applicable threats and vulnerabilities 1355 have been identified.

1356

The order of activities that begins with the update of the criticality analysis ensures that the assessment is scoped to include only relevant critical mission functions and the impact of ICT supply chain on these mission functions. The likelihood of exploitability is a key step to understanding impact. It becomes a synthesis point for criticality analysis, vulnerability analysis, and threat analysis and helps to further clarify impact to support an efficient and cost-effective risk decision.

1363 1364 *Activities*

1366 CRITICALITY ANALYSIS 1367

TASK 2-0: Update Criticality Analysis of mission-critical functions, systems, and components to
 narrow the scope (and resources) for ICT SCRM activities to those most important to mission
 success.

1371 Supplemental Guidance

1372

1365

1373 Criticality analysis should include the ICT supply chain infrastructure for both the federal agency
1374 and applicable system integrators, suppliers, external service providers, and the
1375 systems/components/services. Criticality analysis assesses the direct impact they each have on the
1376 mission priorities. ICT supply chain infrastructure includes the SDLC for applicable systems,
1377 services, and components because the SDLC defines whether security considerations are built
1378 into the systems/components or added after systems/components have been created.

1379

Organizations should update and tailor Baseline Criticality established during the Frame Step of
 the risk management process, including FIPS 199 system categorization, based on the information
 newly discovered in the Assess step. Organizations should use their own discretion for whether to
 perform criticality analysis for moderate-impact systems.

In addition to updating and tailoring Baseline Criticality, performing criticality analysis in theAssess Step may include the following:

1387 1388

1389

- Perform a dependency analysis and assessment to establish which components may require hardening given the system architecture;
- Obtain and review existing information that the agency has about critical ICT
 systems/components such as locations where they are manufactured or developed,
 physical and logical delivery paths, information flows and financial transactions

1393 1394	associated with these components, and any other available information that can provide insights into ICT supply chain of these components ¹⁵ and
1395	 Correlate identified critical components/services to the information about the ICT supply
1396	chain, the ICT supply chain infrastructure, historical data, and SDLC to identify critical
1397	ICT supply chain paths.
1398	
1399	
1400	The outcome of the updated criticality analysis is a narrowed, prioritized list of the organization's
1401	critical functions, systems, and components. Organizations can use the Baseline Criticality
1402	process in Section 2.2.1, Task 1-1, to update Criticality Analysis.
1403	F
1404	Because more information will be available in the Assess step, organizations can narrow the
1405	scope and increase the granularity of a criticality analysis. When identifying critical functions and
1406	associated systems/components and assigning them criticality levels, consider the following:
1407	
1408	• Functional breakdown is an effective method to identify functions associated critical
1409	components and supporting defensive functions.
1410	 Dependency analysis is used to identify the functions on which critical functions depend
1411	(e.g. defensive functions such as digital signatures used in software natch accentance)
1412	Those functions become critical functions themselves:
1413	 Identification of all access points to identify and limit unmediated access to critical
1414	function/components (e.g. least-privilege implementation): and
1415	 Malicious alteration can happen throughout the SDLC
1415	• Wancibus alteration can happen throughout the SDLC.
1410 1417	The resulting list of critical functions is used to guide and inform the vulnerability analysis and
1418	threat analysis to determine the initial ICT SCRM risk as denicted in Figure 2-4. ICT supply
1419	chain countermeasures and mitigations can then be selected and implemented to reduce risk to
1420	accentable levels
1420	
1421	Criticality analysis is performed iteratively and may be performed at any point in the SDLC and
1422	concurrently at each tier. The first iteration is likely to identify critical functions and
1424	systems/components that have a direct impact on mission functions. Successive iterations will
1425	include information from the criticality analysis threat analysis vulnerability analysis and
1426	mitigation strategies defined at each of the other tiers. Each iteration will refine the criticality
1420	analysis outcomes and result in the addition of defensive functions. Several iterations are likely
1427	needed to establish and maintain the criticality analysis results
1429	needed to establish and mantani the entreality analysis results.
1430	THREAT AND VULNERABILITY IDENTIFICATION
1 1 2 0	

¹⁵ This information may be available from a supply chain map for the agency or individual IT projects or systems. Supply chain maps are descriptions or depictions of supply chains including the physical and logical flow of goods, information, processes, and money upstream and downstream through a supply chain. They may include supply chain nodes, locations, delivery paths, or transactions.

TASK 2-1: Identify threats to and vulnerabilities in organizational information systems and the
 environments in which the systems operate.

1433

1434 Supplemental Guidance

1435

In addition to threat and vulnerability identification, as described in NIST SP 800-39 and NIST
SP 800-30, organizations should conduct ICT supply chain threat analysis and vulnerability
analysis.

- 1439
- 1440 Threat Analysis

1441 For ICT SCRM, threat analysis provides specific and timely threat characterization of natural 1442 1443 disaster possibilities and potential threat actors, including any identified system integrators, suppliers, or external service providers,¹⁶ to inform management, acquisition, engineering, and 1444 1445 operational activities within an organization. Threat analysis can use a variety of information to 1446 assess potential threats, including open source, intelligence, and counterintelligence. 1447 Organizations should use the threat sources defined during the Frame Step in threat analysis 1448 conducted during the Assess Step. Organizations should use the results of the threat analysis in 1449 the Assess Step to ultimately support acquisition decisions, alternative build decisions, and 1450 development and selection of appropriate mitigations in the Respond Step. ICT supply chain 1451 threat analysis should be based on the results of the criticality analysis. Specific identified threats may include people, processes, technologies, or natural and man-made disasters.

1452 1453

Agencies should use information available from existing incident management activities to
determine whether they have experienced an ICT supply chain compromise and to further
investigate such compromises. Some ICT supply chain compromises may not be recognized as
such at first and may be initially identified as an information security incident. Agencies should
define criteria for what constitutes an ICT supply chain compromise to ensure that such
compromises can be identified as a part of post-incident activities including forensics
investigations.

1461

1463

1464

1465

1466

1467

1468

1469

1462 ICT supply chain threat analysis should capture at least the following data:

- Changes to the systems/components or SDLC environment;
- Observation of ICT supply chain-related attacks while they are occurring;
- Incident data collected post-ICT supply chain-related compromise;
- Observation of tactics, techniques, and procedures used in specific attacks, whether observed or collected using audit mechanisms; and
- Natural and man-made disasters before, during, and after occurrence.

1470 Vulnerability Analysis

¹⁶ Please note that threat characterization of system integrators, suppliers, and external service providers may be benign.

- 1472 Within an ICT SCRM context, a vulnerability is any weakness in system/component design,
- development, production, or operation that can be exploited by a threat to defeat a system's
- 1474 mission objectives or to significantly degrade its performance.
- 1475
- 1476 Vulnerability analysis is an iterative process that informs risk assessment and countermeasure
 1477 selection. The vulnerability analysis works alongside the threat analysis to help inform the impact
 1478 analysis and to help scope and prioritize vulnerabilities to be mitigated.
- 1479

1480 Vulnerability analysis in the Assess Step should use the approaches used during the Frame Step
 1481 to characterize ICT supply chain vulnerabilities. Vulnerability analysis should begin with

- 1482 identifying vulnerabilities that are applicable to mission-critical functions and
- 1483 systems/components identified by criticality analysis. Investigation of vulnerabilities may
- 1484 indicate the need to raise or at least reconsider the criticality levels of functions and components
- 1485 identified in earlier criticality analyses. Later iterations of vulnerability analysis may also identify
- additional threats, or opportunities for threats, that were not considered in earlier threatassessments.
- 1488

Table 2-6 provides examples of applicable ICT supply chain vulnerabilities that can be observedwithin the three organizational tiers.

1491

1492

1493

Table 2-6: Examples of ICT Supply Chain Vulnerabilities Mapped to the Organizational Tiers

	Vulnerability Types	Mitigation Types
Tier 1 – Organization	 Deficiencies or weaknesses in organizational governance structures or processes such as a lack of ICT SCRM Plan 	 Provide guidance on how to consider dependencies on external organizations as vulnerabilities. Seek out alternate sources of new technology including building in- house.
Tier 2 – Mission/ Business	 No operational process is in place for detecting counterfeits. No budget was allocated for the implementation of a technical 	 Develop a program for detecting counterfeits and allocate appropriate budgets for putting in resources and training
	 screening for acceptance testing of ICT components entering the SDLC as replacement parts. 3) Susceptibility to adverse issues from innovative technology supply sources (e.g., technology owned or managed by third parties is buggy). 	 Allocate budget for acceptance testing – technical screening of components entering into SDLC.
Tier 3 –	1) Discrepancy in system functions	1) Initiate engineering change.
Operation	not meeting requirements, resulting in substantial impact to performance	Malicious alteration can happen throughout the system life cycle to an agency system to address functional discrepancy and test correction for performance

		Vulnerability Types	Mitigation Types
			impact.
4			
	The princip	al vulnerabilities to identify are:	
	• Ac	cess paths within the supply chain that would	allow malicious actors to gain
	inte	ormation about the system and ultimately inti	oduce components that could cause the
	sys	tem to fall at some later time (components	here include hardware, software, and
		nware),	to trigger a component malfunction or
	fail	ure during system operations and	to trigger a component martinetion of
	• De	pendencies on supporting or associated com	onents that might be more accessible or
	eas	ier for malicious actors to subvert than comp	onents that directly perform critical
	fun	ctions.	
	Factors to c	consider include the ease or difficulty of succ	essfully attacking through a vulnerability
	and the abil	lity to detect access used to introduce or trigg	er a vulnerability. The objective is to
	assess the n	the effect of the vulnerability, which will be c	ombined with threat information to
	determine t	he likelihood of successful attacks in the risk	assessment process.
	RISK DET	ERMINATION	
	TASK 2-2:	Determine the risk to organizational operational	ons and assets, individuals, other
	organizatio	ns, and the Nation if identified threats exploi	t identified vulnerabilities.
	Supplamar	ntal Cuidanca	
	Supplemen	ital Guidance	
	Organizatio	ons determine ICT supply chain risk by consi	dering the likelihood that known threats
	exploit kno	wn vulnerabilities to and through the ICT su	only chain and the resulting consequences
	or adverse i	impacts (i.e., magnitude of harm) if such exp	loitations occur. Organizations use threat
	and vulnera	ability information together with likelihood a	nd consequences/impact information to
	determine I	CT SCRM risk either qualitatively or quantit	atively.
	Likelihood		
	Likelihood	is the probability that an exploit occurrence	may result in the loss of mission
	capability.	Determining the likelihood requires the const the identified such architities, and the architic	deration of the characteristics of the
	threat source	es, the identified vulnerabilities, and the organization prior to and with the sefection of which the sefection of the prior of the sefection	anizations susceptibility to the ICT supply
	chain comp	formise, prior to and with the saleguards/miti	gations implemented. This analysis
	Should cons	sider the degree of an adversary's intent to in	are an and to validate the aviateneo of
	ror exampl	e, now much time or money would the adver	sary spend to varidate the existence of
	and leverag	e the vulnerability to attack a system? ICT s	uppry chain risk assessment should
	consider tw	o views:	
	• Th	e likelihood that the ICT supply shain itself i	compromised This may impact for
		mple the availability of quality components	or increase the risk of IP theft and
	• The	e likelihood that the system or component wi	thin the supply chain may be
		nromised for example if malicious code is	inserted into a system or an electric storm
	dar	nages a component	inserved into a system of an electric storin
	uai	nuges a component.	

1540 In some cases, these two views may overlap or be indistinguishable, but both may have an impact 1541 on the agency's ability to perform its mission.

1542

1544 1545

1546

1547

1548

1549

1550

1551

1552

1553

1554

1555

1543 Likelihood determination should consider:

- Threat assumptions that articulate the types of threats that the system or the component may be subject to, such as cybersecurity threats, natural disasters, or physical security threats;
- Actual supply chain threat information such as adversaries' capabilities, tools, intentions, and targets;
 - Exposure of components to external access;
 - Identified system, process, or component vulnerabilities; and
 - Empirical data on weaknesses and vulnerabilities available from any completed analysis (e.g., system analysis, process analysis) to determine probabilities of ICT supply chain threat occurrence.

1556 The likelihood can be based on threat assumptions or actual threat data, such as previous breaches 1557 of the supply chain, specific adversary capability, historical breach trends, or frequency of 1558 breaches. The organization may use empirical data and statistical analysis to determine specific 1559 probabilities of breach occurrence, depending on the type of data available and accessible within 1560 the federal agency and from supporting organizations.

- 1561 1562 *Impact*
- 1563

1564 Organizations should begin impact analysis with the potential impacts identified during the Frame 1565 Step, determining the *impact* of a compromise and then the impact of mitigating that compromise. 1566 Organizations need to identify the various adverse impacts of compromise, including: (i) the 1567 characteristics of the threat sources that could initiate the events; (ii) identified vulnerabilities; 1568 and (iii) the organizational susceptibility to such events based on planned or implemented 1569 countermeasures. Impact analysis is an iterative process performed initially when a compromise 1570 occurs, when mitigation approach is decided to evaluate the impact of change, and finally, in the 1571 ever-changing SDLC, when the situation/context of the system or environment changes. 1572

Organizations should use the result of impact analysis to define an acceptable level of ICT supply chain risk for a given system. Impact is derived from criticality, threat, and vulnerability analyses results, and should be based on the likelihood of exploit occurrence. Impact is likely to be a qualitative measure requiring analytic judgment. Executive/decision makers use impact as an input into the risk-based decisions whether to accept, avoid, mitigate, share, or transfer the resulting risks and the consequences of such decisions.

1579

Organizations should document the overall results of ICT supply chain risk assessments in risk
 assessment reports.¹⁷ ICT supply chain risk assessment reports should cover risks in all three

¹⁷ See NIST SP 800-30, Appendix K, for a description of risk assessment reports.

- 1582 organizational tiers as applicable. Based on the organizational structure and size, multiple ICT
- supply chain risk assessment reports may be required. Agencies are encouraged to develop
- 1584 individual reports at Tier 1. For Tier 2, agencies may want to integrate ICT supply chain risks
- 1585 into the respective mission-level Business Impact Assessments (BIA) or develop separate
- 1586 mission-level ICT supply chain risk assessment reports. For Tier 3, agencies may want to 1587 integrate ICT supply chain risks into the respective System Risk assessment reports or develop
- separate system-level ICT supply chain risk assessment reports. The ICT supply chain risk
 assessment report applies only to High Criticality systems per FIPS 199. Organizations may
 decide to develop ICT supply chain risk assessment reports for Moderate Criticality systems per
 FIPS 199.
- 1591 1592

1593 ICT supply chain risk assessment reports at all three tiers should be interconnected, reference1594 each other when appropriate, and integrated into the ICT SCRM Plans.

1595

1599

1600

1601

1602

1603 1604

1605

1606

1607

1608

1596 Outputs and Post Conditions

- 1597 This step results in: 1598
 - Confirmed mission function criticality;
 - Establishment of relationships between the critical aspects of the system's ICT supply chain infrastructure (e.g., SDLC) and applicable threats and vulnerabilities;
 - Understanding of the likelihood and the impact of a potential ICT supply chain compromise;
 - Understanding of mission and system-specific risks;
 - Documented ICT supply chain risk assessments for mission functions and individual systems; and
 - Integration of relevant ICT supply chain risk assessment results into the organization risk management process.
- 1609

1610 **2.2.3 RESPOND**

1611 Inputs and Preconditions

1612

1613 *Respond* is the step in which the individuals conducting risk assessment will communicate the 1614 assessment results, proposed mitigation/controls options, and the corresponding acceptable level 1615 of risk for each proposed option to the decision makers. This information should be presented in a 1616 manner appropriate to inform and guide risk-based decisions. This will allow decision makers to 1617 finalize appropriate risk response based on the set of options along with the corresponding risk 1618 factors for choosing the various options. Sometimes an appropriate response is to do nothing and 1619 to monitor the adversary's activities and behavior to better understand the tactics and to attribute 1620 the activities.

- 1621
- ICT supply chain risk response should be integrated into the overall organization risk response.
 Figure 2-7 depicts the Respond Step with its inputs and outputs along the three organizational
 tiers.
- 1624 ti 1625
- 1625



Figure 2-7: ICT SCRM in the Respond Step

1630 Figure 2-7 depicts inputs, activities, and outputs of the Respond Step distributed along the three 1631 organizational tiers. The large arrows on the left and right sides of the activities depict the inputs 1632 from the other steps of the Risk Management Process, with the arrow on the left depicting that the 1633 steps are in constant interaction. Inputs into the Respond Step include inputs from other steps. 1634 Outputs of the Respond Steps serve as inputs into the other steps, as well as inputs into the overall 1635 organization Risk Management Program at all three tiers. Up-down arrows between the tiers 1636 depict flow of information and guidance from the upper tiers to the lower tiers and the flow of 1637 information and feedback from the lower tiers to the upper tiers. Together the arrows indicate that 1638 the inputs, activities, and outputs are continuously interacting and influencing one another. 1639

- 1640
- 1641 Activities
- 1642 RISK RESPONSE IDENTIFICATION

```
1643
```

- 1644 TASK 3-1: Identify alternative courses of action to respond to risk determined during the risk1645 assessment.
- 1646
- 1647 Organizations should select ICT SCRM controls and tailor these controls based on the risk
- determination. ICT SCRM controls should be selected for all three organizational tiers, as
- appropriate per findings of the risk assessments for each of the tiers.
- 1650

- 1651 This process should begin with determining acceptable risk to support the evaluation of
- 1652 alternatives (also known as trade-off analysis).
- 1653
- 1654 EVALUATION OF ALTERNATIVES
- 1655 **TASK 3-2:** Evaluate alternative courses of action for responding to risk.
- 1656

1657 Once an initial acceptable level of risk has been defined and options identified, these options 1658 should be identified and evaluated for achieving this level of risk by selecting mitigations from 1659 ICT SCRM controls and tailoring them to the organization's context. Chapter 3 provides risk 1660 mitigations and more information on how to select and tailor them.

1661

1662 This step involves conducting analysis of alternatives to select the proposed options for ICT 1663 SCRM mitigations/controls to be applied throughout the organization.

1664

1665 To tailor a set of ICT SCRM controls, the organization should perform ICT SCRM and mission-1666 level trade-off analysis to achieve appropriate balance among ICT SCRM and functionality needs 1667 of the organization. This analysis will result in a set of cost-effective ICT SCRM controls that is 1668 dynamically updated to ensure that mission-related considerations trigger updates to ICT SCRM 1669 controls.

1670

1671 During this evaluation, applicable requirements and constraints are reviewed with the 1672 stakeholders to ensure that ICT SCRM controls appropriately balance ICT SCRM and the broader 1673 organizational requirements, such as cost, schedule, performance, policy, and compliance.

1674

1675 ICT SCRM controls will vary depending on where they are applied within organizational tiers 1676 and SDLC processes. For example, ICT SCRM controls may range from using a blind buying 1677 strategy to obscure end use of a critical component, to design attributes (e.g., input validation, 1678 sandboxes, and anti-tamper design). For each implemented control, the organization should 1679 identify someone responsible for its execution and develop a time- or event-phased plan for 1680 implementation throughout the SDLC. Multiple controls may address a wide range of possible 1681 risks. Therefore, understanding how the controls impact the overall risk is critical and must be 1682 considered before choosing and tailoring the combination of controls as yet another trade-off 1683 analysis may be needed before the controls can be finalized. The federal agency may be trading 1684 one risk for a larger risk unknowingly if the dependencies between the proposed controls and the 1685 overall risk are not understood and addressed. 1686

1687 RISK RESPONSE DECISION

1688 **TASK 3-3:** Decide on the appropriate course of action for responding to risk.

1689 As described in NIST SP 800-39, organizations should finalize identified and tailored ICT SCRM 1690 controls, based on the evaluation of alternatives and an overall understanding of threats, risks, and 1691 supply chain priorities.

1692

1693 Risk response decisions may be made by a risk executive or be delegated by the risk executive to 1694 someone else in the organization. While the decision can be delegated to Tier 2 or Tier 3, the 1695 significance and the reach of the impact should determine the tier where the decision is being 1696 made. Risk response decisions may be made in collaboration with federal agency risk executives, 1697 mission owners, and system owners, as appropriate.

1698

1699 The resulting decision, along with the selected and tailored controls should be documented in an

1700 ICT SCRM Plan. While the ICT SCRM Plan should ideally be developed proactively, it may also

1701	be developed in response to an ICT supply chain compromise. Ultimately, the ICT SCRM Plan		
1702	should document an ICT SCRM baseline and identify ICT supply chain requirements and		
1703	controls for Tiers 1, 2, and 3. The ICT SCRM Plan should be revised and updated based on the		
1704	output of ICT supply chain monitoring.		
1705			
1706	The ICT SCRM Plan should cover activities in all three organizational tiers as applicable. Based		
1707	on the organizational structure and size, multiple ICT SCRM plans may be required. Agencies are		
1708	encouraged to develop individual plans at Tiers 1 and 2. For Tier 3, agencies may want to		
1709	integrate ICT SCRM controls into the respective System Security Plans or develop separate		
1710	system-level ICT SCRM Plans. At Tier 3, ICT SCRM Plan applies only to High Criticality		
1711	systems per FIPS 199. Organizations may decide to develop an ICT SCRM Plan for Moderate		
1712	Criticality systems per FIPS 199.		
1713			
1714	ICT SCRM Plans at all three tiers should be interconnected and reference each other when		
1715	appropriate.		
1716			
1717	At each Tier, the plan should:		
1718			
1719	• Summarize the environment as determined in Frame such as applicable policies		
1720	processes and procedures based on organization and mission requirements currently		
1721	implemented in the organization.		
1722	• State the role responsible for the plan such as Risk Executive CEO CIO Program		
1723	Manager System Owner		
1724	 Identify key contributors such as CEO_COO_Acquisition/Contracting_System Engineer 		
1724	System Security Engineer, Developer/Maintenance Engineer, Operations Manager		
1725	System Architect:		
1720	 Drovide applicable (per tier) set of controls resulting from the Analysis of Alternatives (in 		
1727	• Flowlde applicable (per tier) set of controls resulting from the Analysis of Alternatives (in Despond):		
1720	 Dravida tailoring decision for selected controls including the rationals for the decision: 		
1720	 Frovide tailoring decision for selected controls including the fationale for the decision, Describe feedback messages among the tigra to anyong ICT symply shoir 		
1721	• Describe reedback processes among the tiers to ensure ICT suppry chain		
1/31	D C C C C C C C C C C C C C C C C C C C		
1/32	• Define frequency for deciding whether the plan needs to be revised; and		
1/33	• Include criteria that would trigger revision.		
1/34			
1/35	Table 2-7 summarizes the controls to be contained in the ICT SCRM Plans at Tiers 1, 2, and 3		
1/30	and provides examples of those controls.		
1/3/			
1/38			
1/39			
1/40			
1741			
1/42			
1743			
1744			
1745			
1/46			
1747			
1748			
1749	Table 2-7: ICT SCRM Plan Controls at Tiers 1, 2, and 3		

Tier	Controls	Examples
Tier 1	 Provides organization common controls baseline to Tiers 2 and 3 	 Minimum sets of controls applicable to all ICT suppliers Organization-level controls applied to processing and storing supplier information ICT supply chain training and awareness for acquirer staff at the organization level
Tier 2	 Inherits common controls from Tier 1 Provides mission function-level common controls baseline to Tier 3 Provides feedback to Tier 1 about what is working and what needs to be changed 	 Minimum sets of controls applicable to ICT suppliers for the specific mission function Program-level refinement of Identity and Access Management controls to address ICT SCRM concerns Program-specific ICT supply chain training and awareness
Tier 3	 Inherits common controls from Tiers 1 and 2 Provides system- specific controls for Tier 3 Provides feedback to Tier 2 and Tier 1 about what is working and what needs to be changed 	 Minimum sets of controls applicable to specific hardware and software for the individual system Appropriately rigorous acceptance criteria for change management for systems that support ICT supply chain, e.g., as testing or integrated development environments System-specific ICT supply chain training and awareness Intersections with the SDLC

1756

1752 Appendix H provides an ICT SCRM Plan Template.

17531754 RISK RESPONSE IMPLEMENTATION

1755 **TASK 3-4:** Implement the course of action selected to respond to risk.

Organizations should implement the ICT SCRM Plan in a manner that integrates the ICT SCRM
controls into the overall agency risk management processes.

1760 Outputs and Post Conditions

1761
1762 The output of this step is a set of ICT SCRM controls that address ICT SCRM requirements and can be incorporated into the system requirements baseline. These requirements and resulting
1764 controls will be incorporated into the SDLC and other organizational processes, throughout the
1765 three tiers.

1767 This step results in:

- Selected, evaluated, and tailored ICT SCRM controls that address identified risks;
- Identified consequences of accepting or not accepting the proposed mitigations; and
- Development and implementation of the ICT SCRM Plan.
- 1770 1771

1768

1772 2.2.4 MONITOR

1773 **Inputs and Preconditions**

1774

1775 Monitor is the step in which the project/program is routinely evaluated to maintain or adjust the 1776 acceptable level of risk. Changes to the organization, mission/business, operations, or the supply 1777 chain can directly impact an individual project/program and the organization's ICT supply chain 1778 processes. The monitor step provides a mechanism for tracking such changes and ensuring that 1779 they are appropriately assessed for impact (in Assess). Organizations should integrate ICT SCRM into existing continuous monitoring programs.¹⁸ In case a Continuous Monitoring program does 1780 1781 not exist, ICT SCRM can serve as a catalyst for establishment of a more comprehensive 1782 continuous monitoring program. Figure 2-8 depicts the Monitor Step with its inputs and outputs 1783 along the three organizational tiers.

1784

1785



¹⁸ NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, describes how to establish and implement a continuous monitoring program.

1787 1788	Figure 2-8: ICT SCRM in the Assess Step
1789 1790 1791 1792 1793 1794 1795 1796 1797 1798 1799	Similarly to Figures 2-5, 2-6, and 2-7, Figure 2-8 depicts inputs, activities, and outputs of the Monitor Step distributed along the three organizational tiers. The large arrows on the left and right sides of the activities depict the inputs from the other steps of the risk management process, with the arrow on the left depicting that the steps are in constant interaction. Inputs into the Monitor Step include inputs from other steps, as well as from the organization Continuous Monitoring program and activities. Up-down arrows between the tiers depict flow of information and guidance from the upper tiers to the lower tiers and the flow of information and feedback from the lower tiers to the upper tiers. Together the arrows indicate that the inputs, activities, and outputs are continuously interacting and influencing one another.
1800	Activities
1801	RISK MONITORING STRATEGY
1802 1803	TASK 4-1: Develop a risk monitoring strategy for the organization that includes the purpose, type, and frequency of monitoring activities.
1804 1805 1806	Supplemental Guidance:
1807 1808 1809 1810 1811 1812 1813 1814	Organizations should integrate ICT SCRM considerations into their overall risk monitoring strategy. Because some of the information will be gathered from outside of the agency – from open sources, suppliers and integrators, monitoring ICT supply chain risk may require information that agencies have not traditionally collected. The strategy should, among other things, include the data to be collected, state the specific measures that will be compiled from the data, identify existing or required tools to collect the data, identify how the data will be protected, and define reporting formats for the data. Potential data sources may include:
1814 1815 1816 1817 1818 1819 1820 1821 1822	 Agency vulnerability management and incident management activities; Agency manual reviews Interagency information sharing; Information sharing between the agency and system integrator or external service provider; Supplier information sharing; and Contractual reviews of system integrator or external service provider.
1823 1824 1825 1826 1827	Organizations should ensure appropriate protection of supplier data if that data is collected and stored by the agency. Agencies may also require additional data collection and analysis tools to appropriately evaluate the data to achieve the objective of monitoring applicable ICT supply chain risks.
1828	KIŞK MONTLOKING
1829 1830 1831 1832 1833	TASK 4-2: Monitor organizational information systems and environments of operation on an ongoing basis to verify compliance, determine effectiveness of risk response measures, and identify changes.
1834 1835	According to NIST SP 800-39, organizations should monitor compliance, effectiveness, and change. Monitoring compliance within the context of ICT SCRM involves monitoring federal

agency processes and ICT products and services for compliance with the established security and
ICT SCRM requirements. Monitoring effectiveness involves monitoring the resulting risks to
determine whether these established security and ICT SCRM requirements produce the intended
results. Monitoring change involves monitoring the environment for any changes that would
require changing requirements and mitigations/controls to maintain an acceptable level of ICT
supply chain risk.

1842

1843 To monitor changes, organizations need to identify and document the set of triggers that would 1844 change ICT supply chain risk. While the categories of triggers will likely include changes to 1845 constraints, identified in Table 2-6 (during the Frame Step), such as policy, mission, change to the 1846 threat environment, enterprise architecture, SDLC, or requirements, the specific triggers within 1847 those categories may be substantially different for different organizations.

1848

1849 An example of the ICT supply chain infrastructure change is two key vetted suppliers¹⁹ 1850 announcing their departure from a specific market, therefore creating a supply shortage for 1851 specific components. This would trigger the need to evaluate whether reducing the number of 1852 suppliers would create vulnerabilities in component availability and integrity. In this scenario, 1853 potential deficit of components may result simply from insufficient supply of components. 1854 because fewer components are available. If none of the remaining suppliers are vetted, this deficit 1855 may result in uncertain integrity of the remaining components. If the organizational policy directs 1856 use of vetted components, this event may result in the organization's inability to fulfill its mission 1857 needs. 1858

In addition to regularly updating existing risks assessments with the results of the ongoing
monitoring, the organization should determine what would trigger a reassessment. Some of these
triggers may include availability of resources, changes to ICT supply chain risk, natural disasters,
or mission collapse.

1863

1864 *Outputs and Post Conditions*

1865

Organizations should integrate the ICT supply chain outputs of the Monitor Step into the ICT
 SCRM Plan. This plan will provide inputs into iterative implementations of the Frame, Assess,
 and Respond Steps as required.

- 1869
- 1870

¹⁹ A vetted supplier is a supplier with whom the organization is comfortable doing business. This level of comfort is usually achieved through developing an organization-defined set of supply chain criteria and then *vetting* suppliers against those criteria.

1871 CHAPTER THREE

1872 ICT SCRM CONTROLS

1873

1874 During the Respond Step of the risk management process discussed in Section 2.2.3. 1875 organizations select, tailor, and implement controls for mitigating ICT supply chain risk. 1876 Appendix E of NIST 800-53 Revision 4 lists a set of information security controls at the FIPS 1877 high-, moderate-, and low-impact levels. This chapter uses those controls as a basis for describing 1878 controls that help mitigate risks both to high-impact information systems and components and the 1879 ICT supply chain infrastructure. This chapter provides 19 ICT SCRM control families that 1880 include relevant ICT controls and supplemental guidance. The process that was used to identify and refine ICT SCRM-related controls from NIST SP 800-53 Revision 4, add new controls to 1881 1882 address specific ICT SCRM concerns, and offer ICT SCRM-specific supplemental guidance 1883 where appropriate, is illustrated in Figure 3-1 (which repeats Figure 1-5) and includes the 1884 following:. 1885

- Individual controls and enhancements from NIST SP 800-53 Revision 4 were selected that were relevant and especially applicable to ICT SCRM and were extracted;
 - These controls were then analyzed to determine how they apply to ICT SCRM;
 - Additional supplemental guidance was developed and included for each control and control enhancement;
 - The resulting set of controls and enhancements were then evaluated to determine whether all ICT SCRM concerns were addressed;
 - Additional controls currently not defined in NIST SP 800-54 Revision 4 were developed;
 - Applicable tiers were assigned to each ICT SCRM control; and
 - ICT SCRM-specific supplemental guidance was defined for each ICT SCRM control.

1895 1896 1807

1886

1887

1888

1889

1890

1891

1892

1893

1894

1897 It should be noted that NIST SP 800-53 Revision 4 provides some ICT SCRM-related controls.
1898 These controls may be listed in this publication with a summary or additional guidance and a
1899 reference back to original NIST SP 800-53 Rev 4 control and supplemental guidance detail.
1900



1908 Federal agencies should be aware that implementing these controls will require financial and

1909 human resources. Furthermore, any requirements for system integrators, suppliers, or external

1910 service providers that result from federal agencies implementing these controls may also require

1911 financial and human resources from those system integrators, suppliers, and external service

providers, potentially resulting in increased costs to the acquirers. The acquirers should be

cognizant of the costs and weigh them against the benefits when selecting ICT SCRM controls.
 This challenge of balancing ICT supply chain risks with benefits and costs of mitigating controls

914 This challenge of balancing ICT supply chall risks with benefits and costs of mutgating control 915 should be a key component of the federal agency overall ICT SCPM approach

should be a key component of the federal agency overall ICT SCRM approach.

Managing Cost and Resources

Federal agencies should be aware that implementing these controls will require financial and human resources. Furthermore, any requirements for system integrators, suppliers, or external service providers that result from federal agencies implementing these controls may also require financial and human resources from those system integrators, suppliers, and external service providers, potentially resulting in increased costs to the federal acquirers. The acquirers should be cognizant of the costs and weigh them against the benefits when selecting ICT SCRM controls. This challenge of balancing ICT supply chain risks with benefits and costs of mitigating controls should be a key component of the federal agency overall approach to ICT SCRM.

3.1 ICT SCRM CONTROLS SUMMARY

1934 NIST defines security controls as:

1917 1918

1919 1920

1921

1922

1923

1924

1925

1926

1927

1928

1933

1935 1936

1937

1938 1939 The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.²⁰

1940 NIST SP 800-53 Revision 4 defines a number of ICT supply chain-related controls within the 1941 catalog of information security controls. This chapter is structured as an enhanced overlay of 1942 NIST SP 800-53 Revision 4. It identifies and augments ICT SCRM-related controls with 1943 additional supplemental guidance and provides new controls as appropriate. The ICT SCRM 1944 controls are organized into the eighteen control families of NIST SP 800-53 Revision 4. Also, an 1945 ICT SCRM-specific family, Provenance, was created, resulting in nineteen ICT SCRM control 1946 families. This approach facilitates use of the security controls assessment techniques provided in 1947 800-53A to be used to assess implementation of ICT SCRM controls.

- 1948 1949 The controls provided in this publication are intended for federal agencies to implement 1950 internally. As with NIST SP 800-53Revision 4, the security controls and control enhancements
- are a starting point from which controls/enhancements may be removed, added, or specialized
- based on federal agency needs. Each control in this section is listed for its applicability to ICT

²⁰NIST SP 800-53; 800-37; 800-53A; 800-60; FIPS 200; FIPS 199; CNSSI-4009

SCRM. Those controls from NIST SP 800-53 Revision 4 not listed are not considered directly
applicable, and as such were not included in this publication. Details and supplemental guidance
for the various ICT SCRM controls in this publication are contained in Section 3.4.1. Appendix D
maps the ICT SCRM controls in this publication to their corresponding NIST SP 800-53 Revision
4 controls as appropriate.

1958 1959

1960 **3.2 ICT SCRM CONTROLS THROUGHOUT ORGANIZATIONAL HIERARCHY** 1961

1962 As noted in Table 3-1, ICT SCRM controls in this publication are designated by the three tiers 1963 comprising the organizational hierarchy. This is to facilitate ICT SCRM control selection specific 1964 to organizations, their various missions, and individual systems, as described in Chapter 2 under 1965 Respond Step of the risk management process. During controls selection, organizations should 1966 use the ICT SCRM controls in this chapter to identify appropriate ICT SCRM controls for 1967 tailoring, per risk assessment. By selecting and implementing applicable ICT SCRM controls for 1968 each tier, organizations will ensure that they have appropriately addressed ICT SCRM throughout 1969 their enterprises. 1970

1971 3.3 APPLYING ICT SCRM CONTROLS TO ACQUIRING ICT PRODUCTS AND SERVICES 1973

Acquirers may use ICT SCRM controls to communicate their ICT SCRM requirements to
different types of organizations, described within this publication, that provide ICT products and
services to federal agencies acquirers: system integrators, suppliers, and external service
providers. Acquirers are encouraged to use ICT SCRM Plans for their respective systems and
missions throughout their acquisition activities. More detail on how to use ICT SCRM plan for
acquisition is provided in Appendix H.

1981 It is important to recognize that the controls in this chapter do not provide specific contracting 1982 language. Acquirers should develop their own contracting language using this publication as 1983 guidance to develop specific ICT SCRM requirements to be included in contracts. The sections 1984 below expand upon the system integrator, supplier, and external service provider roles with 1985 respect to ICT SCRM expectations for acquirers.

In this document the word *organization* means *federal department/agency*. In the context of this document, federal department/agency is the *acquirer*.

1986

1980

1987

- 1988
- 1989 1990

0 **3.3.1 System Integrators**

1991 System integrators are those organizations that provide customized services to the federal agency 1992 acquirer including custom development, test, operations, and maintenance. This group usually 1993 replies to a request for proposal from a federal agency acquirer with a proposal that describes 1994 solution or services that are customized to the federal agency acquirer requirements. Such 1995 proposals provided by system integrators can include many layers of suppliers (see 3.3.2). The 1996 system integrator should carry the responsibility for ensuring that those suppliers are vetted and 1997 verified with the respect to federal agency acquirer ICT SCRM requirements. Because of the 1998 level of visibility that can be obtained in the relationship with the system integrator, the federal 1999 agency acquirer has the ability to require rigorous supplier acceptance criteria as well as any 2000 relevant countermeasures to address identified or potential risks.

2002 **3.3.2** Suppliers

2003 Suppliers may provide either commercial off-the-shelf (COTS) or government off-the-shelf 2004 (GOTS) solutions to the federal agency acquirer. COTS solutions include non-developmental 2005 items (NDI), such as commercially licensing solutions/products as well as Open Source Solutions 2006 (OSS). GOTS solutions are government-only license-able solutions. Suppliers are a diverse 2007 group, ranging from very small to large, specialized to diversified, based in a single country to 2008 transnational, and range widely in the level of sophistication, resources, and 2009 transparency/visibility in both process and solution. Suppliers also have diverse levels and types 2010 of ICT SCRM practices in place. These practices and other related practices may provide the 2011 evidence needed for SCRM evaluation. When appropriate, allow suppliers the opportunity to 2012 reuse any existing data and documentation that may provide evidence of ICT SCRM 2013 implementation.

2014

2015 Organizations should consider that the costs of doing business with suppliers may be directly 2016 impacted by the level of visibility the suppliers allow into how they apply security controls to 2017 their solutions. When organizations or system integrators require greater levels of transparency 2018 from suppliers, they must consider the possible cost implications of such requirements. Suppliers 2019 may select to not participate in procurements to avoid increased costs or perceived risks to their 2020 intellectual property, limiting an organization's supply or technology choices. The risk to 2021 suppliers is the potential for multiple, different sets of requirements that they may have to 2022 individually comply with, which is not scalable.

2023

2037

2024 3.3.3 External Providers of Information System Services

2025 Organizations use external IT service providers to manage their mission and business functions.²¹ 2026 The outsourcing of federal IT systems and services creates a set of ICT supply chain concerns 2027 that reduces the acquirer's visibility into, and control of, the outsourced functions. Therefore, it 2028 requires increased rigor from the organizations in defining ICT SCRM requirements, stating them 2029 in procurements, and then monitoring delivered services and evaluating them for compliance with 2030 the stated requirements. Regardless of who performs the services, the acquirer is ultimately 2031 responsible and accountable for the risk to the federal agency's systems and data that may result 2032 from using these services. Organizations should implement a set of compensating ICT SCRM 2033 controls to address this risk and work with the federal agency risk executive to accept this risk. A 2034 variety of methods may be used to communicate and subsequently verify and monitor ICT SCRM 2035 requirements through such vehicles as contracts, interagency agreements, lines of business 2036 arrangements, licensing agreements, and/or supply chain transactions.

3.4 SELECTING AND TAILORING IMPLEMENTING ICT SCRM SECURITY CONTROLS

The ICT SCRM controls defined in this chapter should be selected and tailored according toindividual federal agency needs and environment using the guidance in NIST SP 800-53 Revision

²¹ NIST SP800-53rev 4, Section 2.4, Security Controls in External Environments, page 12.

2043 4, in order to ensure a cost-effective, risk-based approach to providing ICT SCRM organization-2044 wide. The ICT SCRM baseline defined in this publication addresses the basic needs of a broad 2045 and diverse set of constituencies. Organizations must select, tailor, and implement the controls 2046 based on: (i) the environments in which organizational information systems are acquired and 2047 operate: (ii) the nature of operations conducted by organizations; (iii) the types of threats facing 2048 organizations, missions/business processes, supply chains, and information systems; and (iv) the 2049 type of information processed, stored, or transmitted by information systems and the supply chain 2050 infrastructure.

2051

2052 After selecting the initial set of security controls from Chapter 3, the federal agency acquirer 2053 should initiate the tailoring process according to the NIST SP 800-53 Revision 4 to appropriately 2054 modify and more closely align the controls with the specific conditions within the organization. 2055 The tailoring should be coordinated with and approved by the appropriate organizational officials 2056 [e.g., authorizing officials, authorizing official designated representatives, risk executive 2057 (function), chief information officers, or senior information security officers] prior to 2058 implementing the ICT SCRM controls. Additionally, federal agencies have the flexibility to 2059 perform the tailoring process at the organization level (either as the required tailored baseline or 2060 as the starting point for policy, program or system-specific tailoring), in support of a specific program, at the individual information system level, or using a combination of organization-level, 2061 2062 program/mission-level and system-specific approaches. 2063

Selection and tailoring decisions, including the specific rationale for those decisions, should be
 documented in the ICT SCRM Plans for Tiers 1, 2, and 3 and approved by the appropriate
 organizational officials as part of the ICT SCRM Plan approval process.

2067 2068

3.4.1 ICT SCRM Control Format

2069

2076

2077

Table 3-2 shows the format used in this publication for controls which provide supplemental ICT
SCRM guidance on existing NIST SP 800-53 Rev. 4 controls or control enhancements. Each
control is hyperlinked to the appropriate parent control in Appendix E. ICT SCRM controls that
do not have a parent NIST SP 800-53 Rev. 4 control follow the format described in NIST SP 80053 Rev. 4.

Table 3-2: ICT SCRM Control Format

SCRM CONTROL	CONTROL NAME	LINK TO ASSOCIATED NIST SP 800-53 CONTROL
Control	<u>:</u>	
Supple	mental ICT SCRM Guidance:	
<u>TIER:</u>		
<u>Control</u>	Enhancements:	
(1)	CONTROL NAME CONTROL ENHANCEMENT NAME Enhancement Text	LINK TO ASSOCIATED NIST SP 800-53 CONTROL ENHANCEMENT
	Supplemental ICT SCRM Guidance:	

	<u>TIER:</u>			
2078 2079 2080 2081	An example of the ICT SCRM control format is shown below using ICT SCRM control SCRM_AC-3 and SCRM_AC-3(1):			
2082	SCRM_AC-3 ACCESS ENFORCEMENT <u>AC-3</u>			
2083 2084 2085 2086 2087 2088 2089 2090	Supplemental ICT SCRM Guidance: Ensure that the information systems and ICT supply chain infrastructure have appropriate access enforcement mechanisms in place. This includes both physical and logical access enforcement mechanisms that are likely to work in coordination for ICT supply chain needs. Organizations should ensure detailed definition of access enforcement. <u>TIER: 2, 3</u> <u>Control Enhancements:</u>			
2091	(2) ACCESS ENFORCEMENT REVOCATION OF ACCESS AUTHORIZATIONS AC-3 (8)			
2092 2093 2094 2095 2096 2097 2098	<u>Supplemental ICT SCRM Guidance:</u> Prompt revocation is critical for ICT supply chain security to ensure that system integrators, suppliers, and external service providers who no longer require access are not able to access a organization's system. For example, in a "badge flipping" situation, a contract is transferred from one system integrator organization to another with the same personnel supporting the contract. In that situation, the organization should retire the old credentials and issue new credentials.			
2099 2100 2101	<u>TIER: 2,3</u>			
2101	3.4.2 Using ICT SCRM Controls in This Publication			
2103 2104 2105 2106 2107	The remainder of Chapter 3 provides the enhanced ICT SCRM overlay of NIST SP 800-53 Revision 4. Appendix E includes the NIST SP 800-53 Revision 4 controls and enhancements. This chapter displays the relationship between NIST SP 800-53 Revision 4 controls and ICT SCRM controls in one of the following ways:			
2108 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2120 2121 2122 2123	 If a NIST SP 800-53 Revision 4 control or enhancement was determined to be an information security control that serves as a foundational control for ICT SCRM but is not specific to ICT SCRM, it is not included in this publication. If a NIST SP 800-53 Revision 4 control or enhancement was determined to be relevant to ICT SCRM, the number and title of that control or enhancement is included in Chapter 3 with the complete control (unchanged from NIST SP 800-53 Revision 4) provided in Appendix E. The tiers in which the control applies are also provided. If a NIST SP 800-53 Revision 4 enhancement was determined to be relevant to ICT SCRM, but the parent control was not, the parent control number and title is included, but there is no supplemental ICT SCRM guidance, and the parent control text is not included in Appendix E. ICT SCRM controls/enhancements that do not have an associated NIST 800-53 Revision 4 control/enhancement are listed with their titles and the control/enhancement text. All ICT SCRM controls include the tiers in which the control applies and supplemental ICT SCRM guidance as applicable. 			
2124	The following new controls and control enhancement have been added:			

2125	
2126	• The Provenance control family is included in Chapter 3 with a description of the control
2127	family and three associated controls;
2128	• The control SCRM_MA-7 – Maintenance Monitoring and Information Sharing - is added
2129	to the Maintenance control family; and
2130	• The control enhancement SCRM_SA-15(3) – Tamper Resistance and Detection / Return
2131	<i>Policy</i> – is added to the System Acquisition.
2132	
2133	Each control that originated in NIST SP 800-53 Revision 4 contains a link to Appendix E where
2134	the full NIST SP 800-53 Revision 4 control text is provided. Controls in Appendix E contain
2135	links back to the related ICT SCRM control in Section 3.5. This feature is provided to increase
2136	the usability of the publication by having all pertinent material in a single publication.
2137	
2138	

2139 2140	3.3 ICT SCRM SECURITY CONTROLS	
2141 2142 2143	FAMILY: ACCESS CONTROL	
2143 2144 2145	FIPS 200 specifies the Access Control minimum security requirement as follows:	
2146 2147 2148 2149 2150	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	
2150 2151 2152 2153 2154 2155 2156 2157 2158 2159	Systems and components that traverse the ICT supply chain infrastructure are subject to access be a variety of individuals within federal agency, system integrator, supplier, or external service provider organizations. Such access should be defined and managed to ensure that it does not inadvertently result in unauthorized release, modification, or destruction of sensitive federal agency information or sensitive system integrator, supplier, and external service provider information. This access should be limited to only the necessary access for authorized individual and monitored for ICT supply chain impact.	'Y .s
2160	SCRM_AC-1 ACCESS CONTROL POLICY AND PROCEDURES AC	<u>-1</u>
2161 2162 2163 2164 2165 2166	<u>Supplemental ICT SCRM Guidance</u> : Organizations should specify and include in agreements (e.g., contracting language) access control policies for their system integrators, suppliers, and external service providers. These should include both physical and logical access. <u>TIER</u> : 1, 2, 3	
2167	SCRM_AC-2 ACCOUNT MANAGEMENT ACCOUNT MANAGEMENT	<u>-2</u>
2168 2169 2170 2171 2172	<u>Supplemental ICT SCRM Guidance</u> : Use of this control helps in traceability of actions and actors in the supply chain. <u>TIER</u> : 2, 3	
2173	SCRM_AC-3 ACCESS ENFORCEMENT ACC	-3
2174 2175 2176 2177 2178	<u>Supplemental ICT SCRM Guidance</u> : Ensure that the information systems and ICT supply chain infrastructure have appropriate access enforcement mechanisms in place. This includes both physical and logical access enforcement mechanisms, which are likely to work in coordination for ICT supply chain needs. Organizations should ensure detailed definition of access enforcement.	r
2179 2180	<u>TIER</u> : 2, 3	
2181 2182		(0)
2182 2183 2184 2185	Supplemental ICT SCRM Guidance: Prompt revocation is critical for ICT supply chain security t ensure that system integrators, suppliers, and external service providers who no longer requir access are not able to access a federal agency system. For example, in a "badge flipping"	<u>o)</u> 0 :e

2186 2187 2188 2189 2190		situation, a contract is transferred from one system integrator organization to anot same personnel supporting the contract. In that situation, the organization should credentials and issue completely new credentials. <u>TIER</u> : 2, 3	her with the retire the old
2191	(2)	ACCESS ENFORCEMENT / CONTROLLED RELEASE	<u>AC-3 (9)</u>
2192 2193 2194 2195 2196		<u>Supplemental ICT SCRM Guidance:</u> Information about the ICT supply chain should be for release between the organizations. Information is continuously exchanged betw organization and its system integrator, supplier, and external service provider. Co release provides proper information protection to manage risks.	be controlled ween the ntrolled
2197		<u>TIER: 2, 3</u>	
2198	SCRM_AC-4	INFORMATION FLOW ENFORCEMENT	<u>AC-4</u>
2199 2200 2201 2202 2203 2204 2205	Suj inf sta Re and <u>TIE</u>	pplemental ICT SCRM Guidance: Supply chain information may traverse a large ICT su trastructure to a broad set of stakeholders including the organization and its various keholders as well as system integrators, suppliers, and external service providers. quirements of information flow enforcement should ensure that only the required in d not more is communicated to the various participants in the supply chain, <u>iR</u> : 2, 3	apply chain federal aformation
2206 2207	Co	ntrol enhancements:	
2208	(1)	INFORMATION FLOW ENFORCEMENT METADATA	AC-4 (6)
2209 2210 2211 2212 2213 2214 2215 2216		Supplemental ICT SCRM Guidance: In ICT SCRM, information about systems a components, acquisition details, and delivery is considered metadata and should be appropriately protected. Metadata relevant to ICT SCRM is quite extensive and in activities within the SDLC. Organizations should identify which metadata is direct to their ICT supply chain security and ensure that control information flow enforce implemented in order to protect the metadata.	and system be includes of the relevant beement is
2217	(2)	INFORMATION FLOW ENFORCEMENT DOMAIN AUTHENTICATION	AC-4 (17)
2218 2219 2220 2221 2222 2223	()	<u>Supplemental ICT SCRM Guidance</u> : Within the ICT SCRM context, organizations sho various source and destination points for information about ICT supply chain and that flows through the supply chain. This is so that organizations have visibility in physical and logical origins of systems and components that they use. <u>TIER</u> : 2, 3	ould specify information nto the
2224	(3)	INFORMATION FLOW ENFORCEMENT / VALIDATION OF METADATA	<u>AC-4 (19)</u>
2225 2226 2227 2228 2229 2230		<u>Supplemental ICT SCRM Guidance</u> : For ICT SCRM, data and the relationship to its in the validation of it become critical. Much of the data transmitted through the ICT chain infrastructure is validated with the verification of the metadata that is bound Ensuring that proper filtering and inspection is put in place for validation before a payloads into the ICT supply chain infrastructure.	netadata and supply l to it. lllowing
2231		<u>11ER: 2, 3</u>	
2232 2233	(4)	INFORMATION FLOW ENFORCEMENT PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS	<u>AC-4 (21)</u>

2234 2235 2236 2237 2238 2239 2240 2241 2242 2243 2244 2245 2244	Supplemental ICT SCRM Guidance: The organization should ensure the separation of the information system and ICT supply chain infrastructure information flow. Various mechanisms can be implemented including, for example, encryption methods (e.g., digita signing) for protecting of information as well as the management of flow control of the information where feasible. Flow control within the organizations operations may be manageable. However, addressing information flow between the organization and its syst integrator, external service provider, and even supplier is likely more challenging, especia when leveraging public networks. Organizations should ensure that, at a minimum, protect measures are implemented for any appropriate data (e.g., component data and any related metadata). <u>TIER</u> : 3	l em ully xion
2247	SCRM_AC-5 SEPERATION OF DUTIES	<u>AC-5</u>
2248 2249 2250 2251 2252 2253 2254 2255 2256	<u>Supplemental ICT SCRM Guidance</u> : The organization should ensure that appropriate separation of duties is established for decisions requiring the acquisition of both information system and IC supply chain infrastructure components. Separation of duties helps to ensure that adequate protections are in place for components entering organizations supply chain. Examples include separating technical decision makers from the procurement personnel for deciding on compon in the supply chain, or having two engineers review and test component samples from multiple suppliers to ensure availability of multiple supply and standards-based standards to verify abil for components to be interchanged or replaced.	Γ ents e ity
2257	<u>TIER: 2, 3</u>	
2258	SCRM_AC-6 LEAST PRIVILEGE	<u>AC-6</u>
2259	Supplemental ICT SCRM Guidance: Supplemental guidance provided in control enhancement.	
2260	(1) LEAST PRIVILEGE PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS	<u>]-6 (</u> 6)
2261 2262 2263 2264 2265 2266 2267 2268 2269 2270 2271 2272	<u>Supplemental ICT SCRM Guidance</u> : Organizations should ensure that protections are in place prevent non-organizational users from having privileged access to organizational ICT sup chain infrastructure and related supply chain information. When organizational users may include independent consultants, system integrators, suppliers, and external services providers, relevant access requirements may need to be more precisely defined regarding which information and or components are accessible, for what duration, at which frequen- using which access methods, and by whom, using least privilege mechanisms. Understand which components are critical and noncritical can aid in understanding the level of detail may need to be defined regarding least privilege access for non-organizational users. TIER: 2.3	e to ply cy, ling that
2273	SCRM_AC-7 REMOTE ACCESS	<u>AC-17</u>
2274 2275 2276 2277 2278 2279 2280 2281 2282 2283	<u>Supplemental ICT SCRM Guidance</u> : With the push toward distributed approaches to accessing ICT supply chain infrastructures, whether for development, maintenance, or operations, organization should implement secure remote access mechanisms and allow remote access only to vetted personnel. Remote access to an organization's distributed software development environments access to the ICT supply chain infrastructure should be limited to the organization or system integrator personnel as required to perform their tasks. Ensure that appropriate levels of remot access requirements are properly defined (including agreements between organization and its system integrators).	Γ ons and e

2284 2285 2286 2287	<u>TIER</u> : 2 <u>Control e</u>	enhancements:	
2288	(1) REI	MOTE ACCESS / PROTECTION OF INFORMATION	<u>AC-17 (6)</u>
2289 2290 2291 2292 2293 2294 2295 2296 2297	Sup pro cha dat mis inf En	pplemental ICT SCRM Guidance: Organizations should ensure that detailed requirements operly defined and access to information regarding the information system and IC ain infrastructure is protected from unauthorized use and disclosure. Since supply ta and metadata disclosure or access can have significant implications to an organi ssion processes, appropriate measures must be taken to vet both the ICT supply cl rastructure and personnel processes to ensure that adequate protections are impler issure that remote access to such information is included in requirements. ER: 2, 3	ents are T supply v chain ization's hain mented.
2298	SCRM AC-8	WIRELESS ACCESS	AC-18
2299 2300 2301 2302 2303 2304 2305 2306 2307 2308 2309 2310	Serial_reso Supplem wireless Device such IC within t Ensurin enables metada wireless appropi	<u>hental ICT SCRM Guidance</u> : An organization's ICT supply chain infrastructure may is s infrastructure that supports supply chain logistics (e.g., Radio Frequency Identif [RFID] support, software call home features). Supply chain systems/components CT supply chain infrastructures as they are moved from one location to another wh the organizations own environment or during delivery from system integrators or ng appropriate access mechanisms are in place within this ICT supply chain infras s the protection of the information systems and components, and logistics technolo ta within tracking sensors during shipping. Acquirers should explicitly define app s access control mechanisms for ICT supply chain infrastructure in policy and imp riate mechanisms.	include ication traverse tether suppliers. tructure ogies and oropriate plement
2311	SCRM_AC-9	ACCESS CONTROL FOR MOBILE DEVICES	<u>AC-19</u>
2312 2313 2314 2315 2316 2317 2318 2319 2320	Supplem infrastr systems infrastr relevan implem units in and me	nental ICT SCRM Guidance: Use of mobile devices has become common in ICT supp ucture. They are used as mechanisms for tracking supply chain logistics data as in s and components traverse organization or systems integrator ICT supply chain ucture. Ensure that access control mechanisms are clearly defined and implement it when managing organizations ICT supply chain components. An example of suc nentation includes access control mechanisms implemented for use with remote ha RFID for tracking components traversing the supply chain as well as any associa stadata.	oly chain formation ed where ch an andheld ited data
2322	<u>IIER. 2</u> SCRM_AC-10	USE OF EXTERNAL INFORMATION SYSTEMS	AC-20
2323 2324 2325 2326 2327 2328 2329 2330 2331 2332	Supplem system organiz relation agreem <u>TIER</u> : 1 <u>Control e</u>	<u>nental ICT SCRM Guidance</u> : Organizations' external information systems include the integrators, suppliers, and external service providers. Unlike in federal agency's i zations where direct and continuous monitoring is possible, in the external supplier iship, information may be shared on an as-needed basis and should be articulated inent. Access from such external information systems should be monitored and aud , 2, 3 <u>enhancements:</u>	ose of nternal r in an lited.

2333	(1)	USE OF EXTERNAL INFORMATION SYSTEMS / LIMITS ON AUTHORIZED USE	<u>AC-20 (1)</u>
2334 2335 2226	<u>s</u>	Supplemental ICT SCRM Guidance: This enhancement helps limit exposure to syst suppliers, and external service provider systems.	em integrators,
2330	-	<u>TIER: 2, 3</u>	
2338 2339	(2)	USE OF EXTERNAL INFORMATION SYSTEMS NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES	<u>AC-20 (3)</u>
2340 2341	<u>9</u>	Supplemental ICT SCRM Guidance: Devices that do not belong to the organization organization's exposure to ICT supply chain risks.	increase the
2342 2343	-	<u>TIER</u> : 2, 3	
2344 2345 2346	SCRM_AC-11	COLLABORATION AND INFORMATION SHARING	<u>AC-21</u>
2347 2348 2349 2350 2351 2352 2353 2354 2355 2356 2357	Suppl ICT s and c mana organ shari requi infor syste	lemental ICT SCRM Guidance: Sharing information within the ICT supply chain h supply chain risks. This information may include vulnerabilities, threats, critica components, or delivery information. However, this information sharing should aged to ensure that the information is accessible only to authorized individuals nization's ICT supply chain. Organizations should clearly define boundaries fo ng with respect to temporal, informational, contractual, security, access, syster irements. Organizations should monitor and review for unintentional or intention mation sharing within its ITC supply chain activities including information share mintegrators, suppliers, and external service providers.	elps to manage ality of systems l be carefully within the r information n, and other onal uring with
2357	SCPM AC-12	PURI ICI V ACCESSIRI E CONTENT	AC 22
2550	SCRM_AC-12	FUBLICLT ACCESSIBLE CONTENT	<u>AC-22</u>
2359	Suppl	lemental ICT SCRM Guidance: Within the ICT SCRM context, publicly accessible	e content may
2360	inclu	de Requests for Information, Requests for Proposal, or information about deliv	very of systems
2361	and c	components. This information should be reviewed to ensure that only appropria	ate content is
2362	relea	sed for public consumption, alone or in aggregation with other information.	
2363			
2364	<u>TIER</u> :	: 2, 3	
2365	SCRM_AC-13	ACCESS CONTROL DECISIONS	<u>AC-24</u>
2366	Suppl	lemental ICT SCRM Guidance: Organizations should assign access control decisio	ns to support
2367	autho	prized accesses to the ICT supply chain infrastructure. Ensure that if a system i	ntegrator or
2368	exter	rnal service provider is used, there is consistency in access control decision reg	uirements and
2369	how	the requirements are implemented to deliver consistency in support of the orga	nizations
2370	supp	ly chain needs. This may require defining such requirements in service-level as	greements in
2371	many	y cases as part of the upfront relationship established between organization and	system
2372	integ	rator or organization and external service provider.	-
2373 2374 2275	<u>TIER</u> :	: 1, 2, 3	
2313			

2376 FAMILY: AWARENESS AND TRAINING

2377

2378 FIPS 200 specifies the Awareness and Training minimum security requirement as follows: 2379 2380 Organizations must: (i) ensure that managers and users of organizational information 2381 systems are made aware of the security risks associated with their activities and of the 2382 applicable laws, Executive Orders, directives, policies, standards, instructions, 2383 regulations, or procedures related to the security of organizational information 2384 systems; and (ii) ensure that organizational personnel are adequately trained to carry 2385 out their assigned information security-related duties and responsibilities. 2386 2387 NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems 2388 and Organizations, expands the Awareness and Training control of FIPS 200 to include ICT 2389 SCRM. Making the workforce aware of ICT SCRM concerns is key to a successful ICT SCRM 2390 strategy. ICT SCRM awareness and training provides understanding of the problem space and of 2391 the appropriate processes and controls that can help mitigate ICT supply chain risk. Federal 2392 agencies should provide ICT SCRM awareness and training to individuals at all levels within the 2393 organization including, for example, risk executive function, acquisition and contracting 2394 professionals, program managers, supply chain and logistics professionals, shipping and receiving 2395 staff, information technology professionals, quality professionals, mission and business owners, 2396 system owners, and information security engineers. Organizations should also work with system 2397 integrators and external service providers to ensure that their personnel that interact with federal 2398 agency ICT supply chains receive appropriate ICT SCRM awareness and training, as appropriate. 2399 2400 SCRM_AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES **AT-1** 2401 Supplemental ICT SCRM Guidance: Organizations should integrate ICT supply chain risk 2402 management training and awareness policy into the security training and awareness policy. The 2403 ICT SCRM training should target both the organization and its system integrators. The policy 2404 should ensure that ICT supply chain role-based training is required for those individuals who 2405 touch or impact the ICT supply chain and its security, such as system owner, acquisition, supply 2406 chain logistics, system engineering, program management, IT, quality, and incident response. 2407 2408 ICT SCRM training procedures should address: 2409 а Roles throughout the supply chain and system/element life cycle to limit opportunities 2410 and means available to individuals performing these roles that could result in adverse 2411 consequences; 2412 b. Requirements for interaction between an organization's personnel and individuals not 2413 employed by the organization that participate in the ICT supply chain throughout the 2414 SDLC; and 2415 Incorporating feedback and lessons learned from ICT SCRM activities into the ICT c. 2416 SCRM training. 2417 2418 TIER: 1, 2 2419 SCRM AT-2 **ROLE-BASED SECURITY TRAINING** 2420 Control enhancements: 2421 2422 (1) SECURITY TRAINING / PHYSICAL SECURITY CONTROLS AT-3 (2)

2423 Supplemental ICT SCRM Guidance: ICT SCRM is impacted by a number of physical security 2424 mechanisms and procedures for both the information systems and ICT supply chain 2425 infrastructure, such as manufacturing, shipping and receiving, physical access to facilities, 2426 inventory management, and warehousing. Organization and system integrator personnel 2427 providing development and operational support to the organization should receive training on 2428 how to handle these physical security mechanisms and on the associated ICT supply chain 2429 risks. 2430 2431 2432 <u>TIER</u>: 2
2436

2437 2438

2439

2440

2441

2442

2443

FAMILY: AUDIT AND ACCOUNTABILITY

2444 Audit and accountability are important for ICT supply chain to provide information about what 2445 happened in the federal agency supply chain in case of an ICT supply chain compromise. 2446 Organizations should ensure that they designate ICT supply chain-relevant events and audit for 2447 those events within their own system boundaries using appropriate audit mechanisms (e.g., 2448 system logs, Intrusion Detection System (IDS) logs, and firewall logs). Organizations may 2449 encourage their system integrators and external service providers to do the same and may include 2450 contract clauses that require such monitoring. However, organizations should not deploy audit 2451 mechanisms on the systems outside of their agency boundary including those of system 2452 integrators and external service providers. 2453 2454 SCRM_AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES <u>AU-1</u> 2455 Supplemental ICT SCRM Guidance: Audit mechanisms provide data for tracking activities in an 2456 organization's ICT supply chain infrastructure. Audit and accountability policy and procedures 2457 should appropriately address such tracking and its availability for other organization ICT supply 2458 chain activities, such as configuration management. System integrator, supplier, and external 2459 service provider activities should not be included in such policy, unless those are performed on the 2460 organization's information systems. 2461 2462 TIER: 1, 2, 3 2463 SCRM AU-2 AUDIT EVENTS AU-2 2464 Supplemental ICT SCRM Guidance: An ICT supply chain auditable event is an observable occurrence 2465 within the information system or ICT supply chain infrastructure. Such events should be identified 2466 as ICT supply chain auditable events and captured by appropriate audit mechanisms including: 2467 event occurrence, length and frequency of event occurrence. ICT supply chain events should be 2468 identified as auditable based on the organization's SDLC context and requirements. An example 2469 of such an auditable event can include tracking change, frequency of change, as well as event of 2470 handing off of software source code to ensure that it is authorized, traceable, and verifiable. 2471 2472 2473 TIER: 1, 2, 3 2474 SCRM AU-3 AUDIT REVIEW, ANALYSIS, AND REPORTING AU-6

FIPS 200 specifies the Audit and Accountability minimum security requirement as follows:

users so they can be held accountable for their actions.

Organizations must: (i) create, protect, and retain information system audit records to

the extent needed to enable the monitoring, analysis, investigation, and reporting of

unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure

that the actions of individual information system users can be uniquely traced to those

2475Supplemental ICT SCRM Guidance: For ICT SCRM, the organization should ensure that both ICT2476supply chain and information security events are appropriately filtered and correlated for analysis2477and reporting. For example, if new maintenance or a patch upgrade is recognized to have an2478invalid digital signature, the identification of the patch arrival qualifies as an ICT supply chain2479auditable event, while invalid signature is an information security auditable event. The2480combination of these two events indicates an ICT supply chain auditable event.

2482	TIE	<u>ER</u> : 2, 3	
2485	Col	ntrol enhancements:	
2485 2486	(1)	AUDIT REVIEW, ANALYSIS, AND REPORTING / CORRELATION WITH INFORMATION FROM NON-TECHNICAL SOURCES	<u>AU-6 (9)</u>
2487 2488 2489 2490 2491 2492		<u>Supplemental ICT SCRM Guidance</u> : In an ICT SCRM context, nontechnical sources inc changes to organizational security or operational policy, changes to procurement or contracting processes, and notifications from system integrators, suppliers, and exte service providers regarding plans to update, enhance, patch, or retire/dispose of a system/component.	lude: rnal
2493		TIER: 3	
2494	SCRM_AU-4	NON-REPUDIATION	<u>AU-10</u>
2495 2496 2497 2498 2499 2500 2501 2502 2503 2504	Sup pro rec sup be han rep abo	pplemental ICT SCRM Guidance: Organizations should implement non-repudiation technicotect both information systems and ICT supply chain infrastructure. Examples of what quire non-repudiation include ICT supply chain metadata describing the components, I pply chain communication, delivery acceptance information, etc. For information system patch or maintenance upgrades for software as well as component replacement in a la rdware system. Verifying that such components originate from the OEM is part of nor pudiation. Additionally, ensuring that mechanisms are in place to prevent and detect fa out the absence of performing organization-defined ICT supply chain activities are component.	iques to t may ICT ems, it can irge 1- alse claims nsidered
2504	TIE	<u>ER</u> : 3	
2506 2507	Co	ntrol enhancements:	
2508	(1)	NON-REPUDIATION / ASSOCIATION OF IDENTITIES	<u>AU-10 (1)</u>
2509 2510 2511 2512 2513		<u>Supplemental ICT SCRM Guidance</u> : This enhancement helps traceability in ICT supply also facilitates the accuracy of provenance. <u>TIER</u> : 2	chain. It
2514	(2)	NON-REPUDIATION / VALIDATE BINDING OF INFORMATION PRODCUER IDENTITIY	<u>AU-10 (2)</u>
2515 2516 2517 2518 2519 2520		<u>Supplemental ICT SCRM Guidance</u> : This enhancement validates the relationship of provand the component. Therefore, it ensures integrity of provenance. <u>TIER</u> : 2, 3	venance
2521 2522 2523	(1)	NON-REPUDIATION CHAIN OF CUSTODY	<u>AU-10 (3)</u>
2523 2524 2525 2526 2527 2528		<u>Supplemental ICT SCRM Guidance</u> : Chain of custody is fundamental to provenance and traceability in the ICT supply chain. It also helps verification of system and componintegrity. TIER: 2, 3	l ient
2529	SCRM_AU-5	AUDIT GENERATION	<u>AU-12</u>
2530 2531	<u>Su</u> are	pplemental ICT SCRM Guidance: Organizations should ensure that audit generation mech e in place to capture all relevant supply chain auditable events. Examples of such even	anisms its include:

2532 2533 2534	com capt	ponent version updates, component approvals from acceptance testing results, logistics turing inventory or transportation information, etc.	data
2535	TIEF	<u>R: 2, 3</u>	
2536	SCRM_AU-6	MONITORING FOR INFORMATION DISCLOSURE	<u>AU-13</u>
2537 2538 2539 2540 2541	Supp mul reve incr	<u>plemental ICT SCRM Guidance</u> : Within ICT SCRM context, information disclosure may oc ltiple avenues including open source information. For example, supplier-provided errata eal information about an organization's system that may provide insight into the system reases the risk to the system.	cur via may that
2542	TIEF	<u>R</u> : 2, 3	
2543	SCRM_AU-7	CROSS-ORGANIZATIONAL AUDITING	<u>AU-16</u>
2544 2545 2546	<u>Sup</u> syst	plemental ICT SCRM Guidance: In ICT SCRM context, this control includes organizations' tem integrator or external service provider organizational infrastructure.	use of
2547	TIEF	<u>R</u> : 2, 3	
2549	Cont	trol enhancements:	
2550	(1)	CROSS-ORGANIZATIONAL AUDITING / SHARING OF AUDIT INFORMATION	<u>AU-16(2)</u>
2551 2552 2553 2554 2555 2556 2557 2558 2559 2560 2561 2562 2563 2564 2565 2566		Supplemental ICT SCRM Guidance: Whether managing a distributed audit environment or a audit data sharing environment between organizations and its system integrators or externates services providers, organizations should establish a set of requirements for the process of sharing audit information. In the case of the system integrator and external service provand the organization, a service-level agreement of the type of audit data required vs. where the organization needed for ensuring that appropriate protections are in place to meet mission operation protection needs. Ensure that coverage of both information systems a ICT supply chain infrastructure are addressed for the collection and sharing of audit information.	an ernal of rider nat can levant its and

FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION

2569 FIPS 200 specifies the Certification, Accreditation, and Security Assessments minimum security 2570 requirement as follows: 2571 2572 Organizations must: (i) periodically assess the security controls in organizational 2573 information systems to determine if the controls are effective in their application; (ii) 2574 develop and implement plans of action designed to correct deficiencies and reduce or 2575 eliminate vulnerabilities in organizational information systems; (iii) authorize the 2576 operation of organizational information systems and any associated information system 2577 connections: and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls. 2578 2579 2580 Organizations should integrate ICT supply chain considerations, including the supply chain risk 2581 management process and the use of relevant controls defined in this publication, into ongoing 2582 security assessment and authorization activities. This includes activities to assess and authorize an 2583 organization's information systems and ICT supply chain infrastructure, as well as external 2584 assessments of system integrators and external service providers, where appropriate. ICT supply 2585 chain aspects include documentation and tracking of chain of custody and system 2586 interconnections within and between organizations, verification of ICT supply chain security 2587 training, verification of suppliers claims of conformance to security, product/component integrity, 2588 and validation tools and techniques for noninvasive approaches to detect counterfeits or malware 2589 (e.g., Trojans) using inspection for genuine components including manual inspection techniques. 2590 2591 2592 SCRM CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES <u>CA-1</u> 2593 2594 Supplemental ICT SCRM Guidance: Integrate the development and implementation of assessment and 2595 authorization policies and procedures for ICT supply chain security into the security assessment 2596 and authorization policy. 2597 2598 2599 2600 TIER: 1, 2, 3 2601 2602 SCRM_CA-2 SECURITY ASSESSMENTS CA-2 2603 2604 Supplemental ICT SCRM Guidance: Ensure that the security assessment plan incorporates relevant 2605 ICT SCRM security controls and control enhancements. The security assessment should cover the 2606 assessment of both information systems and ICT supply chain infrastructure and ensure that an 2607 organization-relevant baseline set of controls and control enhancements are identified and used for 2608 the assessment. 2609 2610 TIER: 2, 3 2611 2612 Control enhancements: 2613 (1) SECURITY ASSESSMENTS / SPECIALIZED ASSESSMENTS CA-2(2) 2614 Supplemental ICT SCRM Guidance: Organizations may want to use a variety of assessment 2615 techniques and methodologies such as continuous monitoring, insider threat assessment, and 2616 malicious user's assessment. These assessment mechanisms are context-specific and require 2617 the organization to understand its ICT supply chain infrastructure and to define the required

2618 2619 2620		set of measures for assessing and verifying that appropriate protections have been implemented.	
2620 2621		<u>TIER</u> : 3	
2622	(2)	SECURITY ASSESSMENTS EXTERNAL ORGANIZATIONS	<u>CA-2 (3)</u>
2623 2624 2625 2626 2627 2628 2629		<u>Supplemental ICT SCRM Guidance</u> : For ICT SCRM, organizations may use external assess for system integrators, suppliers, and external service providers. External assessments in certifications and third- party assessments, such as those driven by organizations such as International Organization for Standardization (ISO), the National Information Assurance Partnership (Common Criteria), and The Open Group Trusted Technology Forum (TTF) such certifications meet agency needs.	nents iclude is the ce) if
2630		<u>TIER: 3</u>	
2631	SCRM_CA-3	SYSTEM INTERCONNECTIONS	<u>CA-3</u>
2632 2633 2634 2635 2636 2637 2638	Sup from com pro ens and	plemental ICT SCRM Guidance: Interconnected systems and mission operations require scrut m a supply chain perspective. This includes understanding the connections of those nponents/systems that are directly interconnected with system integrators, external service oviders and, in some cases, suppliers. Ensure that proper service-level agreements are in pl sure compliance to interconnect requirements defined by the organization to system integr d external service providers. Examples of such connections can include:	tiny e lace to ators
2638 2639 2640 2641 2642 2643 2643		 a. A shared development and operational environment between the organization and syintegrator; b. Product update/patch management connection to an off-the-shelf (OTS) supplier; ar c. Data request and retrieval transactions into a processing system residing on an extensive provider shared environment. 	ystem nd mal
2645	TIE	<u>R</u> : 3	
2647	<u>Cor</u>	<u>itrol enhancements:</u>	
2648 2649	(1)	INFORMATION SYSTEM INTERCONNECTIONS / UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS	<u>CA-3 (3)</u>
2650 2651 2652 2653 2654 2655 2656 2657 2658		Supplemental ICT SCRM Guidance: The organization ensures that any connections within the ICT supply chain infrastructure including any connections to their system integrator and external service provider infrastructures are appropriately protected with boundary protected mechanisms including strict mediation of communications across the organization and it supply chain. Any information sharing across these boundaries needs to be vetted and mediated to ensure appropriate sharing practices that meet organization's information sharing strict. TIER: 3	ection ts naring
2659	(2)	SYSTEM INTERCONNECTIONS / CONNECTIONS TO PUBLIC NETWORKS	CA-3 (4)
2660 2661 2662 2663 2664 2665 2666 2666		Supplemental ICT SCRM Guidance: For ICT SCRM, ensure that the system integrator and external service provider appropriately protect connections to public networks. Impleme appropriate processes for review and inspection, evidence gathering, and incident management. Ensure that configurations at the external boundaries and the interfaces this which organizations are communicating with their system integrators and external service providers are monitored and audited periodically.	nt rough ce
2668			

2669 2670	Control enhancements:		
2671 2672	(3)	INFORMATION SYSTEM INTERCONNECTIONS / RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS	<u>CA-3 (5)</u>
2673		Supplemental ICT SCRM Guidance: For ICT SCRM ensure that the system integra	ator and
2674		external service provider appropriately protect connections to public networks	Implement
2675		appropriate processes for review and inspection, evidence gathering, and incide	nt
2676		management	
2670		management.	
2678		<u>TIER: 3</u>	
2679	SCRM_CA-4	PLAN OF ACTION AND MILESTONES	<u>CA-5</u>
2680	Sur	polemental ICT SCRM Guidance: Organizations need to ensure that plan of actions a	nd milestones
2681	inc	<u>picture net root outdation</u> . Of guilligations need to ensure that plan of actions a	he
2682	org	and both information systems and icit supply chain infrastructure. Ensure that t	not of
2682	org	allization includes in its plan of actions and innestones relevant weaknesses, impactores on information systems or ICT supply about infrastructure, and any ran	act of
2005	wea	aknesses on miormation systems of ICT supply chain minastructure, and any ten	legiation to
2004	add	iress weaknesses, as well as any continuous monitoring activities.	
2085	TIE		
2080	<u>11E</u>	<u>R: 2,3</u>	
2687	SCRM_CA-5	SECURITY AUTHORIZATIONS	<u>CA-6</u>
2688	Sup	plemental ICT SCRM Guidance: Authorizing officials should include ICT supply ch	nain
2689	con	isiderations in authorization decisions. To accomplish this, ICT supply chain risk	ks and
2690	con	npensating controls documented in ICT SCRM Plans or system security plans sh	ould be
2691	inc	luded in the decision-making process. Risks should be determined and associated	d compensating
2692	con	strols selected based on output from criticality, threat, and vulnerability analysis.	1 1 1 1
2693		······································	
2694	TIE	<u>R: 1, 2, 3</u>	
2695	SCRM_CA-6	CONTINUOUS MONITORING	<u>CA</u> -7
2696	Sup	oplemental ICT SCRM Guidance: In addition to NIST SP 800-53 Revision 4, Securit	y and Privacy
2697	Con	ntrols for Federal Information Systems and Organizations, control description, s	ee Chapter 2
2698	for	more information.	
2699			
2700	TIE	R: 1, 2, 3	
2701		_ / /	
2702	Cor	trol enhancements:	
2703	(1)	CONTINUOUS MONITORING / TREND ANALYSES	<u>CA-7(3)</u>
2704		Supplemental ICT SCRM Guidance: Information gathered during continuous monit	toring serves as
2705		inputs into ICT SCRM decisions including criticality analysis vulnerability an	d threat
2706		analysis and risk assessment. It also provides information that can be used in it	ncident
2700		analysis, and lisk assessment. It also provides information that call be used in in records and potentially can identify ICT supply chain compromise	
2707		response and potentiarly can identify it i supply chain compromise.	
$\frac{2}{2709}$		TIED: 3	
271ó		<u>11LN</u> , 9	

2711 2712 FAMILY: CONFIGURATION MANAGEMENT 2713 2714 FIPS 200 specifies the Configuration Management minimum security requirement as follows: 2715 2716 Organizations must: (i) establish and maintain baseline configurations and inventories 2717 of organizational information systems (including hardware, software, firmware, and 2718 documentation) throughout the respective system development life cycles; and (ii) 2719 establish and enforce security configuration settings for information technology 2720 products employed in organizational information systems. 2721 2722 Configuration Management helps track systems, components, and documentation throughout the 2723 ICT supply chain. This is important for knowing what changes were made to those systems. 2724 components, and documentation, who made the changes, and who authorized the changes. 2725 Basically, configuration management provides the tools to establish the chain of custody for 2726 systems, components, and documentation. Configuration management also provides evidence for 2727 ICT supply chain compromise investigations when determining which changes were authorized 2728 and which were not, which can provide useful information. Organizations should apply 2729 configuration management controls to their own systems and encourage use of configuration 2730 management controls by their system integrators, suppliers, and external service providers. 2731 2732 SCRM CM-1 CONFIGURATION MANGEMENT POLICY AND PROCEDURES **CM-1** 2733 Supplemental ICT SCRM Guidance: Configuration management is a critical activity that impacts 2734 nearly every aspect of ICT supply chain security. When defining configuration management 2735 policy and procedures, organizations should address the full SDLC. This should include 2736 procedures for introducing and removing components to and from the agency as configuration 2737 items, data retention for configuration items and corresponding metadata, and tracking of the 2738 configuration item and its metadata. The organization should assign the system integrator, 2739 supplier, and external service provider roles for receiving the configuration management policy. 2740 2741 TIER: 1, 2, 3 2742 SCRM CM-2 **BASELINE CONFIGURATION CM-2** 2743 Supplemental ICT SCRM Guidance: Organizations should establish a baseline configuration of both 2744 information systems and ICT supply chain infrastructure by documenting, formally reviewing, and 2745 securing the agreement of stakeholders. The baseline configuration must take into consideration 2746 the organization and any relevant system integrator, supplier, and external service provider 2747 involvement within the organization's ICT supply chain infrastructure where relevant. If the 2748 system integrator, for example, uses the existing organization's infrastructure, appropriate 2749 measures should be taken to establish a baseline that reflects an appropriate set of agreed-upon 2750 2751 criteria for access and operation. 2752 TIER: 2, 3 2753 2754 Control enhancements: 2755 (1) BASELINE CONFIGURATION / REVIEWS AND UPDATES CM-2(1) 2756 Supplemental ICT SCRM Guidance: Reviews and updates of baseline configuration are critical for 2757 traceability and provenance. TIER: 2, 3

2760 2761 2762	(1)	BASELINE CONFIGURATION DEVELOPMENT AND TEST ENVIRONMENTS	<u>CM-2 (6)</u>
2763 2764 2765 2766 2767 2768 2769		Supplemental ICT SCRM Guidance: Organizations should ensure that ICT supply is addressed in the baseline configuration of the development and test environ part of the ICT supply chain infrastructure including meeting requirements for configurations interfacing system integrators, external service providers, and suppliers.	y chain security nments which are or the , in some cases,
2770	SCRM_CM-3	CONFIGURATION CHANGE CONTROL	<u>CM-3</u>
2771 2772 2773 2774 2775 2776 2777 2778	Sup con <i>Con</i> and data <u>TIE</u>	plemental ICT SCRM Guidance: Organizations should determine, implement, mon figuration settings and change controls for federal agency ICT information system throl supports traceability for ICT SCRM. NIST SP 800-53 Revision 4, Security throls for Federal Information Systems and Organizations, control enhancements (4) are mechanisms that can be used for ICT SCRM to collect and manage chance. R: 2, 3	nitor, and audit stems. This <i>y and Privacy</i> <u>s</u> CM-3 (1), (2), ange control
2779	SCRM_CM-4	SECURITY IMPACT ANALYSIS	<u>CM-4</u>
2780 2781 2782 2783 2784 2785 2786 2787 2788 2788 2789 2790	Sup info cha Ens the Sec <u>enh</u> sys suc	plemental ICT SCRM Guidance: Organizations should take under consideration of ormation systems and ICT supply chain infrastructure to determine whether the nges warrants additional protection to maintain an acceptable level of ICT sup sure that such stakeholders as system engineers and system security engineers impact analysis activities to provide their perspectives for SCRM. NIST SP 86 <i>urity and Privacy Controls for Federal Information Systems and Organization</i> ancements CM-4 (1) is a mechanism that can be used for ICT SCRM to protect tem and ICT supply chain infrastructure that may be introduced through the te h as acceptance testing. <u>R</u> : 3	hanges to the e impact of these oply chain risk. are included in 00-53 Revision 4, <i>as</i> , <u>control</u> t the information st environment
2791	SCRM_CM-5	ACCESS RESTRICTIONS FOR CHANGE	<u>CM-5</u>
2792 2793 2794 2795 2796 2797 2798 2799 2800 2801	Sup and infr Exa con <u>TIE</u> <u>Con</u>	<u>plemental ICT SCRM Guidance</u> : Organizations should ensure that requirements real logical access restrictions for changes to information systems or ICT supply or astructure are defined and included in the organization's implementation of a camples include access restriction changes to centrally managed processes for semponent updates and the deployment of the updates $\frac{R}{2}: 2, 3$ http://dx.org.org.nl/dx.or	egarding physical chain ccess restrictions. oftware
2802 2803	(1)	ACCESS RESTRICTIONS FOR CHANGE AUTOMATED ACCESS ENFORCEMENT / AUDITING	<u>CM-5(1)</u>
2804 2805 2806 2807		<u>Supplemental ICT SCRM Guidance</u> : Organizations should implement mechanism access enforcement to information systems and ICT supply chain infrastructu <u>TIER</u> : 3	ns to ensure audit are.
2808	(2)	ACCESS RESTRICTIONS FOR CHANGE / REVIEW SYSTEM CHANGES	<u>CM-5(2)</u>

2809 2810 2811 2812 2813 2814 2815 2816		<u>Supplemental ICT SCRM Guidance</u> : Organizations should define a set of system chang critical to the protection and risk management of information systems and ICT sup infrastructure. These changes may be defined based on the understanding of what i (component, process, or function) and where vulnerabilities exist that are not yet re due to resource constraints. TIER: 2, 3	ges that are ply chain is critical emediated
2817	(3)	ACCESS RESTRICTIONS FOR CHANGE / SIGNED COMPONENTS	CM-5(3)
2818 2819 2820		Supplemental ICT SCRM Guidance: This control aids in verifying that the component or software) is valid, unchanged, and originated from the expected source.	(hardware
2821		<u>TIER</u> : 3	
2822	(4)	ACCESS RESTRICTIONS FOR CHANGE LIMIT LIBRARY PRIVILEGES	<u>CM-5(6)</u>
2823 2824 2825		Supplemental ICT SCRM Guidance: Organizations should note that software libraries of considered configuration items, access to which should be managed and controlled	could be l.
2825		<u>TIER</u> : 3	
2827	SCRM_CM-6	CONFIGURATION SETTINGS	<u>CM-6</u>
2828 2829 2830 2831 2832 2833 2834 2835	Sup con con imp occ infc nee	plemental ICT SCRM Guidance: Organizations should oversee the function of modifyir figuration settings if performed by system integrator or external service provider to npliance with policy. These changes should be tested and approved before they are plemented. Configuration settings should be monitored and audited to alert when a c urred. Methods of oversight include periodic verification, reporting, and review. Th ormation may be shared with various parties within the ICT supply chain infrastructu d-to-know basis.	ng ensure hange has is ure on a
2836 2837	TIE	<u>R</u> : 2, 3	
2838	<u>Con</u>	trol enhancements:	
2839 2840	(1)	CONFIGURATION SETTINGS / AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION	<u>CM-6(1)</u>
2841 2842 2843 2844		<u>Supplemental ICT SCRM Guidance</u> : The organization should employ automated mecha centrally manage, apply, and verify configuration settings for ICT supply chain inf and components.	anisms to rastructure
2845		<u>TIER</u> : 3	
2846	(2)	CONFIGURATION SETTINGS / RESPOND TO UNAUTHORIZED CHANGES	<u>CM-6(2)</u>
2847 2848 2849 2850 2851 2852 2853		<u>Supplemental ICT SCRM Guidance</u> : Organizations should ensure that (1) designated so IT personnel are alerted regarding unauthorized changes to configuration settings t they need to respond; and (2) a specific predefined set of ICT SCRM stakeholders for a more comprehensive review of the ICT SCRM impact of unauthorized chang impact is assessed, relevant stakeholders help define and implement appropriate m activities to ensure a more comprehensive resolution.	ecurity or o which is alerted es. When itigation
2854		<u>TIER</u> : 3	
2855	SCRM_CM-7	LEAST FUNCTIONALITY	<u>CM-7</u>

2856 2857 2858 2859 2860 2861 2862		Sup surf spec <u>TIEF</u>	<u>plemental ICT SCRM Guidance</u> : Within ICT SCRM context, least functionality reduces the face. Organizations should select components that allow the flexibility and options for cifying and implementing least functionality. <u>R</u> : 3	e attack
2002		Con	ttor ennancements.	
2863		(1)	LEAST FUNCTIONALITY UNAUTHORIZED SOFTWARE/BLACKLISTING	<u>CM-7(4)</u>
2864 2865 2866 2867 2868			Supplemental ICT SCRM Guidance: Organizations should define requirements and deploy appropriate processes to specify not allowable software. This can be aided by defining requirement to not use disreputable software. <u>TIER</u> : 2, 3	y g a
2869		(2)	LEAST FUNCTIONALITY AUTHORIZED SOFTWARE/WHITELISTING	CM-7(5)
2870 2871 2872 2873 2874 2875 2876 2877			Supplemental ICT SCRM Guidance: Organizations should define requirements and deploy appropriate processes to specify allowable software. This can be aided by defining a requirement to use only reputable software. This can include requirements for alerts w new software and updates to software are introduced into the organization's environmexample of such requirements is to allow only open source software if its code is availan organization. <u>TIER</u> : 3	/ hen ent. An lable for
2878	SCRM_CI	M-8	INFORMATION SYSTEM COMPONENT INVENTORY	<u>CM-8</u>
2879 2880 2881 2882 2883 2883 2884		Sup the The lice add	plemental ICT SCRM Guidance: Organizations should ensure that critical component asset information system and ICT supply chain infrastructure are included in the asset inven inventory should include information for critical component accountability including ensing, version numbers, component supplier and owners, machine names and network resses, etc.	s within tory.
2885 2886		TIEF	<u>R</u> : 2, 3	
2887		<u>Con</u>	trol enhancements:	
2888 2889		(1)	INFORMATION SYSTEM COMPONENT INVENTORY / UPDATES DURING INSTALLATIONS / REMOVALS	<u>CM-8(1)</u>
2890 2891 2892 2893 2894 2895			<u>Supplemental ICT SCRM Guidance:</u> Organizations, when installing, updating or removing information systems or ICT supply chain infrastructure components, needs to update t inventory of the asset to ensure traceability for tracking critical components, and their configuration needs to ensure accurate inventory of appropriate supply chain protection <u>TIER</u> : 3	g he updated on.
2896		(2)	INFORMATION SYSTEM COMPONENT INVENTORY AUTOMATED MAINTENANCE	<u>CM-8(2)</u>
2897 2898 2899 2900 2901 2902 2903 2904 2905			<u>Supplemental ICT SCRM Guidance:</u> Automated maintenance mechanisms should be implet to ensure that changes to component inventory information system and ICT supply chainfrastructure are monitored for installation, update, and removal. When automated maintenance is performed with a predefined frequency and with the automated collation relevant inventory information about each defined component, ensure that updates are available to relevant stakeholders for evaluation. Also ensure that predefined frequence data collection are highly predictable to reduce the risk of an insider threat bypassing mechanisms.	emented ain on of vies for security

2906		TIER: 3	
2907	(3)	INFORMATION SYSTEM COMPONENT INVENTORY / ACCOUNTABILITY INFORMATION	<u>(4)</u>
2908 2909 2910 2911 2912 2913 2914		Supplemental ICT SCRM Guidance: Organizations should ensure that individuals who originated the acquisition along with intended end users are identified in the property accountability information. Ensure that accountability information is collected for information systems and ICT supply chain infrastructure including any associated personnel who may administer or use the system/components. TIER: 3	l
2915 2916	(4)	INFORMATION SYSTEM COMPONENT INVENTORY ASSESSED CONFIGURATIONS / APPROVED DEVIATIONS <u>CM-8(</u>	<u>(6)</u>
2917 2918 2919 2920 2921 2922		<u>Supplemental ICT SCRM Guidance:</u> Assessed component configurations and any approved deviations must be documented and tracked. Any changes to the baseline configurations of ICT supply chain infrastructure require a review by relevant stakeholders to ensure that the changes do not result in increased ICT supply chain risk. TIER: 3	
2923	(5)	INFORMATION SYSTEM COMPONENT INVENTORY / CENTRALIZED REPOSITORY	(7)
2924 2925 2926 2927 2928 2929 2930 2931 2932 2933 2933 2933 2935	(3)	<u>Supplemental ICT SCRM Guidance:</u> Organizations may choose to implement centralized ICT supply chain infrastructure and system component inventories that include components from all organizational information systems. Centralized repositories of component inventories provide opportunities for efficiencies in accounting for ICT supply chain infrastructure and information system components. Such repositories may also help organizations to rapidly identify the location and responsible individuals of components that have been compromised breached, or are otherwise in need of mitigation actions. Organizations ensure that the resulting centralized inventories include supply chain-specific information required for proper component accountability (e.g., supply chain relevance and ICT supply chain infrastructure of system component owner).	, er or
2936	(6)	INFORMATION SYSTEM COMPONENT INVENTORY AUTOMATED LOCATION TRACKING CM-8(<u>(8)</u>
2937 2938 2939 2940 2941 2942		<u>Supplemental ICT SCRM Guidance: When employing automated mechanisms for tracking of information system components by geographic location, organization should take into consideration information systems and ICT supply chain infrastructure tracking needs to ensure accurate supply chain component inventory.</u> <u>TIER</u> : 2, 3	
2943 2944	(7)	INFORMATION SYSTEM COMPONENT INVENTORY ASSIGNMENT OF COMPONENTS TO SYSTEMS CCM-8(<u>(9)</u>
2945 2946 2947 2948 2949 2950 2951 2952		<u>Supplemental ICT SCRM Guidance:</u> When assigning components to systems, the organization should ensure that information systems and ICT supply chain infrastructure with all relevant components are inventoried, marked, and properly assigned. This facilitates quick inventory of all components relevant to information systems and ICT supply chain infrastructure and enables tracking of components that are considered critical and require differentiating treatment as part of the information system and ICT supply chain infrastructure protection activities.	
2953		<u>TIER</u> : 3	
2954	SCRM_CM-9	CONFIGURATION MANAGEMENT PLAN CM	-9

2955 2956	55 <u>Supplemental ICT SCRM Guidance</u> : Organizations should ensure that ICT SCRM consideratio 56 incorporated into the configuration management planning activities.		
2957 2958 2959	TIER:	2, 3.	
2960	Contro	ol enhancements:	
2961	(1) C	CONFIGURATION MANAGEMENT PLAN ASSIGNMENT OF RESPONSIBILITY	<u>CM-9(1)</u>
2962 2963 2964 2965 2966 2967 2968 2968 2969	<u>S</u> d Iu s d r	Supplemental ICT SCRM Guidance: Organizations should ensure that all relevant lefined to address configuration management activities for ICT information sy CT supply chain infrastructure. Federal agencies should consider whether the supply chain activities are appropriately included in the configuration manages levelopment, sustainment, test, market analysis, Request for Proposal develop review/approval, procurement, integration, sustainment, and maintenance.	roles are /stems and the following ICT ment plan: oment and
2970	<u>T</u>	<u>'IER</u> : 2, 3	
2971	SCRM_CM-10	SOFTWARE USAGE RESTRICTIONS	<u>CM-10</u>
2972 2973	Supple	emental ICT SCRM Guidance: Supplemental guidance provided in control enhan	cement.
2974	Contro	ol enhancements:	
2975	(1) <i>S</i>	OFTWARE USAGE RESTRICTIONS / OPEN SOURCE SOFTWARE	<u>CM-10(1)</u>
2976 2977 2978 2979 2980 2981 2982 2983 2983	S o c r n t t f E	Supplemental ICT SCRM Guidance: When considering software, organizations shoppions and corresponding risks including commercially licensed and open sou components. As an alternative to commercially licensed software, use of open equires an understanding of open source communities' provenance, configura nanagement, sources, binaries, reusable frameworks, reusable libraries' availa esting and use, and much more. Numerous open source solutions are currently ederal agencies, including integrated development environments (IDEs) and v Ensure Organizations are able to:	ould review all arce source software ttion ability for y in use by web servers.
2984 2985 2986 2987 2988		 a) Track the use of all software and associated documentation protected agreements to control copying and distribution; b) Ensure open source opponent use also adheres to the licensing terms Software. 	by licensing of Open Source
2989 2990 2991 2992 2993 2994		 c) Document and monitor the distribution of software as it relates to lice agreement; and d) Evaluate and periodically audit the Open source ICT supply chain inf provided by the open source organization. This evaluation can be dor easily by the organization through obtaining a number of existing doc as experience based on software update and download processes in w 	ensing frastructure as ne reasonably cuments as well which the
2995		organization may have participated.	
2996	I	<u>⁻IER</u> : 2, 3	
2997	SCRM_CM-11	USER-INSTALLED SOFTWARE	<u>CM-11</u>
2998 2999 3000 3001 3002	<u>Supplemental ICT SCRM Guidance</u> : This enhancement extends to the organizational information system users who are not employed by the organization such as system integrators, suppliers, and external service providers. It is therefore relevant to ICT SCRM. <u>TIER</u> : 2, 3		

3005	FAMILY:	CONTINGENCY PLANNING	
3000	FIPS 200 s	specifies the Contingency Planning minimum security requirement as fol	llows:
3008 3009 3010 3011 3012	Or res sys op	rganizations must establish, maintain, and effectively implement plans fo sponse, backup operations, and post-disaster recovery for organizationa stems to ensure the availability of critical information resources and cor perations in emergency situations.	or emergency Il information ntinuity of
3013 3014 3015 3016 3017 3018 3019 3020 3021	ICT supply system cor supply cha Additional sites, have Federal ag dependenc	y chain concerns of contingency planning include planning for alternativ nponents, alternative suppliers of systems and services, denial of service in, and planning for alternate delivery routes for critical system compon ly, many techniques used for contingency planning, such as alternative p their own ICT supply chains including their own specific ICT supply ch encies should ensure that they understand and manage ICT supply chain ties related to the contingency planning activities as necessary.	e suppliers of e attacks to the ents. processing nain risks. risks and
3022	SCRM_CP-1	CONTIGENCY PLANNING POLICY AND PROCEDURES	<u>CP-1</u>
3023 3024 3025 3026 3027 3028 3029 3030	<u>Su</u> the su	 <u>pplemental ICT SCRM Guidance</u>: Organizations should integrate ICT supply chain contingency planning policy. The policy should cover ICT information system pply chain infrastructure and address: a. Unplanned components failure and subsequent replacement; b. Planned replacement related to feature improvements, maintenance, upgr modernization; and c. Product unavailability. 	concerns into as and the ICT rades, and
3031	TIE	<u>=R</u> : 1, 2, 3	
3032	SCRM_CP-2	CONTIGENCY PLAN	<u>CP-2</u>
3033 3034 3035 3036 3037 3038 3039 3040 3041	Su for cha (es pro <u>TIE</u>	pplemental ICT SCRM Guidance: Organizations should define and implement a cor ICT supply chain infrastructure so that there is no loss of data or operations in ain. Contingencies should be put in place for ICT supply chain infrastructure, s specially critical components), and processes to ensure protection against compr ovide appropriate failover.	ntingency plan the supply ystems romise and to
3042	(1)	CONTINGENCY PLAN / COORDINATE WITH EYTERNAL SERVICE PROVIDERS	(P-2 (7)
3043 3044 3045 3046 3047 3048 3049 3050 3051 3052 3052		<u>Supplemental ICT SCRM Guidance</u> : Organizations should ensure that supply chain ICT supply chain infrastructure provided by an external service provider has a failover to ensure lack of service interruption. Organizations should ensure the planning requirements are defined as part of the service-level agreement. The have specific terms addressing critical components and function support in ca service to ensure continuity of operation for critical information systems. Org should work with external service providers to identify service providers' exist contingency plan practices and build on them as required by the organization's business needs to aid in cost reduction and efficient implementation.	in systems and appropriate at contingency agreement may use of denial of anizations sting 's mission and

3054	(2)	CONTINGENCY PLAN / IDENTIFY CRITICAL ASSETS	<u>CP-2 (8)</u>
3055 3056 3057 3058 3059 3060		<u>Supplemental ICT SCRM Guidance</u> : Ensure that critical assets are identified to ensure that appropriate requirements are defined for contingency planning and administered to continuity of operation. A key step in this process is to complete a criticality analysis components, functions, and processes to identify all critical assets. See Chapter 2, 4 Analysis.	hat ensure sis on Criticality
3061		TIER: 3	
3062	SCRM_CP-3	ALTERNATE STORAGE SITE	<u>CP-6</u>
3063 3064 3065 3066 3067	<u>Sup</u> pro infi	plemental ICT SCRM Guidance: When managed by system integrators or external servi widers, alternate storage sites are considered within an organization's ICT supply ch rastructure. In that case, organizations should apply appropriate ICT supply chain co	ce ain ntrols.
3068	TIE	<u>R</u> : 2, 3	
3069	SCRM_CP-4	ALTERNATE PROCESSING SITE	<u>CP-7</u>
3070 3071 3072 3073 3074	<u>Sur</u> pro pro infi <u>TIE</u>	<u>plemental ICT SCRM Guidance</u> : When managed by system integrators or external servividers, alternate processing sites are considered within an organization's ICT supply rastructure. In that case, organizations should apply appropriate ICT supply chain co <u>R</u> : 2, 3	ce ⁷ chain ntrols.
3075	SCRM_CP-5	TELECOMMUNICATIONS SERVICES	<u>CP-8</u>
3076 3077 3078	<u>Sur</u> Cor	plemental ICT SCRM Guidance: Supplemental guidance provided in control enhancementer of enhancements:	ent.
3079 3080	(1)) TELECOMMUNICATIONS SERVICES SEPARATION OF PRIMARY / ALTERNATE PROVIDERS	<u>CP-8 (3)</u>
3081 3082 3083 3084		<u>Supplemental ICT SCRM Guidance</u> : Separation of primary and alternate providers is cu ICT supply chain resilience. <u>TIER</u> : 2, 3	ritical for
3085	(2)	TELECOMMUNICATIONS SERVICES / PROVIDER CONTINGENCY PLAN	<u>CP-8 (4)</u>
3086 3087 3088 3089		<u>Supplemental ICT SCRM Guidance</u> : For ICT SCRM, system integrator and external se provider contingency plans should provide separation in infrastructure, service, propersonnel where appropriate.	rvice ocess, and
3090 3091 3092		<u>TIER:</u> 2, 3	

- 3093 FAMILY: IDENTIFICATION AND AUTHENTICATION
- FIPS 200 specifies the Identification and Authentication minimum security requirement asfollows:
- 3097

3098 3099

3100

Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

- 3101 3102 NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems 3103 and Organizations, expands the FIPS 200 identification and authentication control family to 3104 include identification and authentication of components, in addition to individuals (users) and 3105 processes acting on behalf of individuals. Identification and authentication is critical for ICT 3106 SCRM because it provides traceability of individuals, processes acting on behalf of individuals, 3107 and specific systems/components in an organization's ICT supply chains. Identification and 3108 authentication is required to appropriately manage ICT supply chain risks to both reduce risks of 3109 ICT supply chain compromise and to help have needed evidence in case of ICT supply chain
- 3110 compromise.
- 3111
- 3112 SCRM_IA-1 IDENTIFICATION AND AUTHENCITCATION POLICY AND PROCEDURES IA-1
- 3113Supplemental ICT SCRM Guidance: The organization should enhance their identity and access3114management policies for ICT SCRM to ensure that critical acquirer roles are defined and critical3115acquirer systems, components, and processes are identified for traceability. It is important not to3116provide identity for all things in the ICT supply chain that are cost-prohibitive and too voluminous3117to process. This should include the identity of components that in the past were not considered3118under identification and authentication.
- 3119 3120 <u>TIER: 1,2,3</u>

3121 SCRM_IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) IA-2

- 3122Supplemental ICT SCRM Guidance: Organizations should ensure that appropriate identification and3123authentication is defined for organizational users accessing the information system or ICT supply3124chain infrastructure. An organizational user can include employees and individuals deemed to3125have equivalent status of employees (e.g., contractors, guest researchers, etc.) and may include3126system integrators brought in to take on contractor roles. Criteria such as duration in a role can aid3127in defining which identification and authentication mechanisms are used. Defining a set of roles3128and the level of authorization may be needed for proper implementation.
- 3129 3130 <u>TIER: 1,2,3</u>

3131 SCRM_IA-3 IDENTIFIER MANAGEMENT

3132Supplemental ICT SCRM Guidance: Especially in the ICT SCRM context, identifiers are not limited to3133those for individuals; identifiers also should be assigned to documentation, devices, and3134components throughout the agency SDLC, from concept to retirement. The benefit of having these3135identifiers is greater visibility within an organization's ICT supply chain infrastructure.3136For software development, the identifiers should be assigned for those components that have3138achieved configuration item recognition. For devices and for operational systems, identifiers3139should be assigned when the items enter the organization's ICT supply chain infrastructure, such

IA-4

3140 3141 3142	as rec	as when they are transferred to federal agency ownership or control through shipping and receiving or download.		
3142 3143 3144 3145 3146 3147 3148 3149	System ide 53 con wit	stem integrators, suppliers, and external service providers typically use their own identifiers for cking within their own ICT supply chain infrastructures. Federal agencies should correlate those ntifiers with the agency-assigned identifiers for traceability and accountability. NIST SP 800- Revision 4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i> , ntrol IA-3 enhancements (4) and (5) are mechanisms that can be used to manage identities hin ICT SCRM context.		
3150 3151	TIE	<u>R: 2, 3</u>		
3152	<u>Cor</u>	ntrol enhancements:		
3153	(1)	IDENTIFIER MANAGEMENT / CROSS-ORGANIZATION MANAGEMENT		
3154 3155 3156 3157 3158 3159		Supplemental ICT SCRM Guidance: This enhancement helps traceability and provenance throughout the ICT SCRM among the organization and its system integrators, suppliers, and external service providers. This includes individuals as well as systems and devices engaged in ICT supply chain activities.		
3139		<u>11EK</u> . 1, 2, 3		
3160	SCRM_IA-4	AUTHENTICATOR MANAGEMENT IA-5		
3161 3162 2163	<u>Sur</u> thr	oplemental ICT SCRM Guidance: This control facilitates traceability and non-repudiation oughout the ICT supply chain.		
3164 3165	TIE	<u>R</u> : 2, 3		
3166	Cor	ntrol enhancements:		
3167	(1)	AUTHENTICATOR MANAGEMENT / CHANGE AUTHENTICATORS PRIOR TO DELIVERY		
3168		Supplemental ICT SCRM Guidance: This enhancement provides verification of chain of custody.		
3170		TIER: 3		
3171	(2)	AUTHENTICATOR MANAGEMENT / CROSS-ORGANIZATION CREDENTIAL MANGEMENT IA-5 (9)		
3172 3173 3174		Supplemental ICT SCRM Guidance: This enhancement facilitates provenance and chain of custody.		
3175		<u>TIER</u> : 3		
3176	SCRM_IA-5	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)		
3177 3178 3179 3180 3181 3182 3183 3184 3185	<u>Supplemental ICT SCRM Guidance</u> : For SCRM, managing the identification and authentication of non-organizational users is critical. All organizations who deliver maintenance, including system integrators, perhaps external services providers, and certainly suppliers have the potential of engaging in organizational ICT supply chain infrastructure for service delivery (development/integration services, product support, etc.). Managing the establishment, auditing, use, and revocation of identification and authentication is critical to ensure promptness is achieved, especially in the case of revocation management.			

- 3186 FAMILY: INCIDENT RESPONSE
- 3187
- 3188 FIPS 200 specifies the Incident Response minimum security requirement as follows:
- 3189 3190

3192

3193

3194

Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection,

- analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.
- 3195 ICT supply chain compromises may span federal agency, system integrators, suppliers, and
 and external service provider systems and organizations. Organizations should ensure that their
 incident response controls address ICT supply chain concerns including how information about
 incidents will be shared with system integrators, suppliers, and external service integrators.
 Incident response will help determine whether an incident is related to the ICT supply chain.
- 3200

3223

3224

3225

3226

3227 3228

- 3201 SCRM_IR-1 IDENTIFICATION AND AUTHENCITCATION POLICY AND PROCEDURES
- 3202 Supplemental ICT SCRM Guidance: Integrate ICT SCRM considerations into incident response policy 3203 and procedures. ICT supply chain-related incidents and those cybersecurity incidents that may 3204 complicate or impact ICT supply chain concerns must be defined in the policy. Additionally, the 3205 policy should define when, how, and with whom to communicate within the broader ICT supply 3206 chain security stakeholders and ICT supply chain partners in the event of an incident. Incident 3207 information may also be shared with organizations such as the FBI. US CERT (United States 3208 Computer Emergency Readiness Team), and NCCIC (National Cybersecurity and 3209 Communications Integration Center) as appropriate. This communication to ICT supply chain 3210 partners should be defined in agreements with system integrators, suppliers, and external service 3211 providers and be bidirectional to inform all involved parties. Depending on the severity of the 3212 incident, the need to accelerate communications upstream and downstream may be necessary. 3213 Appropriate agreements should be put in place with system integrators, suppliers, and external 3214 service providers to ensure speed of communication, response, corrective actions, and other 3215 related activities. 3216
- Individuals working within specific mission and system environments need to recognize and
 report ICT supply chain-related incidents. Policy should state when and how this reporting is to be
 done. Additionally, the communications response process must be defined addressing when, how,
 and with whom to communicate with the broader supply chain security stakeholders and supply
 chain partners in the event of an incident.

Additionally, in Tiers 2 and 3, procedures and organization-specific incident response methods must be in place, training completed (consider including IPSec and any appropriate threat briefing in training), and coordinated communication established between the acquirer and its many suppliers to ensure efficient coordinated incident response effort.

<u>TIER</u>: 1, 2, 3

- 3229 SCRM_IR-2 INCIDENT HANDLING
- 3230 <u>Control enhancements:</u>
- 3231 (1) INCIDENT HANDLING / SUPPLY CHAIN COORDINATION
- 3232Supplemental ICT SCRM Guidance: In many cases, a number of organizations are involved in3233managing incidents and responses for supply chain security. After an initial processing of the3234incident is completed and a decision is made to take action (in some cases, no action may be

IR-4 (10)

IR-1

 providers need to conduct coordinated communications, incident response, not call corrective actions activities. Securely sharing information through a coordinated set personnel in key roles will allow for a more comprehensive approach, which is key handling incidents. Acquirers need to work closely with system integrators, supplier external service providers for the handling of incidents. Therefore, selecting system integrators, suppliers, and external service providers with mature capabilities for suppliced incident handling is important for handling ICT SCRM incidents. If transparency for handling is limited due to the nature of the relationship, define a set of acceptable or the agreement (e.g., contract). A review (and potential revision) of the agreement is recommended, based on the lessons learned from previous incidents. <u>TIER</u>: 2 	e se, and for rs, and pporting or incident riteria in
S SCRM_IR-3 INCIDENT REPORTING	
Control enhancements:	
(1) INCIDENT REPORTING / COORDINATION WITH SUPPLY CHAIN	<u>IR-6 (3)</u>
Supplemental ICT SCRM Guidance:The reporting of security incident information from acquirer to the supplier or from the supplier to the acquirer requires protection. Orga ensure that information is reviewed and approved for sending based on acquirer/sup agreements. Any escalation of or exception from this reporting should be clearly de the agreement. The methods of communications regarding such data must ensure th is adequately protected for transmission and received by approved individuals withi organization only.TIER: 3	n the anizations oplier fined in at the data in the
	<u>IR-9</u>
J SCRM_IR-4 INFORMATION SPILLAGE RESPONSE	age
 SCRM_IR-4 INFORMATION SPILLAGE RESPONSE <u>Supplemental ICT SCRM Guidance</u>: The ICT supply chain is vulnerable to information spillage response activities should include ICT supply chain-information spills. This may require coordination with system integrators, suppliers, service providers. The details of how this coordination is to be conducted should be the agreement (a question spill). See SA 4 	rela anc incl

3270 FAMILY: MAINTENANCE 3271

3273 3274

3275

3276

3277

3286

3287

3288

3289

3290

3291

3292

3293

3294 3295

3296

3297

3298

3299

3300

3301

3302

3303 3304

3305

3306

3307

3308

3315 3316

3317 3318

3319

3320

3321

3322

3323

3324

FIPS 200 specifies the Maintenance minimum security requirement as follows: 3272

> Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

3278 Maintenance is frequently performed by an organization that is different from the federal agency. 3279 As such, maintenance becomes part of the ICT supply chain. Maintenance includes performing 3280 updates and replacements. This document can be applied to a maintenance situation including 3281 assessing the ICT supply chain risks, selecting ICT SCRM controls, implementing these controls, 3282 and monitoring them. 3283 3284

SCRM MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES 3285

MA-1

Supplemental ICT SCRM Guidance: Organizations should ensure that ICT supply chain concerns are included in maintenance policies and procedures for all organizational information systems. With standard maintenance contracts, mission, organization, and system-specific objectives and requirements are shared between agency and system integrator, leaving room for significant vulnerabilities and insider opportunities for attack. In many cases, the maintenance of systems is outsourced to a system integrator and as such, appropriate measures must be taken to ensure proper assessment of the organization and its IT infrastructure doing maintenance. Even when maintenance is not outsourced, the upgrades and patches, frequency of maintenance, replacement parts, and other aspects of system maintenance are affected by the supply chain.

Maintenance policies should be defined both for the information systems and the agency ICT supply chain infrastructure. The maintenance policy should reflect appropriate controls based on an applicable risk assessment (including criticality analysis) within the maintenance context, such as remote access, roles and attributes of maintenance personnel that have access, the frequency of updates, duration of contract, logistical path used for updates or maintenance, and monitoring and audit mechanisms. The maintenance policy should state which tools are explicitly allowed or not allowed. For example, in the case of software maintenance, source code, test cases, and other item accessibility to maintain a system or components should be stated in the contract.

Maintenance policies should be refined and augmented at each tier. At Tier 1, the policy should define allowed maintenance activities. At Tier 2, the policy should reflect the mission operation's needs and critical functions. At Tier 3 it should reflect the specific system needs. The requirements in Tier 1, such as nonlocal maintenance, should flow to Tiers 2 and 3; for example, when nonlocal maintenance is not allowed by Tier 1, it should also not be allowed at Tiers 2 and 3.

TIER: 1,2, 3

3309 3310 3311 3312 3313 3314 SCRM MA-2 **CONTROLLED MAINTENANCE**

Control enhancements:

(1) CONTROLLED MAINTENANCE JAUTOMATED MAINTENANCE ACTIVITIES

MA-2 (2)

Supplemental ICT SCRM Guidance: Organizations should ensure that all automated maintenance activities are controlled and managed according to maintenance policy. Examples of automated maintenance activities can include COTS product patch updates, call home features with failure notification feedback, etc. Managing these activities may require establishing staging processes with appropriate supporting mechanisms to provide vetting or filtering as appropriate. These processes are especially important for critical components.

TIER: 3

3326 3327 3328 3329 3330 3331 3332 3333 3334 3335 3336 3337 3338 3339	SCRM_MA-3 Sup mail sect upg the rep dep too <u>TIE</u>	MAINTENANCE TOOLS <u>plemental ICT SCRM Guidance</u> : Maintenance tools have an ICT supply chain of their own. intenance tools are introduced and upgraded, organizations should consider supply chain urity implications of this set of actions. This is applicable when there is a need to acquire grade a maintenance tool (e.g., an update to development environment or testing tool), in selection, ordering, storage, and integration of the maintenance tool. This should include lacement parts for maintenance tools. This activity may be performed at both <u>Tiers</u> 2 and bending on how an agency handles the acquisition, operations, and oversight of maintenands. <u>R</u> : 2, 3. <u>http://dx.upu.com/activity.com/</u>	MA-3 When e or cluding e .3, ince
3340	(1)	MAINTENANCE TOOLS / INSPECT TOOLS	<u>MA-3(1)</u>
3341 3342 3343 3344 3345 3346		<u>Supplemental ICT SCRM Guidance</u> : Organizations should deploy acceptance testing to ver the maintenance tools are as expected and provide only required functions. Maintenance should be authorized with appropriate paperwork, verified as claimed through initial verification, and then acceptance tested for stated functionality. <u>TIER</u> : 3	ify that e tools
3347	(2)	MAINTENANCE TOOLS / INSPECT MEDIA	<u>MA-3(2)</u>
3348 3349 3350 3351 3352 3353		Supplemental ICT SCRM Guidance: Organizations should verify that the media are as experient and provide only required functions. Media should be authorized with appropriate paper verified as claimed through initial verification, and then acceptance tested for stated functionality. <u>TIER</u> : 3	cted rwork,
3354	(3)	MAINTENANCE TOOLS PREVENT UNAUTHORIZED REMOVAL	<u>MA-3(3)</u>
3355 3356 3357 3358 3359 3360 3361 3362 3363 3364 3365 3366		<u>Supplemental ICT SCRM Guidance</u> : Unauthorized removal of ICT maintenance tools may introduce ICT Supply Chain risk including, for example, unauthorized modification, replacement with counterfeit, or malware insertion while the tool is outside of the organization's control. ICT maintenance tools can include integrated development environment (IDE), testing, or vulnerability scanning. For ICT SCRM, it is important t organizations should explicitly authorize, track, and audit any removal of maintenance Once ICT tools are allowed access to an organization/system, they should remain the property/asset of the system owner and tracked if removed and used elsewhere in the organization. ICT maintenance tools currently in use or retired but stored should not be allowed to leave the organization's premises until they are properly vetted for removal. TIER: 3	hat tools.
3367	SCRM_MA-4	NONLOCAL MAINTENANCE	<u>MA-4</u>
3368 3369 3370 3371 3372 3373 3374 3375 3376	Sup exte NIS Org mai	Aplemental ICT SCRM Guidance: Nonlocal maintenance may be provided by system integrate ernal service providers. Appropriate protections should be in place to manage associated ST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information System ganizations, control MA-4 enhancements (2) and (3) provide further guidance on nonloc intenance activities. <u>R:</u> 2, 3. <u>http://dx.uk.uk.uk.uk.uk.uk.uk.uk.uk.uk.uk.uk.uk.</u>	ors or risks. <i>is and</i> al

3382 338**3** (1) NONLOCAL MAINTENANCE / DOCUMENT NONLOCAL MAINTENANCE

- 3378 Supplemental ICT SCRM Guidance: Organizations should deploy acceptance testing to verify that 3379 the maintenance tools are as expected and provide only required functions. Maintenance tools 3380 should be authorized with appropriate paperwork, verified as claimed through initial 3381 verification, and then acceptance tested for stated functionality.
 - TIER: 2, 3
- 3384 SCRM_MA-5 MAINTENANCE PERSONNEL

3385 Supplemental ICT SCRM Guidance: Maintenance personnel may be employed by a system integrator, 3386 supplier, and external service provider. As such, appropriate protections should be in place to 3387 manage associated risks. 3388 3389

- TIER: 2, 3
- 3390 SCRM MA-6 TIMELY MAINTENANCE

3391 Supplemental ICT SCRM Guidance: For spare parts, replacement parts, or alternate sources, agencies 3392 should ensure appropriate lead-times to purchase through original equipment manufacturers 3393 (OEMs) or authorized distributors. If OEMs are not available, it is preferred to acquire from 3394 authorized distributors. If an OEM or an authorized distributor is not available and the only 3395 alternative is to purchase from a non-authorized distributor or secondary market, a risk assessment 3396 should be performed, including a revisit of criticality and threat analysis to identify additional risk 3397 mitigations to be used. For example, the acquirer should check for history of counterfeits. 3398 inappropriate practices, or a criminal record. See Chapter 2 for criticality and threat analysis 3399 details.

3400 3401 TIER: 3

3407

3408

3409

3410

3411

3412

3413

3414

3415

3416

3402 SCRM_MA-7 MAINTENANCE MONITORING AND INFORMATION SHARING

3403 Control: The organization monitors the status of systems and components and communicates out 3404 of bounds and out of spec performance to [Assignment: organization-defined system integrators, 3405 suppliers, or external service providers]. 3406

Supplemental ICT SCRM Guidance: Failure rates provide useful information to the acquirer to help plan for contingencies, alternate sources of supply, and replacements. Failure rates are also useful for monitoring quality and reliability of systems and components. This information provides useful feedback to system integrators, suppliers, and external service providers for corrective action and continuous improvement. In Tier 2, agencies should track and communicate the failure rates to suppliers (OEM and/or an authorized distributor). The failure rates and the issues that can indicate failures including root causes should be identified by an agency's technical personnel (e.g., developers, administrators, or maintenance engineers) in Tier 3 and communicated to Tier 2. These individuals are able to verify the problem and identify technical alternatives.

- 3417 Related Control: IR-4(10) 3418
- 3419 <u>TIER</u>: 3 3420

MA-6

MA-5

3421 FAMILY: MEDIA PROTECTION

3422			
3423	FIPS 200 spec	cifies the Media Protection minimum security requirement as follows:	
3424	_		
3425	Orgai	nizations must: (i) protect information system media, both paper and digital;	(<i>ii</i>)
3426	limit c	access to information on information system media to authorized users; and	(iii)
3427	sanitiz	ze or destroy information system media before disposal or release for reuse.	
3428			
3429	Media itself ca	an be a component traversing the ICT supply chain infrastructure or containi	ing
3430	information al	bout the organization's ICT supply chain. This includes both physical and lo	gical
3431	media includi	ng, for example, system documentation on paper or in electronic files, shipp	ing and
3432	delivery docur	mentation with acquirer information, memory sticks with software code, or	C
3433	complete rout	ers or servers that include permanent media. The information contained on t	he
3434	media may be	e federal agency sensitive information and system integrator, supplier, or exte	ernal
3435	service provid	ler sensitive or proprietary information. Additionally, the media is used through	ughout
3436	the SDLC. fro	om concept to disposal. Organizations should ensure that the Media Protectic)n
3437	controls are ar	polied to both federal agency media and the media received from system inte	egrators
3438	suppliers and	external service providers throughout the SDLC	<i>.B</i> r <i>acors,</i>
3439	suppliels, and		
2440			
3440	SCRM_MP-1	MEDIA PROTECTION POLICY AND PROCEDURES	<u>MP-1</u>
3441	Sunnler	mental ICT SCRM Guidance: A number of documents and information on a variety of t	ohysical
3442	and ele	ectronic media is disseminated across the ICT supply chain. This information contai	ns a
3443	variety	v of acquirer, system integrator, supplier, and external service provider sensitive info	ormation
3444	and int	tellectual property. Because the media traverses or resides in the ICT supply chain, i	it is
3445	especia	ally important to protect it. Media protection policies and procedures should address	s media
3446	and me	edia players in the organization's ICT supply chain.	
3447			
3448	TIER:	1, 2	
3449	SCRM_MP-2	MEDIA TRANSPORT	<u>MP-5</u>
3450	Supple	mental ICT SCRM Guidance: Organizations should consider ICT supply chain risks wh	ien
3451	transpo	orting media, either by acquirer or non-acquirer personnel or organizations. Some of	f the
3452	technic	ques to protect media during transport and storage include cryptographic techniques	and
3453	approv	ved custodian services.	
3454			
3455	TIER:	1, 2	
3456	SCRM_MP-3	MEDIA SANITIZATION	<u>MP-6</u>

- 3457Supplemental ICT SCRM Guidance: Media originate anywhere including from system integrators,3458suppliers, and external service providers. Media is used throughout the SDLC. It can be new,3459refurbished, or reused. Media sanitization is critical to ensure that ICT SCRM information is3460removed before the media is used, reused or discarded. NIST SP 800-53 Revision 4, Security and3461Privacy Controls for Federal Information Systems and Organizations, control enhancements MP-63462(1), (2), (3), (7), and (8) provide further media sanitization mechanisms. See Appendix E for the3463listed control enhancement details.
- 3464 3465 <u>TIER: 2, 3</u>

- 3466 FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION 3467
- FIPS 200 specifies the Physical and Environmental Protection minimum security requirement as
 follows:
 - Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.
- 3478 ICT supply chains span the physical and logical world. Physical factors include, for example, 3479 weather and road conditions that may have an impact to transporting ICT components (or 3480 devices) from one location to another between system integrators, suppliers, and organizations. If 3481 not properly addressed as a part of the ICT SCRM risk management processes, physical and 3482 environmental risks may have a negative impact on the organization's ability to receive critical 3483 components in a timely manner, which may in turn impact their ability to perform mission 3484 operations. Organizations should integrate physical and environmental protection controls to 3485 mitigate such risks and ensure that there are no gaps. It should be noted that the degree of 3486 physical and environmental protection required throughout the ICT supply chain is greatly 3487 dependent on the degree of integration between acquirer and system integrator/supplier/external 3488 service provider organizations, systems, and processes.
- 3489

3472

3473

3474

3475

3476

3477

- 3490 SCRM_PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES PE-1
- 3491Supplemental ICT SCRM Guidance: Organizations should integrate ICT supply chain risks into3492physical and environmental protection policy. The degree of such protection required throughout3493the ICT supply chain is greatly dependent on the degree of integration between acquirer and3494system integrator/supplier/external service provider organizations, systems, and processes. The3495physical and environmental protection policy should ensure that the physical interfaces have3496adequate protection and audit of such protection.
- 3498 <u>TIER</u>: 1, 2, 3
- 3499 SCRM_PE-2 PHYSICAL ACCESS CONTROL
- 3500 Supplemental ICT SCRM Guidance: Organization should ensure that physical access control covers 3501 individuals and organizations engaged in the organizations' ICT supply chain such as system 3502 integrator, supplier, and external service provider personnel. A vetting process should be in place 3503 based on organizational-defined requirements/policy prior to granting access to the ICT supply 3504 chain infrastructure and any relevant elements. Facilities access establishment, maintenance, and 3505 revocation processes should meet organizational access control policy rigor. The speed of 3506 revocation for system integrators, external services providers, and suppliers needing access to 3507 physical facilities should be managed in accordance with the activities performed in their 3508 contracts. Prompt revocation is critical when either individual or organizational need no longer 3509 exists.
- 3510 3511 <u>TIER: 2, 3</u>
- <u>3513</u> <u>Control enhancements:</u>
- 3514 (1) PHYSICAL ACCESS CONTROL / TAMPER PROTECTION

<u>PE-3 (5)</u>

PE-3

3515	S	Supplemental ICT SCRM Guidance: Tamper protection is critical for reducing ICT supply of	chain	
3516	risks in hardware. Tamper protection should be validated prior to implementation.			
3517				
3518	т	ïER: 2, 3		
3519	SCRM PE-3	MONITORING PHYSICAL ACCESS	PE-6	
	~			
3520	Supple	emental ICT SCRM Guidance: Individuals physically accessing organization's facilities		
3521	incluc	ding those supporting ICT supply chain infrastructure may be employed by system		
3522	integr	ators, suppliers, and external service providers. Monitoring these individuals' activitie	es	
3523	reduc	es ICT supply chain risks		
3524	Teade	os ro r supprý chain risko.		
3525	<u>TIER</u> :	3		
3526	SCRM_PE-4	DELIVERY AND REMOVAL	<u>PE-16</u>	
2527				
3521	Supple	emental ICT SCRM Guidance: This enhancement reduces the risks introduced during physic	sical	
3528	delive	ery and removal of hardware components from organizations' information systems or	ICT	
3529	suppl	y chain environment.		
3230				
3331	<u>HER</u> :	3		
3532	SCRM_PE-5	ALTERNATE WORK SITE	<u>PE-17</u>	
2522				
2222	Supple	emental ICI SCRM Guidance. Organizations should consider the risks associated with		
3534	organ	izational employees or system integrator personnel using alternate work sites. This cai	n	
3535	incluc	le work from home or other nonwork locations.		
3536				
3537	<u>TIER</u> :	3		
3538	SCRM_PE-6	LOCATION OF INFORMATION SYSTEM COMPONENTS	<u>PE-18</u>	
2520	Currel	mental ICT CCDM Cuideness Division and any incompanies have an impact on the		
2540	<u>Supple</u>	<u>amental ICT SCRW Guidance</u> . Filysical and environmental nazards have an impact on the		
2540	avalla	ionity of systems and components that are of will be acquired and physically transport	led to	
3541	the or	ganization's locations. For example, organizations should consider the location of		
3542	inforr	nation system components critical for agency operations when planning for alternative	e	
3543	suppl	iers for these components. See CP-6 and CP-7.		
3544				
3040	<u>TIER</u> :	1, 2, 3		
3546	SCRM_PE-8	ASSET MONITORING AND TRACKING	<u>PE-20</u>	
3547	<u>Su</u> pple	emental ICT SCRM Guidance: Organizations should use asset location technologies to tra-	ck	
3548	syster	m and components transported between protected areas. or in storage awaiting		
3549	imple	mentation testing maintenance or disposal Examples include RFID or digital signat	ures to	
3550	accon	nnlish such activities. These technologies help protect against		
3551	uccon	ipinsii suon uotivittos. These teennoiogies neip proteet ugunist.		
3557	0	Diverting system or component for counterfait replacement:		
3552	ä 1.	Loss of confidentiality integrity or evolutibility of system or common and functions	nd	
3333 2551	b	Loss of confidentiality, integrity, or availability of system or component function a	ula	
3334 2555		data (including data contained within the component and data about the componen	t); and	
3222	с	. Interrupting supply chain and logistics processes for critical components.		
3556				
3557	Asset	location technologies also help gather data that can be used later for incident manager	ment.	
3558				
3559	<u>TIER</u> :	2, 3		

3560 FAMILY: PLANNING

3562 FIPS 200 specifies the Planning minimum security requirement as follows:

> Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

3569 ICT SCRM concerns should influence security planning, including such activities as security 3570 architecture, coordination with other organizational entities, and development of System Security 3571 Plans. When acquiring ICT products and services from system integrators, suppliers, and external 3572 service providers, organizations may be sharing facilities with those organizations, having 3573 employees of these organizations on the federal agency premises, or use information systems that 3574 belong to those entities. In these and other applicable situations, organizations should coordinate 3575 their security planning activities with these entities to ensure appropriate protection of federal 3576 agency ICT supply chain infrastructure, as well as of the information systems and components 3577 traversing the ICT supply chain. When establishing security architectures, organizations should 3578 provide for component and supplier diversity to manage the ICT supply chain-related risks of 3579 suppliers going out of business or stopping the production of specific components. Finally, as 3580 stated in Chapter 2, organizations may integrate ICT SCRM controls into System Security Plans 3581 for individual systems.

3582

3591

3592

3593

3594

3595

3596

3597

3598

3599 3600

3601 3602

3561

3563 3564

3565

3566

3567

3568

3583 SCRM_PL-1 SECURITY PLANNING POLICY AND PROCEDURES

- 3584 Supplemental ICT SCRM Guidance: Include ICT supply chain risk management considerations in 3585 security planning policy and procedures. This should include security policy, operational policy, 3586 and procedures for ICT supply chain risk management to shape the requirements and the follow-3587 on implementation of operational systems. 3588 3589
 - TIER: 1

3590 SCRM PL-2 SYSTEM SECURITY PLAN

Supplemental ICT SCRM Guidance: Include ICT supply chain considerations in the System Security Plan. It is also acceptable to develop a stand-alone ICT SCRM Plan for an individual system. The System Security Plan and/or ICT SCRM Plan provide inputs into ICT SCRM Plan(s) at Tier 1 and Tier 2 (Chapter 2 provides guidance on the ICT SCRM Plan.). To include ICT SCRM in the System Security Plan, controls listed in this document (NIST SP 800-161) should be used. Examples of systems that are important for ICT supply chain include acquirer's development environment, testing environment, and other systems that support acquirer's ICT supply chain activities.

TIER: 3

Control enhancements:

3603	(1)	SYSTEM SECURITY PLAN PLAN / COORDINATE WITH OTHER ORGANIZATIONAL	
3604		ENTITIES	<u>PL-2 (3)</u>
3605		Supplemental ICT SCRM Guidance: Include ICT supply chain security activities in c	oordination
3606		with other organizational entities. In this context, in addition to coordinating with	in the
3607		organization, other acquirers should coordinate with system integrators, suppliers	s, and
3608		external service providers. For example, building and operating a system requires	a significant
3609		amount of coordination and collaboration between acquirer and system integrator	personnel.

<u>PL-1</u>

PL-2

3610 3611 3612 3613 3614		This coordination and collaboration should be addressed in the System Security Plan. Sys Security Plans should also take into account that suppliers or external service providers m not be able to customize to the acquirer's requirements.	tem ay
3615	SCRM_PL-3	INFORMATION SECURITY ARCHITECTURE	<u>PL-8</u>
3616 3617 3618 3619 3620 3621	Sur def ICT sec	pplemental ICT SCRM Guidance: Security architecture is important for ICT SCRM because it interest and directs implementation of security methods, mechanisms, and capabilities to both $Γ$ supply chain infrastructure and information systems. The organization should ensure that urity architecture is well understood by system engineers and system security engineers.	the
3622 3623	<u>Cor</u>	rtrol enhancements:	
3624	(1)	INFORMATION SECURITY ARCHITECTURE SUPPLIER DIVERSITY	<u>L-8(2)</u>
3625 3626 3627 3628		<u>Supplemental ICT SCRM Guidance</u> : Include supplier diversity when building security architecture. Supplier diversity is key to providing options for addressing information sec and ICT supply chain concerns. This guidance must consider system integrators, suppliers and external service providers.	urity s,
3630 3631 3632 3633		When acquiring system integrator services, plan for potential replacement system integrator or external service providers in case a system integrator is no longer able to meet requirements (e.g., company goes out of business). For suppliers, plan for alternate source supply in case a supplier is no longer able to meet requirements.	tors es of
3634 3635 3636 3637 3638		Consider supplier diversity for off-the-shelf (commercial, government, or open source) components as well as open source acquisition security assessments. Alternatives evaluati should include, for example, feature parity, standards interfaces, commodity components, multiple delivery paths.	ion , and
3639 3640 3641		<u>TIER</u> : 2, 3	

3642 **FAMILY: PROGRAM MANAGEMENT**

3643

3644 FIPS 200 does not specific Program Management minimum security requirements.

3645

NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states that "the information security program management controls ... are typically implemented at the organization level and not directed at individual organizational information systems." Those controls apply to the entire organization (i.e., federal agency) and support the overall federal agency information security program. Program management controls support ICT SCRM risk management for the organization and provide inputs and feedback to ICT

- 3652 SCRM activities organization-wide.
- 3653

 3654
 SCRM_PM-1
 INFORMATION SECURITY PROGRAM PLAN
 PM-1

 3655
 Supplemental ICT SCRM Guidance: As a part of information security program planning, document common ICT SCRM controls. A separate ICT SCRM Plan may be developed to document
 PM-1

3657common ICT SCRM controls to address organization, program, and system-specific needs. The3658information security program plan and the associated common controls addressing Tiers 1 and 23659can provide additional foundational practices to support the ICT SCRM Plan. For Tier 3, use the3660existing system security plan to incorporate ICT SCRM controls or develop a separate ICT SCRM3661Plan. In Tier 3, ensure that the full SDLC is covered from the ICT supply chain perspective.3662

3663 <u>TIER</u>: 1,2, 3

3664 SCRM_PM-2 SENIOR INFORMATION SECURITY OFFICER

3665Supplemental ICT SCRM Guidance: Ensure that senior information security officer responsibilities3666include ICT SCRM and required cross-organizational coordination and collaboration with other3667senior personnel within the organization such as the CIO, the head of facilities/physical security,3668and the risk executive (function).

3669 3670 <u>TIER</u>: 1, 2, 3

3671 SCRM_PM-3 INFORMATION SECURITY RESOURCES

3672 Supplemental ICT SCRM Guidance: Ensure that ICT supply chain requirements are integrated into 3673 major IT investments to ensure that the funding is appropriately allocated through the capital 3674 planning and investment request process. For example, should RFID infrastructure be required to 3675 improve ICT SCRM and to ensure efficiency as well, appropriate IT investments are likely 3676 required to ensure successful planning and implementation to meet such needs. Other examples 3677 include any investment into the development or test environment in which critical components are 3678 developed and tested. In such a case, funding and resources are needed to ensure acquisition and 3679 maintenance of ICT supply chain infrastructure components that assure critical components meet 3680 their ICT SCRM requirements to support the organization mission. 3681

3682 <u>TIER</u>: 1, 2, 3

3683 SCRM_PM-4 MISSION/BUSINESS PROCESS DEFINITION

3684Supplemental ICT SCRM Guidance: When addressing mission/business process definitions, ensure3685that ICT supply chain activities are incorporated into the support processes for achieving the3686mission success. For example, a system supporting a critical mission function that has been3687designed and implemented for easy removal and replacement should a component fail may require3688the use of somewhat unreliable hardware components. An ICT supply chain activity may need to

PM-2

<u>PM-3</u>

PM-11

3689 be defined to ensure that the supplier makes component spare parts readily available if 3690 replacement is needed. 3691 3692 TIER: 1, 2, 3 3693 SCRM_PM-5 THREAT AWARENESS PROGRAM <u>PM-16</u> 3694 3695 Supplemental ICT SCRM Guidance: When addressing supply chain threat event and threat awareness, knowledge is shared while within the boundaries of organization-specific policy information 3696 sharing of threat data/information. 3697 3698 TIER: 1, 2, 3

3699			
3700	FAMILY: P	ERSONNEL SECURITY	
3701			
3702	FIPS 200 spe	cifies the Personnel Security minimum security requirement as follows:	
3703			
3704	Orga	mizations must: (i) ensure that individuals occupying positions of responsibi	litv
3705	withi	n organizations (including third-party service providers) are trustworthy an	d meet
3706	estab	blished security criteria for those positions: (ii) ensure that organizational	u meet
3707	infor	mation and information systems are protected during and after personnel ac	tions
3708	such	as terminations and transfers: and (iii) employ formal sanctions for personner de	nons
3700	failin	as to comply with organizational security policies and procedures	lei
2710	jann	g to comply with organizational security policies and procedures.	
2711	Dangann al tha	these access to fordered access ICT as males about the second by forde	
3/11	Personnel tha	it have access to rederal agency ICT supply chain should be covered by rede	rai
3/12	agency person	nnel security controls. These personnel include acquisition and contracting	
3/13	professionals	, program managers, supply chain and logistics professionals, shipping and r	receiving
3/14	staff, informa	ition technology professionals, quality professionals, mission and business o	wners,
3715	system owner	rs, and information security engineers. Organizations should also work with	system
3716	integrators an	id external service providers to ensure that they apply appropriate personnel	security
3717	controls to the	eir personnel that interact with the federal agency ICT supply chain, as appre	opriate.
3718			
3719	SCRM PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	PS-1
0,12	bornin_r b r		<u></u>
3720	Supple	emental ICT SCRM Guidance: At each tier, personnel security policy and procedures ne	ed to
3721	define	e the roles for the acquirer personnel who manage and execute ICT supply chain sec	urity
3722	activi	ties. These roles also need to state acquirer personnel responsibilities with regards to	o the
3723	relatio	onships with system integrators, suppliers, and service providers. Policies and proce	dures
3724	need t	to consider the full system development life cycle of systems, and the roles and	
3725	respon	nsibilities to address the various supply chain activities.	
3726			
3727	<u>Tier</u> 1:	: Include such roles as the risk executive, CIO, CISO, contracting, logistics,	
3728	delive	ery/receiving, acquisition security and other functions providing supporting ICT sup	ply chain
3/29	activi	ties.	
$\frac{3}{30}$	– ;),		
2722	<u>Tier</u> 23	: include such roles as program executive and individuals within the acquirer organi	zation
3732	respon	isible for program success (e.g., Program Manager and other individuals).	
3734	ΝΟΤΙ	E: Roles for system integrator, supplier, and external service provider personnel res	onsible
3735	for the	e success of the program should be included in an agreement between acquirer and t	these
3736	nartie	c success of the program should be included in an agreement between acquirer and the c (e.g., contract). This is addressed in SA-4	.11050
3737	purite		
3738	Tier 3	· Include applicable roles (e.g. system engineers or system security engineer) throug	phout the
3739	opera	tional system life cycle from requirements definition, development, test, deployment	t.
3740	maint	enance, updates, replacements, delivery/receiving, and IT.	- 7
3741			
3742	TIER:	1, 2, 3	
3743	SCRM_PS-2	ACCESS AGREEMENTS	<u>PS-6</u>
3744	Supple	emental ICT SCRM Guidance. Define and document access agreements for system inter	orators
3745	<u>exterr</u>	al service providers and suppliers. Access agreements should state the appropriate	level of
3746	acces	s by system integrators, external providers, and suppliers to the acquirer's systems a	nd
3747	should	d be consistent with the acquirer information security policy. Deploy audit mechanis	sms to

3748 3749 3750	revie agree	w, monitor, update, and track access by these parties in accordance with the access ement.	
3751 3752 3753	As p for th	ersonnel vary over time, implement a timely and rigorous personnel security update proces he access agreements.	s
3754 3755 3756	NOT requ	E: While the audit mechanisms may be implemented in $\underline{\text{Tier}}$ 3, the agreement process with ired updates should be implemented at $\underline{\text{Tier}}$ 2 as a part of program management activities.	
3757 3758 3759	NOT orga exist	'E: When ICT products and services are provided by an entity within the acquirer's nization, there may be an existing access agreement in place. When such agreement does not, it should be established.	ot
3760 3761	TIER	: 2	
3762	SCRM_PS-3	THIRD-PARTY PERSONNEL SECURITY	<u>PS-7</u>
3763 3764 3765 3766	<u>Supp</u> of th requ such	<u>lemental ICT SCRM Guidance</u> : Third-party personnel, as soon as they are engaged, become partice of the supply chain infrastructure and as such, must meet the same personnel security irements as those participating in supply chain as organizational personnel. Examples of third-party personnel can include the system integrator, supplier or external service provides the superior of the system integrator.	art ler

of the ICT supply chain infrastructure and as such, must meet the same personnel security requirements as those participating in supply chain as organizational personnel. Examples of such third-party personnel can include the system integrator, supplier or external service provider personnel used for delivery, or supplier maintenance personnel brought in to address component technical issues that were not solvable by the organization or system integrator.

<u>TIER</u>: 2

3767

3768

3769 3770

3771 3772

3773 FAMILY: PROVENANCE

3774 3775

3777

3776 Provenance is a new control family, developed specifically to address ICT supply chain concerns.

3778 All systems and components originate somewhere and may be changed throughout their 3779 existence. The recording of system and component origin along with the history of, the changes 3780 to, and the recording of who made the changes is called "provenance." Acquirers and their system 3781 integrators should maintain the provenance of systems and components under their control to 3782 understand where the systems and components originated, their change history while under 3783 government control, and who might have had an opportunity to change them. Provenance allows 3784 for all changes from the baselines of systems and components to be reported to specific stakeholders. Creating and maintaining provenance within the ICT supply chain helps 3785 3786 government agencies to achieve greater traceability in case of an adverse event and is critical for 3787 understanding and mitigating risks.

3788

3789 COTS suppliers (e.g., OEMs or authorized distributors) and external service providers may use 3790 provenance to demonstrate that the source of goods (e.g., computer hardware or software) are 3791 genuine and not counterfeit. 3792

3793 Provenance is a new control and is likely to require additional resources to implement. Although 3794 some suppliers may collect and preserve certain aspects of component provenance for their 3795 solutions, they may not be able to share such data due to varying sensitivities. Criteria for 3796 collecting and preserving component provenance may be determined based on how critical the 3797 component may be and the reason for keeping provenance, such as intellectual property.

3799 Provenance is an advanced control that requires careful consideration for the level of rigor and 3800 implementation. Agencies should assess the need for better understanding the level of effort that 3801 may be required for the acquirers' ICT supply chain to provide this data because the cost/resource 3802 may likely be reflected in the cost to the acquirer. Factors driving up cost include the collection, 3803 documentation, and the storage for such data, which may require additional protection if there are 3804 intellectual or security properties to protect. Continued conversations and strengthened 3805 relationships between the acquirer and its supply chain (e.g., integrators, suppliers, and external 3806 service providers) can help to enable a conversation for scoping the need and the supply chain 3807 assurance the data may be able to provide the organization.

3808

3821

3822

3798

3809

SCRM PV-1 PROVENANCE POLICY AND PROCEDURES

Control: The organization:

3810	Control:	The organization:
3811	a.	Develops, documents, and disseminates the provenance policy and procedures for
3812		[Assignment: organization-defined information systems, or components or the ICT
3813		supply chain infrastructure]. The policy procedures should address purpose, scope, roles,
3814		responsibilities, management commitment, coordination among organizational entities,
3815		and compliance to support managing the information and documentation describing
3816		systems/components within information systems or the ICT supply chain infrastructure;
3817		and
3818	b.	Reviews and updates the current organization or mission provenance policy and
3819		procedures every [Assignment: organization-defined frequency].
3820		

Supplemental ICT SCRM Guidance: Provenance policy can be included in the overall information security policy for organizations or conversely, can be represented by multiple program security

3823	policie	es reflecting the complex nature of federal agencies. The procedures can be established for
3824	the sec	curity program in general and for individual information systems, if needed.
3825		
3826	The pr	ovenance policy should stipulate that information related to the tracking of the metadata
3827	(analy	tics) associated with provenance of tools, data, and processes should be collected, processed,
3828	stored	, and disseminated in a controlled and protected manner equal to or greater than that of the
3829	individ	lual items for which provenance is maintained. It should include:
3830		
3831	a. Pi	cocedures for proposing, evaluating, and justifying relevant changes to system/component
3832	pı	ovenance for their impact on components, processes, systems, missions, and exposure to
3833	SU	ipply chain risks;
3834	b. A	llocation of responsibilities for the creation, maintenance, and monitoring of provenance are
3835	de	ocumented;
3836	c. M	lethods for tracking relevant purchasing, shipping, receiving, or transfer activities, including
3837	re	cords of reviewer signatures for comparison;
3838	d. Pi	cocesses for transferring provenance responsibility for systems or components between
3839	01	ganizations across physical and logical boundaries including any approvals required, e.g.,
3840	fr	om system integrator or supplier to acquirer. This may include the identification of key
3841	ре	ersonnel for the handling of information; and
3842	e. Pi	rocedures for tracking and documenting chain of custody of the system or component.
3843		
3844	<u>TIER</u> :	1, 2, 3
3845	SCRM_PV-2	TRACKING PROVENANCE AND DEVELOPING A BASELINE
3846	Contro	ol. The organization.
3847	<u>e e nu e</u> a.	Provides unique identification for the provenance document for tracking as it traverses
3848		the ICT supply chain.
3849	b	Develops methods to document monitor and maintain valid provenance baselines for
3850		systems and components of the information system or component and the ICT supply
3851		chain infrastructure:
3852	c.	Tracks, documents and disseminates to relevant supply ICT chain participants changes to
3853		the provenance:
3854	d.	Tracks individuals and processes that have access and make changes to the provenance of
3855		components, tools, data, and processes in ICT information systems or the ICT supply
3856		chain infrastructure: and
3857	е	Ensures that the provenance information and the provenance change records including to
3858	•	whom when and what is non-reputable
3859		whom, whom, and what, is non reparation.
3860	Supple	mental ICT SCRM Guidance. Tracking of provenance helps to detect unauthorized tampering
3861	and m	odification throughout the ICT supply chain, especially during repairs/refurbishing, for
3862	examn	ble by comparing the undated provenance with the original baseline provenance. Tracking of
3863	nrover	ance haselines should be performed through using configuration management mechanisms
3864	Organ	izations should ensure the timely collection of provenance and change information to
3865	provid	e as near real-time traceability as possible
3866	provid	e us neur reur time traceaonity as possible.
3867	Exam	ples include documenting monitoring and maintaining valid baselines for spare parts
3868	develo	inment changes and warehoused items throughout the SDI C
3869		priori enunges, una warenousea nems unougnout the SDLC.
3870	TIFR	2.3
3871	<u></u> .	
3872	<u>Control</u>	enhancements:
3873	(1) 74	RACKING PROVENANCE AND DEVELOPING A BASELINE / AUTOMATED AND
3874	(L) II RI	EPEATABLE PROCESSES

3875 3876 3877 3878 3879 3880 3881 3882	Supplemental ICT SCRM Guidance: Organizations should use a variety of repeatable methods for tracking changes to provenance including number and frequency of changes, reduction of "on/off" processes and procedures, and human error. These methods can be both manual and automated. For example, configuration management databases can be used for the tracking of changes to software modules, hardware components, and documentation. Related Controls: CM-3, CM-5, CM-6, CM-6 (1), CM-6 (2), CM-8, CM-8 (4), CM-8 (6), CM-8 (7), CM-8 (8), CM-8 (9), CM-9, CM-10 (1), CM-11, SA-12 (14)
3883	
3004	<u>TIER</u> : 3
3885	SCRM_PV-3 AUDITING ROLES RESPONSIBLE FOR PROVENANCE
3886 3887 3888 3889 3890 3890 3891	 <u>Control:</u> The organization: Audits and verifies provenance activities performed by [Assignment: Organization-defined individuals granted access to the creation, maintenance or monitoring of provenance]; and Protects provenance audit records.
3892	Supplemental ICT SCRM Guidance: These may include both automated and manual systems. Audits
3893	of provenance should be performed using access control and audit mechanisms.
3895 3896	<u>TIER</u> : 2, 3
3897 3898 3899	<u>RELATED CONTROLS:</u> AU -10 (1), AU -10 (2), AU -10 (3), AU -10 (4), SA-12 (11)

FAMILY: RISK ASSESSMENT

3902 3903	FIPS 200 specifies the Risk Assessment minimum security requirement as follows:
3904 3905 3906 3907 3908	Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operating of organizational information systems and the associated processing, storage, or transmission of organizational information.
3909 3910 3911	NIST SP 800-161 is about managing federal agency ICT supply chain risks and expands this control to integrate ICT supply chain risk assessment activities, as described in Chapter 2.
3912	SCRM_RA-1 RISK ASSESSMENT POLICY AND PROCEDURES <u>RA-1</u>
3913 3914 3915 3916 3917 3918 3919 3920 3921 3922 3923	<u>Supplemental ICT SCRM Guidance</u> : Risk assessment should be performed at the organization, mission/program, and system levels. The system-level risk assessment should include both the ICT supply chain infrastructure (e.g., development environments, test, delivery systems) and the information systems/components traversing the ICT supply chain. The criticality analysis will ensure that mission-critical functions and components are given higher priority due to their impact to the mission, if compromised. The policy should include ICT supply chain-relevant roles applicable to performing and coordinating risk assessments across the organization (see Chapter 2 for the listing and description of roles). Applicable roles within acquirer, system integrator, external service providers, and supplier organizations should be defined.
2024	<u>TIER</u> . 1, 2, 3
3924	SCRM_RA-2 SECURITY CATEGORIZATION RA-2
3925 3926 3927 3928 3929 3930	<u>Supplemental ICT SCRM Guidance</u> : Security categorization is critical to ICT SCRM at <u>Tiers</u> 1, 2, and 3. In addition to FIPS 199, for ICT SCRM, security categorization should be based on the criticality analysis (See Chapter 2 and SA-15[3] for a more detailed description of criticality analysis.).
2021	<u>TIER.</u> 1, 2, 3
3931	SCRM_RA-3 RISK ASSESSMENT RA-3
3932 3933 3934 3935 3936 3937	<u>Supplemental ICT SCRM Guidance</u> : Conduct risk assessment with the consideration of ICT supply chain criticality, threats, vulnerabilities, likelihood, and impact, as described in detail in Chapter 2 (Integration of ICT SCRM into Risk Management). Data to be reviewed and collected includes ICT SCRM-specific roles, processes, and results of system/component implementation and acceptance. Risk assessments should be performed at <u>Tiers 1 and 2</u> .
3938 3939 2040	Risk assessment at <u>Tier</u> 1 should be primarily a synthesis of various risk assessments performed at Tiers 2 and 3 for understanding the organizational impact.
3940 3941 3942	<u>TIER</u> : 1, 2, 3

3943			
3944	FAMILY: SYSTEM AND SERVICES ACQUISITION		
3945	FIPS 200 specifies the System and Services Acquisition minimum security requirement as		
3947	follows:		
3948	10110 ₩5.		
3949	Orga	nizations must: (i) allocate sufficient resources to adequately protect	
3950	organ	nizational information systems: (ii) employ system development life cycle	
3951	processes that incorporate information security considerations: (iii) employ software		
3952	usage	e and installation restrictions: and (iv) ensure that third-party providers employ	v
3953	adeau	and instantion restrictions, and (iv) ensure that third party providers employ ate security measures to protect information applications and/or services	r
3954	outso	urced from the organization	
3955	041501	areca from the organization.	
3956	System and se	ervices acquisition is how federal agencies acquire ICT products and services	These
3957	controls address federal agency acquisition activities, as well as the system integrator, supplier.		
3958	and external service provider activities. They address both physical and logical aspects of ICT		
3959	supply chain security, from tamper resistance and detection to SDLC and security engineering		
3960	principles ICT supply chain concerns are already prominently addressed in NIST SP 800-53		
3961	Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations		
3962	NIST SP 800-161 adds further detail and refinement to these controls		
3963	11151 51 000	To Tuddy further detail and fermement to these controls.	
20(4			
3904	SCRM_SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	<u>SA-1</u>
3965	Supple	mental ICT SCRM Guidance. Organizations should make sure that their system and servic	es
3966	acquisition policy addresses ICT SCRM including changes of location, ownership, and control.		
3967	and requirements to be communicated to the ICT supply chain. ICT supply chains evolve		
3968	continuously through mergers and acquisitions, joint ventures, and other partnership agreements.		
3969	The po	olicy should help organizations to understand these changes and use this information w	ithin
3970	their ICT SCRM activities. Organizations can obtain such status through, for example, monitoring		
39/1	public	announcements about company activities or any communications initiated by a system	1
3972	integra	ator, supplier, or external service provider.	
3974	TIER:	1, 2, 3	
3975	SCRM SA-2	ALLOCATION OF RESOURCES	SA-2
5970	boldin_bit =		0112
3976	Supplemental ICT SCRM Guidance: Organizations should include ICT supply chain requirements in		
3977	the all	ocation of resources.	
3978	TIED		
3979	<u>HER</u> :	1, 2	
3980	SCRM_SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	<u>SA-3</u>
3081	Cumala	montal ICT SCRM Quidance: Organizations should ansure that ICT supply shain acquisity	
3987	<u>Supplemental ICT SCRM Guidance</u> . Organizations should ensure that ICT supply chain security considerations are integrated into the SDLC for information systems and the ICT supply chain		
3983	infrastructure. There is a strong relationship between the SDLC activities and ICT supply chain		
3984	activities. Organizations should ensure that in addition to traditional SDLC activities, such as		
3985	requirements and design, less traditional activities are also considered in the SDLC, such as		
3986	inventory management, acquisition and procurement, and logical delivery of systems and		
3987	compo	onents. See Chapter 2.	
3988	TIED	1 2 3	
5707		1, 2, 0	
3990	SCRM_SA-4	ACQUISITION PROCESS	<u>SA-4</u>
3991	Supplemental ICT SCRM Guidance: To integrate ICT SCRM into the federal agency acquisition		
------	---		
3992	process, organizations should ensure that the following acquisition-related requirements,		
3993	descriptions, and criteria are addressed. NIST SP 800-53 Revision 4, Security and Privacy		
3994	Controls for Federal Information Systems and Organizations, control enhancements SA-4 (1), (2),		
3995	(3), (6) ad (7) provide further acquisition process mechanisms. See Appendix E for the listed and		
3996	rolled up control enhancements details if further understanding is needed.		
3997			
3998	a. Establish a baseline and tailor-able ICT supply chain security requirements to apply to all		
3999	system integrators, suppliers, and external service providers;		
4000	b. Define requirements that cover regulatory requirements (i.e., telecommunications or IT),		
4001	technical requirements, chain of custody, transparency and visibility, sharing information		
4002	on information and supply chain security incidents throughout the supply chain, rules for		
4003	disposal or retention of elements such as components, data, or intellectual property, and		
4004	other relevant requirements:		
4005	c. Define requirements for critical elements in the ICT supply chain to demonstrate a		
4006	canability to remediate emerging vulnerabilities based on open source information		
4007	gathered and other sources:		
4008	d Identify requirements for managing intellectual property ownership and responsibilities		
4009	for elements such as software code data and information the		
4010	manufacturing/development/integration environment, designs, and proprietary processes		
4011	when provided to acquirer for review or use:		
4012	e. Define requirements for the expected life span of the system and which element may be		
4013	in the critical path based on their life span. Establish a plan for any migration that can be		
4014	required in support of continued system and mission operations to ensure that the supplier		
4015	relationship can provide insights into their plans for end-of-life components. Establish a		
4016	plan for acquisition of spare parts to ensure adequate supply.		
4017	f Define requirements for an established system integrator supplier external service		
4018	provider vulnerability response process and their capability to collect inputs on		
4019	vulnerabilities from acquirers and other organizations.		
4020	σ Define requirements for functional properties and implementation information as well as		
4021	any development methods/techniques/practices which may be relevant.		
4022	h Establish and maintain verification procedures and criteria for delivered products and		
4023	services.		
4024	i. Ensure that the continuous monitoring plan includes supply chain aspects in its criteria.		
4025	Include the monitoring of functions/ports/protocols in use See Chapter 2 NIST SP 800-		
4026	161.		
4027	i Monitor system integrators suppliers and external service providers' information		
4028	systems where applicable. Monitor and evaluate the acquired work processes and work		
4029	products where applicable.		
4030	k Report information security weakness and vulnerabilities detected in the use of ICT		
4031	products or services provided within the acquirer organization and to respective OEMs		
4032	where relevant:		
4033	1. Review and confirm that the delivered product or service complies with the agreement on		
4034	an ongoing basis: and		
4035	m Articulate circumstances when secondary market components are permitted if they are		
4036	In. Antioutuce encumstances when secondary market components are permitted, if they are.		
4037	TIER: 1, 2, 3		
4038			
4039	Control enhancements:		
4040	(1) ACQUISITION PROCESS / SYSTEM / COMPONENT / SERVICE CONFIGURATIONS SA-4 (5)		
4041	Supplemental ICT SCRM Guidance: If a organization needs to purchase components, they need to		
4042	ensure that the required item meets its specification, whether purchasing directly from the		
4043	OEM, channel partners, or secondary market.		
4044	,		
4045	TIFR: 3		
	<u></u> 2		

4046	(2)	ACQUISITION PROCESS / NIAP APPROVED PROTECTION PROFILES	<u>SA-4 (7)</u>
4047		Supplemental ICT SCRM Guidance: Organizations should build produce and/or use L	S
1017		<u>Supported to the Columnation</u> of guillations should build be to the second	.5.
4040		government protection profile-certified components. NIAP certification can be ach	leved for
4049		OTS (COTS, Open Source Software [OSS], and GOTS).	
4050			
4051		<u>TIER: </u> 2, 3	
4052	SCRM_SA-5	INFORMATION SYSTEM DOCUMENTATION	<u>SA-5</u>
4053	Sup	plemental ICT SCRM Guidance: An organization should integrate ICT supply chain con	ncerns into
4054	info	ormation system documentation.	
4055		•	
4056	TIER	<u>R:</u> 3	
4057	SCRM_SA-6	SECURITY ENGINEERING PRINCIPLES	<u>SA-8</u>
4058	Sup	plemental ICT SCRM Guidance: The following security engineering techniques are help	oful in
4059	mar	naging ICT supply chain risks:	
4060			
4061		a Anticipating maximum possible ways that the ICT product or service can be n	nisused and
4061		a. Addressing maximum possible ways that the reference of service can be n abugad as to protect the product or sustain from such uses. Addressing intende	d and
4002		abused of to protect the product of system from such uses. Addressing intende	u anu
4063		unintended use scenarios in architecture and design;	
4064		b. Designing based on the organization's risk tolerance as determined by risk ass	essment
4065		(see Chapter 2);	
4066		c. Documenting acceptance of risks that are not fully mitigated through manager	nent
4067		acceptance and approval;	
4068		d. Limiting the number, size, and privileges of critical elements: using criticality	analysis
4069		will aid in determining which elements or functions are critical. See criticality	analysis in
4070		Chanter 7.	unung bib in
4071		e Using security mechanisms that help to reduce opportunities to exploit ICT su	nnly chain
4071		vulnerabilities including for example ensuration access control identity me	ppry cham
4072		wither admites, including, for example, encryption, access control, ruentity ma	nagement,
4073		and marware of tampering discovery,	
40/4		f. Designing components' elements to be difficult to disable (e.g., tramper proof	ing
4075		techniques) and, if disabled, trigger notification methods such as audit trails, ta	amper
40′/6		evidence, or alarms;	
4077		g. Designing delivery mechanisms (e.g., downloads for software) to avoid unnec	essary
4078		exposure or access to the ICT supply chain infrastructure and the systems/com	ponents
4079		traversing ICT supply chain during delivery; and	1
4080		h Designing relevant validation mechanisms to be used during implementation a	ind
4081		operation	iiiu
1082		operation.	
4082	TIC	D. 1 2 2	
4085	<u></u>	<u>K:</u> 1, 2, 3	
4084	SCRM_SA-7	EXTERNAL INFORMATION SYSTEM SERVICES	<u>SA-9</u>
4085	Con	trol enhancements:	
4086 4087	(1)	EXTERNAL INFORMATION SYSTEMS / RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS	$SA_{-}Q(1)$
4088		Supplemental ICT SCPM Guidance: See Chanter 2. Assess and Annendices F and F	<u></u>
1000		<u>oupportentiation outdated</u> . See Chapter 2, resess, and Appendices E and F.	
4089		<u>TIER</u> : 2, 3	
4001			
4091	(2)	EXTERNAL INFORMATION SYSTEMS / ESTABLISH / MAINTAIN CHAIN OF TRUST WITH	
4092		PROVIDERS	<u>SA-9 (3)</u>

4093		Supplemental ICT SCRM Guidance: Organizations should ensure that their relationsh	ips with
4094		external service providers of information systems, whether a system integrator or	an external
4095		service provider, meet the following supply chain security requirements:	
4096			
4097		a. Ensure requirements definition is complete and reviewed for accuracy and co	ompleteness
4098		including the assigning of criticality to various components as well as definit	ng
4099		operational concepts and associated scenarios for intended and unintended u	se in
4100		requirements.	
4101		b Ensure requirements are based on needs relevant compliance drivers critica	lity analysis
4102		and ICT supply chain system risk assessment:	inty unuryous,
4103		c Identify and document threats vulnerabilities and associated risks based on	likelihood of
4104		c. Identify and document tilleats, vulnerabilities, and associated fisks based on occurrence and impact to the defined system component and processes used	l across the
A105		system's SDI C.	i del'oss tile
4105		d Engure that acquirer data and information integrity, confidentiality, and avail	ability
4100		u. Ensure that acquirer data and information integrity, confidentiality, and avail	aunity
4107		requirements are defined and shared with system integrator/external service	provider as
4100		appropriate, for compliance to requirement,	•,
4109		e. Define and document consequences of noncompliance with ICT supply chai	a security
4110		requirements and information system security requirements for ICT product	and service
4111		delivery; and	
4112		f. Define requirements for service contracts completion and what defines the end	nd of the
4113		system integrator/external supplier relationship. This is important to know for	r acquirer re-
4114		compete and potential change in service provider and also to manage system	end-of-life
4115		processes.	
4116			
4117		<u>TIER:</u> 1, 2, 3	
4118 4119	(3)	EXTERNAL INFORMATION SYSTEMS / CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS	SA-9 (4)
4100			<u>511) ()</u>
4120 4121 4122		<u>Supplemental ICT SCRM Guidance</u> : Providers within the context of this enhancement include system integrators, suppliers, and external service providers.	t may
4123		<u>TIER</u> : 3	
4124	(4)	EXTERNAL INFORMATION SYSTEMS / PROCESSING, STORAGE, AND SERVICE LOCATION	<u>SA-9 (5)</u>
4125 4126 4127		Supplemental ICT SCRM Guidance: Location may belong to the system integrator or service provider. Appropriate protections should be in place to address associated risks.	external I ICT SCRM
4128 4129		<u>TIER</u> : 3	
4130	SCRM_SA-8	DEVELOPER CONFIGURATION MANAGEMENT	<u>SA-10</u>
4131 4132 4133 4134 4135	Sup sup Fec and	plemental ICT SCRM Guidance: Developer configuration management is critical for r ply chain risks for the acquirer. NIST SP 800-53 Revision 4, <i>Security and Privacy</i> <i>deral Information Systems and Organizations</i> , control enhancements SA-10 (1), (2), (6) provide specific mechanisms for implementation.	educing ICT <i>Controls for</i> (3), (4), (5),
4136	<u>TIE</u>	<u>R:</u> 2, 3	
4137	SCRM_SA-9	DEVELOPER SECURITY TESTING AND EVALUATION	<u>SA-11</u>
4138 4139 4140	<u>Sup</u> imp that	<u>plemental ICT SCRM Guidance</u> : Depending on the origins of components, this contro plemented differently. For OTS (off-the-shelf) components, the acquirer should rec t the supplier (OEM) has performed such testing as part of their quality/security pr	l may be juest proof ocesses.
4141	Wh	en the acquirer has control over the application and the development processes, th	ey should
4142	req	uire this testing as part of the SDLC. In addition to the specific types of testing act	ivities

4143 4144 4145 4146 4147 4148 4149 4150 4151 4152 4153 4154 4155	c i s e v t t C 8 c c r 1	escribed in the enhance ounterfeits, testing the tegration, and testing nould be prioritized ba fectiveness of testing ulnerability analysis, v e first step prior to en- rganizations may also 00-53 Revision 4, <i>Sectorganizations</i> , control of echanisms for implem <u>ER</u> : 1, 2, 3	cements, examples of ICT SCRM-relevant testing include test e origins of components, examining configuration settings pri- the interfaces. These types of tests may require significant re ased on the system criticality analysis (described in Chapter 2 techniques. Security testing and evaluation may require both which may take significant resource if not, focused. Criticality agaging in threat and vulnerability analysis (both described in o require third-party testing as part of developer security testing <i>urity and Privacy Controls for Federal Information Systems of</i> enhancements SA-11 (1), (2), (3), (4), (5), (6), (7), and (8) pri- nentation.	ting for or to sources and) and threat and y analysis is Chapter 2). ng. NIST SP and ovide specific
4156	SCRM_SA-	0 SUPPLY CHAIN	N PROTECTION	<u>SA-12</u>
4157 4158 4159 4160 4161 4162 4162	<u>s</u> a i 1	upplemental ICT SCRM (equisition. NIST SP 8(cluding acquisition. <u>ER</u> : 1, 2, 3	Guidance: This control is focused on ICT supply chain protect 00-161 comprehensively addresses ICT SCRM across the ent	tion during tire SDLC
4105	<u>(</u>	ontrol enhancements:		
4164	() SUPPLY CHAIN PROT	FECTION ACQUISITION STRATEGIES / TOOLS / METHODS	<u>SA-12 (1)</u>
4165 4166 4167 4168 4169 4170 4171 4172		Supplemental ICT SC strategies, tools and infrastructure and s obscuring the end-u examples include in providers to ensure detail is provided in	<u>CRM Guidance</u> : Organizations should implement various acqui d methods, to ensure the integrity and traceability of ICT sup supply systems/components. Examples of tools and methods use of components from the supplier using blind or filtered b ncentive programs to system integrators, suppliers, or externa e that they provide verification of integrity as well as traceabi n supplemental guidance in NIST 800-53 Revision 4, SA-120	sition ply chain include uys. Other al services lity. More (1).
4173		<u>TIER</u> : 1, 2, 3		
4174	() SUPPLY CHAIN PROT	FECTION / SUPPLIER REVIEWS	<u>SA-12 (2)</u>
4175 4176 4177 4178 4179 4180 4181 4182 4183 4184 4185 4186 4187		Supplemental ICT SC program to analyze relevant. This inclu services providers. integrators, supplie and visibility achie not only is there a c managing the data more detail.	<u>CRM Guidance</u> : Organizations should define and implement as e system integrator, supplier, and external services provider a udes open source software providers as well as closed source Usually an agreement is reached between organization and s ers, and/or external services providers that guides the level of evable. Organizations should be cautious scoping the review p cost for data collection, there is also a cost associated with ke for its relevance once obtained. See NIST 800-53 revision 4,	supplier review ctivities where software and ystem traceability program, as peping and SA-12(2) for
4188	() SUPPLY CHAIN PROT	FECTION / LIMITATION OF HARM	<u>SA-12 (5)</u>
4189 4190 4191 4192		Supplemental ICT SC number of supply c chain detail that ma be incorporated. Sc	<u>CRM Guidance</u> : Organizations, in order to limit harm, can enga chain activities to limit exposure of organizations operational ay be used by adversaries against the organization. Many me ome examples include avoiding purchasing custom configura	ge in a and supply chanisms can tions, or

4193 4194 4105		ensuring that a diverse set of suppliers is used to reduce the possibility of single point failure or threat. See NIST 800-53 Revision 4, SA-12(3) for more detail.	t of
4195 4196		<u>TIER</u> : 2, 3	
4197 4198	(4)	SUPPLY CHAIN PROTECTION ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE	<u>SA-12 (7)</u>
4199 4200 4201 4202 4203 4204 4205 4206 4207		<u>Supplemental ICT SCRM Guidance</u> : Organizations can use multiple methods of assessment to selecting supply chain components used in the organization's information system of supply chain infrastructure. The selection of assessment depends on the level of dept breadth of the assessment used as acceptance criteria for component selection. Organ should ensure a balance of requirements and budgets be evaluated to ensure adequate assessment measures are defined and implemented. See NIST 800-53 Revision 4, S for more detail on the types of assessments available for use prior to selection. TIER: 2, 3	ent prior or ICT th and nizations e A-12(7)
4208	(5)	SUPPLY CHAIN PROTECTION / USE OF ALL-SOURCE INTELLIGENCE	SA-12 (8)
4209 4210 4211 4212 4213		<u>Supplemental ICT SCRM Guidance</u> : Ensure that all-source threat and vulnerability inform includes any available foreign ownership and control (FOCI) data. Review this data periodically as mergers and acquisitions, if affecting a supplier, may impact both three vulnerability information and therefore SCRM.	nation
4214		<u>TIER</u> : 2, 3	
4215	(6)	SUPPLY CHAIN PROTECTION / OPERATIONS SECURITY	<u>SA-12(9)</u>
4216 4217 4218 4219 4220 4221 4222 4223 4223		Supplemental ICT SCRM Guidance: Organizations should ensure that ICT supply chain infrastructure and information systems are scoped as part of organizational OPSEC requirements. ICT supply chain criticality, threat, and vulnerability analyses can provinputs into OPSEC requirements to ensure that supply chain aspects are included for implementing requirements. See Chapter 2 regarding supply chain criticality analysis analysis, and vulnerability analysis as well as NIST 800-53 Revision 4, SA-12(9) for detail	/ide , threat more
4224	-	<u>IIER</u> . 2, 3	
4223 4226 4227 4228 4229 4230	(7)	Supplemental ICT SCRM Guidance: Examples of unauthorized modifications include the deployment of a patch or an upgrade by a maintenance team prior to staging processe verify impact of upgrade to operational environment. <u>TIER</u> : 2, 3	<u>SA-12(10)</u> es to
4231 4232	(8)	SUPPLY CHAIN PROTECTION / PENETRATION TESTING/ANALYSIS, OF ELEMENT PROCESS AND ACTORS	<u>SA-12(11)</u>
4233 4234 4235 4236 4237 4238 4239		<u>Supplemental ICT SCRM Guidance</u> : An example of validation may be the use of digital s by an OEM to prove that the software delivered is from its originating source. When signatures are used for this purpose, the organization should ensure, when receiving s software, that the signed upgrade/download was not altered. <u>TIER</u> : 2, 3	signature digital such
4240	(9)	SUPPLY CHAIN PROTECTION / INTER-ORGANIZATIONAL AGREEMENTS	<u>SA-12(12)</u>

4241	5	Supplemental ICT SCRM Guidance: Organizations should establish inter-organizational	
4242	a	agreements with its system integrators, suppliers, and external service providers to external se	nsure that
4243	8	appropriate resources and system components are available. Additional safeguards in	iclude:
4744	•		
1211		a Sumpliars particularly communicating readmans to their OEM for new prod	duate and
4245		a. Suppliers periodically communicating roadinaps to their OEM for new proc	fucts and
4240		end of life;	
4247		b. Formally reviewing and approving system integrator adding or replacing pe	rsonnel;
4248		and	
4249		c. Ensuring that external service providers provide appropriate notice regarding	ig any
4250		infrastructure changes such as any new operating system rollout, hardware	upgrades.
4251		or replacements due to field failures or data store architecture shifts from c	entral to
4252		distribute	entrui to
1252		distribute.	
4255	-		
4234	<u>-</u>	<u>TIER</u> : 2, 3	
4255	(10) <i>S</i>	SUPPLY CHAIN PROTECTION / CRITICAL INFORMATION SYSTEM COMPONENTS	<u>SA-12 (13)</u>
4256	5	Supplemental ICT SCRM Guidance: Organizations should leverage criticality analysis to	better
4257	i	dentify critical components in the ICT supply chain infrastructure as well as information	ation
4258	- -	systems/components (See Chapter 2 Criticality Analysis) After the analysis is com	nlete a
1250	5 *	number of supply chain mitigations can be put in place to ensure that appropriate pro-	piete, a
4260	1	fumber of supply chain initigations can be put in place to ensure that appropriate pro	
4200	8	are in place including multisource supply, stockplling of spare components for critic	ai
4261	C	component end of life as a shorter term fix prior to redesign, etc. Criticality analysis	provides
4262	i	nsight into where to set priorities for supply chain protection.	
4263			
4264	1	<u>[IER</u> : 2, 3	
4265	(11) <i>S</i>	SUPPLY CHAIN PROTECTION / IDENTITY AND TRACEABILITY	<u>SA-12(14)</u>
4266	<u>s</u>	Supplemental ICT SCRM Guidance: Organizations should ensure that elements, processe	es, and
4267	а	actors participating in its ICT supply chain infrastructure and managing its informati	on
4268	s	system are adequately identified and monitored. Identifying and monitoring may nee	d to be
4269	S	sconed to critical activities, thus helping to scope both cost and resources. Identificat	tion of
4270	0	components should consider inventorving any open source software (OSS) components	inte to
4270	C	components should consider inventorying any open source software (000) compone	1115 10
4271	e	insure full traceability and to ensure a cross-reference and match to known trusted	
4272	r	repositories.	
4273	_		
42/4	<u>1</u>	<u>[IER</u> : 2, 3	
4275	(12) <i>S</i>	SUPPLY CHAIN PROTECTION / PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES	<u>SA-12(15)</u>
42/6	<u> </u>	<u>Supplemental ICT SCRM Guidance</u> : Organizations should ensure that as they collect a va	ariety of
4277	e	evidence resulting from information system ICT supply chain infrastructure assessm	ent, this
4278	e	evidence is documented and integrated into the risk management process to provide	inputs to
4279	C	criticality, threat, and vulnerability analyses. This feedback provides input for ensuri	ng that
4280	I	(CT supply chain protections keep pace with the changes to the ICT supply chain	-
4281	-		
4282	г	TIER: 2.3	
.202	<u>-</u>	<u></u>	
4283	SCRM_SA-11	CRITICALICALITY ANALYSIS	<u>SA-14</u>
4284	Suppl	emental ICT SCRM Guidance: For systems in architectural design perform component	-level
4285	Secur	the systems in architectural design, perform component	iality
720J 1906	secur	ity categorization to support the system-rever criticality analysis to ensure confident	iality,
4280	integr	rity, or availability of the system and the mission it supports. See Chapter 2, Critical	ity
4287	Analy	ysis.	
4288			
4289	<u>TIER</u> :	2, 3	
4290	SCRM_SA-12	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS	<u>SA-15</u>

4291 4292 4293 4294 4295 4296 4297 4298 4299 4300 4301 4302 4303 4304	S (c c e t t a A P I a e v T	Supp dev critic envi his and oroce CT and enha will	<u>elemental ICT SCRM Guidance</u> : Organizations should ensure that ICT supply chain infrasti elopment process, standards, tools, etc.) is appropriately identified, analyzed for their cality, and appropriately protected from insider attacks. Development/maintenance ronment, test environment, and deployment environments are all critical. The tools incl control can be manual or automated. Use of automated tools aids thoroughness, efficient scale of analysis that helps address ICT supply chain risks in the development process. itionally, the output of such activities and tools provides useful inputs for ICT SCRM resses described in Chapter 2. This control has applicability to both internal federal ager supply chain infrastructure and the system integrator. NIST SP 800-53 Revision 4, <i>Sec</i> <i>Privacy Controls for Federal Information Systems and Organizations</i> , control SA-15 ancements (1), (2), (5), (6), and (7) provide further detail on mechanisms and technique aid in completion of activities described in Chapter 2.	ructure luded in ncy, ncy <i>curity</i> es that
4305 4306	<u>C</u>	Cont	rol enhancements:	
4307	(1)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS / CRITICALITY ANALYSIS	<u>SA-15 (3)</u>
4308 4309 4310 4311 4312 4313			<u>Supplemental ICT SCRM Guidance</u> : This enhancement identifies critical components with information system. This provides further detail and clarity to shape the ICT supply ch activities that need to be implemented for those critical components. This criticality an provides useful inputs into the ICT SCRM Criticality Analysis described in Chapter 2. <u>TIER</u> : 2, 3	in the ain alysis
4314 4315	(2	2)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS THREAT MODELING / VULNERABILITY ANALYSIS	<u>SA-15 (4)</u>
4316 4317 4318 4319 4320 4321 4322			Supplemental ICT SCRM Guidance: This enhancement provides threat modeling/vulnerabi analysis for the information system. This provides further detail and clarity to shape th supply chain activities that need to be implemented for those critical components. This analysis provides useful inputs into the ICT SCRM threat and vulnerability analysis de in Chapter 2. <u>TIER</u> : 2, 3	llity e ICT scribed
4323 4324	(3	3)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS REUSE OF THREAT / VULNERABILITY INFORMATION	<u>SA-15 (8)</u>
4325 4326 4327 4328 4329 4330			Supplemental ICT SCRM Guidance: This enhancement encourages developers to inform or development efforts through reuse of threat and vulnerability information produced by development efforts and lessons learned from using the tools. This provides further det clarity to shape the ICT supply chain activities. <u>TIER:</u> 3	ngoing prior ail and
4331	SCRM_SA-	-13	DEVELOPER-PROVIDED TRAINING	<u>SA-16</u>
4332 4333 4334 4335 4336 4337 4338 4339 4340 4341	<u>5</u> 1 ti i i i c c c c	Supp This hrea cont nfoi nfoi choi choi	<u>elemental ICT SCRM Guidance</u> : Developer training is critical for reducing ICT supply chai training should include ICT SCRM material to ensure that developers are aware of pot ats and vulnerabilities when developing, testing, and maintaining hardware and softwar rol includes training the individuals responsible for ICT supply chain infrastructure and rmation system developed within the infrastructure. It also includes individuals who set rmation system and ICT supply chain infrastructure components and should influence t ces made regarding those components. This control applies to both federal agency ICT n infrastructure and system integrators.	n risks. tential re. This I the lect he supply

4342	SCRM_SA-14	DEVELOPER SECURITY ARCHITECTURE AND DESIGN	<u>SA-17</u>
4343 4344			
4345	Suc	polemental ICT SCRM Guidance: This control facilitates the use of ICT SCRM informa	tion to
4346	inf	luence information system architecture, design, and component select decisions inclu	uding
4347	sec	urity functions. Examples include identifying components that compose information	ı system
4348	arc	hitecture and design, or selecting specific components to ensure availability through	multiple
4349	sun	policy of component selections. NIST SP 800-53 Revision 4. Security and Privacy C	ontrols for
4350	Fee	deral Information Systems and Organizations control enhancements SA-17 (1) and	(2) provide
4351	fur	ther details on implementing this control.	(-) Provide
4352			
4353	TIE	<u>R</u> : 2, 3	
4354	SCRM_SA-15	TAMPER RESISTANCE AND DETECTION	<u>SA-18</u>
4355	<u>Sup</u>	oplemental ICT SCRM Guidance: Organizations can use tamper-resistance techniques to	reduce
4356	cou	interfeit and tampering software and hardware in the ICT supply chain. Examples of	i tamper-
4357	res	istance techniques include retarring of chips to avoid rebranding of discarded chips,	or digital
4358	sig	natures to help non-repudiation of software.	
4359			
4300	<u> </u>	<u>R:</u> 1, 2, 3	
4362	Cor	ntrol enhancements:	
1363	(4)		CA 19(1)
4303	(1)	TAMPER RESISTANCE AND DETECTION MULTIPLE PHASES OF SDLC	<u>SA-18(1)</u>
4364		Supplemental ICT SCRM Guidance: To ensure that ICT components are not salvaged,	reclaimed,
4365		otherwise used, or previously rejected for any reason, organizations may require	
4366		documentation (certifications, packing slips, etc.) that is continuous in that it enable	es the
436/		tracing of handling and delivery back to the supplier (OEM).	
4368		TIED: 2.2	
4507		<u>- 11 - 1</u> - 2, 3	
4370	(2)	TAMPER RESISTANCE AND DETECTION / INSPECTION OF INFORMATION SYSTEMS,	G A 10 (0)
43/1		COMPONENTS, OR DEVICES	<u>SA-18 (2)</u>
4372		Supplemental ICT SCRM Guidance: Organizations should examine inconsistencies am	ong
4373		different types of tracking and labeling of delivered ICT components to identify co	ounterfeit
4374		components, for example:	
4375			
4376		a. Mismatched lot and the date code;	
4377		b. Absent or mismatched manufacturer's logo and label on the ICT component	ent and its
4378		documentation;	
4379		c. Mismatched bar code and printed part number; and	
4380		d. Inconsistent descriptions between package materials and datasheet descriptions	ptions.
4381			
4382		These comparisons can be done via visual inspections, or a variety of pattern-mate	hing
4383		techniques used in supply chain logistics.	
4384 4385		TIER: 2.3	
1505		<u>ner</u> , 2,0	
4386	(3)	TAMPER RESISTANCE AND DETECTION / RETURN POLICY	
4387		Control: The organization defines and implements a return policy [Assignment: org	anization-
4388		defined information systems, system components, or devices] [upon [Assignment:	
4389		organization-defined indicator failure against tamper resistance criteria]].	
4390			

SCRM_SA-14 DEVELOPER SECURITY ARCHITECTURE AND DESIGN

4342

4391 4392 4393 4394 4395 4396 4397 4398 4399 4400		Supplemental ICT SCRM Guidance: Organizations should implement a return policy components used in ICT supply chain infrastructure or information systems. Sho components fail tamper-resistance and detection criteria, components should be p processed for return along with appropriate documentation regarding failure. Ensidata describing the failure is send separately from the ICT component. Additiona that both failure metadata and the ICT component are adequately protected durin ensure against potential inappropriate access that impact supplier or organization confidentiality, and integrity. TIER: 2, 3	for ICT uld ICT promptly ure that the lly, ensure g return to s
4401	SCRM_SA-16	COMPONENT AUTHENTICITY	<u>SA-19</u>
4402 4403 4404 4405 4406 4407 4408	Sup cou resi sign <u>TIE</u>	<u>eplemental ICT SCRM Guidance</u> : Organizations can use tamper-resistance techniques to interfeit and tampering software and hardware in the ICT supply chain. Examples of istance techniques include retarring of chips to avoid rebranding of discarded chips natures to help non-repudiation of software. <u>R</u> : 2, 3	to reduce of tamper- s, or digital
4409	<u>Cor</u>	ntrol enhancements:	
4410	(1)	COMPONENT AUTHENTICITY ANTI-COUNTERFEIT TRAINING	<u>SA-19 (1)</u>
4411 4412 4413 4414 4415 4416		Supplemental ICT SCRM Guidance: Counterfeits are a major ICT supply chain risk. personnel to recognize and manage counterfeits in the supply chain will help imp integrity and authenticity of the organization's information systems and ICT supp infrastructure. <u>TIER</u> : 2, 3	Fraining rove bly chain
4417 4418	(2)	COMPONENT AUTHENTICITY / CONFIGURATION CONTROL FOR COMPONENT SERVICE / REPAIR	<u>SA-19 (2)</u>
4419 4420 4421 4422 4423		Supplemental ICT SCRM Guidance: Organizations may be vulnerable to ICT supply compromise through component service and repair processes. Organizations show risks associated with component repair including repair process and any replacent updates, and revisions of hardware and software components. <u>TIER</u> : 2, 3	chain 11d manage 1ents,
4424	(3)	COMPONENT AUTHENTICITY COMPONENT DISPOSAL	<u>SA-19 (3)</u>
4425 4426 4427 4428 4429 4430		 <u>Supplemental ICT SCRM Guidance</u>: Organizations should ensure that ICT componer disposed of without exposing organization, mission, or operational information, we lead to a future ICT supply chain compromise. This includes: a. Considering the transmission of sensitive data (mission, user, operational unauthorized parties or unspecified parties during disposal activities; 	its can be which may al system) to
4431 4432 4433 4434 4435 4436 4437		 b. Monitoring and documenting the chain of custody through the destruction. c. Training disposal service personnel to ensure accurate delivery of service disposal policy and procedure; the training should include OPSec and an threat briefing; and d. Implementing assessment procedures for the verification of disposal profifequency that fits organizational/mission needs. 	on process; e against opropriate cesses with a
4438		<u>TIER</u> : 2, 3	
4439	(4)	COMPONENT AUTHENTICITY ANTI-COUNTERFEIT SCANNING	<u>SA-19 (4)</u>

4440	S	upplemental ICT SCRM Guidance: Scanning for counterfeit components is an I	CT SCRM
4441	ac	ctivity. Examples of techniques to be used can include automated visual sca	nning techniques
4442	fc	r hardware and checking for digital signatures in software	0 1 1
4443		a naraware and enceking for arguar signatures in software.	
4444	<u>TI</u>	<u>ER</u> : 2, 3	
4445	SCRM_SA-17	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS	<u>SA-20</u>
4446	Supple	mental ICT SCRM Guidance: Organizations may decide, based on their ICT S	CRM risk
4447	assess	ment that they require customized development of certain critical component	ents This control
4448	nrovid	les additional guidance on this activity	
4449	provid	is additional guidance on this activity.	
4450	<u>TIER</u> :	2, 3	
4451	SCRM_SA-18	DEVELOPER SCREENING	<u>SA-21</u>
4452	Supple	mental ICT SCRM Guidance: Organizations should implement screening proce	ess for their
1152	intern	al developers. For system integrators who may be providing key developers	that address
4453		a developers. For system integrators who may be providing key developers	
4434	critica	i components, ensure that appropriate processes are in place for developer s	screening.
4433 1156		0.0	
4430 AA57	\underline{HER} .	Ζ, 3	
4458	Control	l enhancements:	
4459	(1) D	EVELOPER SCREENING/ VALIDATION OF SCREENING	SA-21 (1)
1169		EVELOTER SORIELMINO, VILLEMINON OF SORIELMINO	<u>5/1/21(1)</u>
1161	0	and a set of the set o	.1
4401	<u>51</u>	<u>upplemental ICI SCRM Guidance</u> . For developers of components, internal deve	eloper screening
4402	sr	louid be validated. Organizations may validate system integrator developer	screening
4463	th	rough requesting summary data to be provided post-validation.	
4464			
4465	т	FR: 2.3	
4467	<u></u>	<u></u> , 2, 0	
446/	SCRM_SA-19	UNSUPPORTED SYSTEM COMPONENTS	<u>SA-22</u>
4468	Supple	mental ICT SCRM Guidance: Organizations should consider acquiring directly	from qualified
4469	origin	al equipment manufacturers (OFMs) or their authorized distributors and res	ellers In the case
1109	ofuna	unperted system components, it would be useful to ansure that only outhors	and distributors
4470		upported system components, it would be useful to ensure that only authors	
44/1	with a	relationship with the supplier of the unsupported system components be us	sed.
4472		0.0	
4474	<u>11LK</u> .	2, 3	
4475	<u>Control</u>	Enhancements:	
4476 4477	(1) UL SU	NSUPPORTED SYSTEM COMPONENTS / ALTERNATIVE SOURCES FOR CONTINUED JPPORT	<u>SA-22 (1)</u>
4478 4479 4480 4481 4482 4483 4484 4485 4486 4485	<u>Si</u> sc m al di oj ac	<u>upplemental ICT SCRM Guidance</u> : Organizations should consider, when purchaburces for continued support, acquiring directly from vetted original equipmental anufacturers (OEMs) or their authorized distributors and resellers. Decision ternate sources requires input from the organization's engineering resource afferences in the alternate component options. For example, if an alternative pen source software component, what are the open source community develoceptance, and release processes? <u>ER</u> : 2, 3	asing alternate hent hs about using s regarding the e is to acquire an lopment, test,
4488			

- 4489 FAMILY: SYSTEM AND COMMUNICATION PROTECTION 4490
- 4491 FIPS 200 specifies the System and Communications Protection minimum security requirement as 4492 follows.
- 4494 Organizations must: (i) monitor, control, and protect organizational communications 4495 (i.e., information transmitted or received by organizational information systems) at the 4496 external boundaries and key internal boundaries of the information systems; and (ii) 4497 employ architectural designs, software development techniques, and systems 4498 engineering principles that promote effective information security within 4499 organizational information systems.
- 4500

4506

4493

Federal agency communication infrastructures are composed of ICT components and systems, 4501 4502 which have their own ICT, supply chains and also support federal agency ICT supply chain 4503 infrastructure. These communications connect federal agency systems with system integrator and 4504 occasionally supplier systems. Federal agency communications may be provided by system 4505 integrators or external service providers.

- 4507 SCRM SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES SC-1
- 4508 Supplemental ICT SCRM Guidance: Organizations should ensure that system and communications 4509 protection policies and procedures address ICT supply chain security perspective. The need for 4510 such protections includes defining organization-level and program-specific policies, which help to 4511 set the requirements of communication and how the infrastructure is established to meet these 4512 requirements. This can include the coordination of communications among and across multiple 4513 organizational entities within the acquirer organization as well as communications methods and 4514 infrastructure used between the acquirers and its system integrators, suppliers, and external service 4515 providers. 4516
- 4517 TIER: 1, 2, 3
- 4518 SCRM_SC-2 INFORMATION IN SHARED RESOURCES
- 4519 Supplemental ICT SCRM Guidance: The ICT supply chain security context of this control is when an 4520 organization shares information system resources with system integrators or external service 4521 providers. Sharing information in support of various supply chain activities is challenging when 4522 outsourcing key operations. Organizations are compelled to share either too much, increasing their 4523 risk, or sharing too little, making it difficult for the system integrator or external service provider 4524 to be efficient in their service delivery. Organizations should work with developers to define a 4525 structure/process of knowledge sharing including the data shared, method of sharing, and to whom 4526 (the specific roles) it is provided. Appropriate privacy and clearance requirements should be 4527 considered in the information sharing process. 4528 4529
 - TIER: 2, 3
- 4530 INFORMATION IN SHARED RESOURCES SCRM_SC-3
- 4531 Control enhancements:
- 4532 (1) DENIAL OF SERVICE PROTECTION / EXCESS CAPACITY / BANDWIDTH / REDUNDANCY SC-5 (2) 4533 Supplemental ICT SCRM Guidance: Organizations should include requirements for excess 4534 capacity, bandwidth, and redundancy into agreements with system integrators, external 4535 service providers, and suppliers of OEM equipment. 4536

SC-4

4537		<u>TIER</u> : 2	
4538	SCRM_SC-5	BOUNDARY PROTECTION	<u>SC-7</u>
4539 4540 4541 4542 4543 4544 4545 4546 4547	Sup mea sup fed and cha asso asso	oplemental ICT SCRM Guidance: Organizations should implement appropriate monitoric chanisms and processes at the boundaries between the agency systems and system i oplier, and external services provider systems. There may be multiple interfaces through agency ICT supply chain infrastructure and the SDLC. Appropriate vulnerability drisk assessment should be performed to ensure proper boundary protections for boain components as well as supply chain information flow. The vulnerability, threat, a sessment can aid in scoping boundary protection to a relevant set of criteria and help lociated costs. Further detail is provided in Chapter 2.	ng ntegrator, ughout the ty, threat, th supply and risk manage
4548 4549	<u>TIE</u>	<u>R</u> : 2	
4550	<u>Con</u>	ntrol enhancements:	
4551 4552	(1)	BOUNDARY PROTECTION / ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS	<u>SC-7 (13)</u>
4553 4554 4555 4556 4557 4558		<u>Supplemental ICT SCRM Guidance</u> : Organizations should provide separation and isola development, test, security assessment tools, and operational environments and remonitoring tools. Should a compromise or information leakage happen in any one environments, the other environments are still protected through the separation/isomechanisms or techniques.	ation of levant of the lation
4559		<u>TIER</u> : 3	
4560 4561	(2)	BOUNDARY PROTECTION / BLOCKS COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS	<u>SC-7 (19)</u>
4562 4563 4564 4565		Supplemental ICT SCRM Guidance: This control is relevant to ICT SCRM as it applie service providers. TIER: 3	s to external
4566	SCRM_SC-6	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	<u>SC-8</u>
4567 4568 4569 4570 4571 4572 4573 4574	Sup con serv rep ach the <u>TIE</u>	<u>oplemental ICT SCRM Guidance</u> : Organizations should integrate requirements for transpondentiality and integrity into agreements with system integrators, suppliers, and exvice providers. Acquirers, system integrators, suppliers, and external service provide existing security mechanisms (e.g., authentication, authorization, or encrypt nieve these requirements. The degree of protection should be based on the relationsher acquirer and the other party as well as the sensitivity of information to be transmitted. 2, 3	mission ternal ers may ton) to ip between ed.
4575	SCRM_SC-8	MOBILE CODE	<u>SC-18</u>
4576 4577 4578 4579 4580 4581	Sup app acq ema sen	oplemental ICT SCRM Guidance: Organizations should consider the use of this control is polications of mobile code within their ICT supply chain infrastructure. Examples inc quisition processes such as electronic transmission of ICT supply chain information ail), receipt of software components, logistics information management in RFID, or assors infrastructure.	n various lude (e.g., transport
4582 4583	<u>TIE</u>	<u>R</u> : 3	
4584	<u>Con</u>	ntrol enhancements:	
4585	(1)	MOBILE CODE ACQUISITION / DEVELOPMENT / USE	<u>SC-18 (2)</u>

- that is using vulnerable components. 4620 4621 TIER: 2.3 4622 SCRM_SC-12 CONCEALMENT AND MISDIRECTION 4623 Supplemental ICT SCRM Guidance: Within ICT SCRM context, concealment and misdirection 4624 techniques include the establishment of random resupply times, concealment of location, random 4625 change of fake location used and in logical space, and random change/shifting of information 4626 storage into alternate servers/storage mechanisms. 4627 4628 **TIER:** 3 4629 4630 Control enhancements: 4631 (1) CONCEALMENT AND MISDIRECTION / RANDOMNESS 4632 Supplemental ICT SCRM Guidance: Supply chain processes are necessarily structured with 4633 predictable, measurable, and repeatable processes for the purpose of efficiency and cost **CHAPTER 3**
- 4602 Supplemental ICT SCRM Guidance: Organizations should include provisions for protection of federal 4603 agency information at rest into their agreements with system integrators, suppliers, and external 4604 service providers. Conversely, organizations should also ensure that they provide appropriate 4605 protections for data at rest for the system integrator, supplier, and external service provider 4606 information, such as source code, testing data, blueprints, and intellectual property information. 4607 This control should be applied throughout the SDLC including during requirements, development, 4608 manufacturing, test, inventory management, maintenance, and disposal. 4609
- 4610 TIER: 2, 3

4611 SCRM_SC-11 HETEROGENEITY

4612 Supplemental ICT SCRM Guidance: Organizations should consider using multiple sources of supply to 4613 improve component availability and reduce ICT supply chain compromise impact. Heterogeneity 4614 techniques include use of different operating systems, virtualization techniques, and multiple 4615 sources of supply for the same function. In case of an ICT supply chain compromise, an 4616 alternative source of supply will allow the organizations to quickly switch to an alternative 4617 system/component which may not be affected by the compromise. Also, heterogeneous 4618 components decrease the attack surface by limiting the impact to only a subset of the infrastructure 4619

- Supplemental ICT SCRM Guidance: Organizations should ensure that the acquisition, development, and use of mobile code uses rigorous supply chain protection techniques. Examples include ensuring that mobile code originates from vetted sources when acquired, that vetted system integrators are used for the development of custom mobile code or prior to installing mobile code, and that verification processes are in place for acceptance criteria prior to install in order to verify the source and integrity of code. Note that mobile code can be both code for ICT supply chain infrastructure (e.g., RFID device applications) or for information systems/components.
 - **TIER:** 3
- 4595 SCRM SC-9 PLATFORM-INDEPENDENT APPLICATIONS 4596 Supplemental ICT SCRM Guidance: Organizations may consider using platform-independent 4597 applications for ICT SCRM to make the ICT SCRM application more resilient to changes in 4598 infrastructure. 4599 4600
 - TIER: 2, 3

4586

4587

4588

4589

4590

4591

4592

4593 4594

- 4601 PROTECTION OF INFORMATION AT REST SCRM_SC-10

SC-29

SC-30

SC-30(2)

<u>SC-27</u>

<u>SC-28</u>

4634 4635 4636 4637 4638 4639		reduction. This opens up the opportunity for potential breach. In order to protect a compromise, employ techniques to introduce randomness into organizational oper assets into the organization's information systems or ICT supply chain infrastructur randomly switching among several delivery organizations or routes, or changing t date of receiving supplier software updates if previously predictably scheduled).	gainst ations and .re (e.g. he time and
4640		<u>TIER</u> : 2, 3	
4641	(2)	CONCEALMENT AND MISDIRECTION / CHANGE PROCESSING / STORAGE LOCATIONS	<u>SC-30(3)</u>
4642 4643 4644 4645 4646 4647 4648 4649 4650 4651		<u>Supplemental ICT SCRM Guidance</u> : Change in processing or storage locations is a commethod of protecting downloads, deliveries, or the supply chain metadata associated Organizations should leverage such techniques to create uncertainty into the target by adversaries. Specifically in supply chain activities, efficiency and cost reduction organizations to streamline processes. By establishing a few process changes and the use of them, whether it is for receiving, acceptance testing, storage, or other su activities, will aid in reducing adversary impact. <u>TIER</u> : 2, 3	mmon ed with it. ted activities n drive randomizing upply chain
4652	(3)	CONCEALMENT AND MISDIRECTION / MISLEADING INFORMATION	<u>SC-30 (4)</u>
4653 4654 4655 4656 4657 4658 4659 4660		Supplemental ICT SCRM Guidance: Organizations can convey misleading information the concealment and misdirection efforts to protect both the ICT supply chain infr and information systems. Examples of such efforts in security include honeynets of virtualized environments. Such infrastructure implementation can be leveraged in misleading information. These may be considered advanced techniques requiring resources to effectively implement them.	n as part of astructure or conveying experienced
4661	(4)	TILL, 2, 3	RG 20 (5)
4662 4663 4664 4665 4666 4667 4668 4669 4669 4670 4671	(4)	Supplemental ICT SCRM Guidance: Organizations can employ various concealment a misdirection techniques to protect information about the information system and I chain infrastructure. For example, delivery of critical components to a central or the party depot can be used to conceal or misdirect any information regarding comport the organization using the component. Separating components from their associated information into differing physical and electronic delivery channels and obfuscating information through various techniques can be used to conceal information. The semechanism is a key approach for reducing the opportunity for potential loss of con of the component or its use, condition, etc.	nd CT supply custed third- nent use or ed ng the eparation nfidentiality
4072		<u>IIER</u> : 2, 3	
4673	SCRM_SC-14	DISTRIBUTED PROCESSING AND STORAGE	<u>SC-36</u>
4674 4675 4676 4677 4678 4679	Supp distr tech and oper	plemental ICT SCRM Guidance: Organizations should be aware that processing and stoributed both across the ICT supply chain and across the SDLC and should ensure the iniques are applied in both contexts. The following activities can use distributed prostorage: development, manufacturing, configuration management, test, maintenance rations.	brage can be hat these ocessing be, and
4680	TIEF	<u>R</u> : 2, 3	
4681	SCRM_SC-15	OUT-OF-BAND CHANNELS	<u>SC-37</u>
4682	Cont	trol enhancements:	

- 4683 (1) OUT-OF-BAND CHANNELS | ENSURE DELIVERY / TRANSMISSION SC-37(1) 4684 Supplemental ICT SCRM Guidance: Organizations should employ security safeguards to ensure 4685 that only specific individuals or information systems or ICT supply chain infrastructure 4686 receive the information about the information system or ICT supply chain infrastructure 4687 components. For example, proper credentialing and authorization documents should be 4688 requested and verified prior to the release of critical components such as custom chips or 4689 custom software or information during delivery. 4690 4691 TIER: 2, 3 4692 SCRM_SC-16 OPERATIONS SECURITY SC-38
- 4693Supplemental ICT SCRM Guidance: Organizations should ensure that appropriate ICT supply chain4694threat and vulnerability information is obtained from and provided to the operational security4695processes.46964696

4697 <u>Tier: 2, 3</u>

4698 4699

4701			
4702	FIPS 200 specifies the System and Information Integrity minimum security requirement as		
4703	follows:		
4704			
4705	Orga	anizations must: (i) identify, report, and correct information and information	
4706	syste	em flaws in a timely manner; (ii) provide protection from malicious code at	
4707	appr	ropriate locations within organizational information systems; and (iii) monitor	~
4708	infor	rmation system security alerts and advisories and take appropriate actions in	
4709	resp	onse.	
4710	1		
4711	System and i	information integrity for systems and components traversing the ICT supply cl	nain
4712	and ICT sup	ply chain infrastructure is critical for managing ICT supply chain risks. Inserti	on of
4713	malicious co	de and counterfeits are two primary examples of ICT supply chain risks both	of
4714	which can be	e at least partially addressed by deploying system and information integrity cou	ntrols
4715	Organization	s should ensure that adequate system and information integrity protections are	1015. s
4715 A716	considered a	s part of ICT supply chain risk management	,
4717		s part of fe T suppry chain fisk management.	
4718	SCRM_SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	<u>SI-1</u>
4710	0	Langel LIOT CODM On the set Organizations should include ICT SCDM considerations i	
4/19	<u>Suppi</u>	<u>iemental ICT SCRM Guidance</u> . Organizations should include ICT SCRM considerations i	II onto for
4720	empl	and information integrity policy including ensuring that program-specific requirem	nd
4722	infor	mation integrity for information systems and components and ICT supply chain infras	tructure
4723	is cri	tical for managing ICT supply chain risks. Insertion of malicious code and counterfeit	s are
4724	two r	primary examples of ICT supply chain risks, both of which can be at least partially add	dressed
4725	by de	eploying system and information integrity controls.	
4726	5		
4/2/	<u>TIER</u> :	: 1, 2, 3	
4728	SCRM_SI-2	FLAW REMEDIATION	<u>SI-2</u>
4729	<u>Suppl</u>	lemental ICT SCRM Guidance: Output of flaw remediation activities provides useful inpu	t into
4730	ICT S	SCRM processes described in Chapter 2.	
4732	TIER:	: 2, 3	
4734	Contre	ol enhancements:	
4735	(1)	FLAW REMEDIATION AUTOMATIC SOFTWARE / FIRMWARE UPDATES	<u>SI-2(5)</u>
4736	S	Supplemental ICT SCRM Guidance: Organizations should specify the various software ass	sets
4737	N N	within its infrastructure that require automated updates (both indirect and direct). This	
4738	S	specification of assets should be defined from criticality analysis results, which provid	e
4739	i	information on critical and noncritical functions and components. (See Chapter 2.) A	
4740	(centralized patch management process should be employed providing a buffer for eval	uating
4741	8	and managing updates prior to deployment. Those software assets that require direct u	pdates
4742	f	from a supplier should only accept updates originating directly from the OEM unless	
4/43	S	specifically deployed by the acquirer, such as a centralized patch management process	•
4745]	<u>TIER</u> : 2	
4746	SCRM_SI-3	INFORMATION SYSTEM MONITORING	<u>SI-4</u>

FAMILY: SYSTEM AND INFORMATION INTEGRITY

4747 4748 4749 4750 4751 4752	Su ex the of im	pplemental ICT SCRM Guidance: Information system monitoring is frequently performation service providers. Organizations should structure their service-level agreem ese providers to appropriately reflect this control. Additionally, this control include vulnerabilities resulting from past ICT supply chain compromises, such as malicing planted during software development that was set to activate after deployment.	med by ents with es monitoring ous code
4753	TIE	<u>ER</u> : 1, 2, 3	
4754 4755	<u>Co</u>	ntrol enhancements:	
4756	(1)	INFORMATION SYSTEM MONITORING / INTEGRATED SITUATIONAL AWARENESS	<u>SI-4 (17)</u>
4757 4758 4759 4760 4761 4762 4763		<u>Supplemental ICT SCRM Guidance</u> : Organizations may correlate monitoring inform that of system integrators, suppliers, and external service providers, if appropria Additionally, the results of correlating monitoring information may point to ICT compromises. <u>TIER:</u> 2, 3	nation with te. Supply chain
4764	(2)	INFORMATION SYSTEM MONITORING / INDIVIDUALS POSING GREATER RISK	<u>SI-4 (19)</u>
4765 4766 4767 4768 4769 4770		<u>Supplemental ICT SCRM Guidance:</u> Organizations may implement vetting processe that employees meet requirements to participate in the ICT supply chain infrastr developing, testing, or operating of information systems and components. The or can leverage human resource records, intelligence agencies, law enforcement or and/or other credible sources for vetting organizations' personnel.	s to ensure ructure or in organization ganizations,
4771 4771		<u>TIER</u> : 2, 3	
4772	SCRM_SI-4	SECURITY ALERTS, ADVSORIES, AND DIRECTIVES	<u>SI-5</u>
4773 4774 4775 4776	<u>Su</u> dir <u>TIE</u>	pplemental ICT SCRM Guidance: The organization should evaluate security alerts, advectives for ICT supply chain impact and follow up if needed.	visories, and
4777	SCRM_SI-5	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY (<u>SI-7</u>
4778 4779 4780 4781 4782 4783 4784 4785 4786 4787 4788 4787 4788 4789 4790 4791 4792 4793 4793	Su sy: sh sy su wa ve so co co co co me <i>Cc</i> an <u>TIE</u>	pplemental ICT SCRM Guidance: Within ICT SCRM context, this control applies to t stems and ICT supply chain infrastructure. Systemic ICT supply chain infrastructu ould be tested and verified to ensure that it remains as required so that the informa stems/components traversing through it are not impacted by unanticipated changes oply chain. Information systems and components should be tested and verified that by they are supposed to be. Applicable verification tools include digital signature of rification, acceptance testing for physical components received by an organization ftware in limited privilege environments such as sandboxes, code execution methor ntained environments to verify prior to use, and ensure if only binary or machine- de is available, it is obtained directly from the OEM or verified open source group echanisms are discussed in more detail in NIST SP 800-53 Revision 4, <i>Security an</i> <i>instrols for Federal Information Systems and Organizations</i> , <u>control enhancements</u> S d (13).	he information ire integrity tion s in the ICT t they are the or checksum i, confining ods in executable o. These <i>ad Privacy</i> I-7 (11), (12),
4/94	<u>Co</u>	ntrol enhancements:	
4795 4796	(1)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY BINARY OR MACHINE EXECUTABLE CODE	<u>SI-7(14)</u>

4797 4798 4799		<u>Supplemental ICT SCRM Guidance</u> : Organizations should obtain only binary or machine- executable code directly from the OEM or verified open source.	
4800		<u>TIER</u> : 2, 3	
4801	(2)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / CODE AUTHENTICATION	<u>' (15)</u>
4802		Supplemental ICT SCRM Guidance: Organizations should ensure that code authentication	
4803		mechanisms such as digital signatures are implemented to ensure software, firmware, and	
4804		information integrity of the ICT supply chain infrastructure and information	
4805		systems/components.	
4806		<u>TIER</u> : 3	
4807	SCRM_SI-6	INFORMATION OUTPUT HANDLING AND RETENTION	<u>SI-12</u>
4808	<u>Sup</u>	oplemental ICT SCRM Guidance: ICT SCRM concerns should be included as operational	
4809	req	uirements, especially when system integrator, supplier, and external service provider sensitiv	ve
4810	and	d proprietary information is concerned.	
4811			
4812	<u>TIER</u> : 3		

APPENDIX A

GLOSSARY

Term	Definition	Source
Access	Ability to make use of any information system resource.	NISTIR 7298
Acquirer	Stakeholder that acquires or procures a product or service.	ISO/IEC 15288, adapted
Acquisition	Includes all stages of the process of acquiring product or services, beginning with the process for determining the need for the product or services and ending with contract completion and closeout.	NIST SP 800-64, adapted
Authorization	The official management decision given by a senior organizational official to authorize operation of an information	NIST SP 800-53 Rev 4
(to operate)	system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.	
Authorization Boundary	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.	NIST SP 800-53 Rev 4
Authorizing Official (AO)	Senior federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.	CNSSI-4009
Baseline	Hardware, software, databases, and relevant documentation for an information system at a given point in time.	CNSSI-4009
Baseline Criticality	The identification of system and its components, whether physical or logical, that are considered critical to the federal agency acquirer mission. The reduced functional capability, incapacity, or destruction of such systems and components would have a significant adverse impact on federal agency operations (including mission, functions, image, or reputation), assets, individuals, other organizations, and the Nation.	Based on CNSSI- 4009
Commercial off- the-shelf (COTS)	Software and hardware that already exists and is available from commercial sources. It is also referred to as off-the-shelf.	NIST SP 800-64

Contract	A mutually binding legal relationship obligating the seller to	48 CFR
	furnish the supplies or services (including construction) and	
	the buyer to pay for them. It includes all types of	
	commitments that obligate the Government to an expenditure	
	of appropriated funds and that, except as otherwise	
	authorized, are in writing. In addition to bilateral instruments	
	contracts include (but are not limited to) awards and notices	
	of awards: ioh orders or task letters issued under basic	
	ordering agreements: letter contracts; orders, such as	
	nurchase orders, under which the contract becomes effective	
	by written accentance or performance; and bilateral contract	
	modifications. Contracts do not include grants and cooperative	
	agreements covered by 21 U.S.C. (201, et seg	
Courture et	agreements covered by 31 0.5.C. 6301, et seq.	40.050
Contract	An office that performs— (1) Assigned post-award functions	48 CFR
administration	related to the administration of contracts; and (2) Assigned	
office	pre-award functions.	
Contracting	An office that awards or executes a contract for supplies or	48 CFR
office	services and performs post-award functions not assigned to a	
	contract administration office (except as defined in 48 CFR).	
Contracting	An individual who has the authority to enter into, administer,	Federal
Officer (CO)	or terminate contracts and make related determinations and	Acquisition
	findings.	Regulation
Counterfeit	An unauthorized copy or substitute that has been identified,	18 U.S.C. § 2320
(Goods)	marked, and/or altered by a source other than the item's	
	legally authorized source and has been misrepresented to be	
	an authorized item of the legally authorized source.	
Critical	A system element that, if compromised, damaged, or failed,	
Component	could cause a mission or business failure.	
Defense-in-	A planned, systematic set of multidisciplinary activities that	CNSSI-4009
Breadth –	seek to identify, manage, and reduce risk of exploitable	
	vulnerabilities at every stage of the system, network, or sub-	
	component life cycle (system, network, or product design and	
	development; manufacturing; packaging; assembly; system	
	integration; distribution; operations; maintenance; and	
	retirement).	
Defense-in-Depth	Information security strategy integrating people, technology,	CNSSI-4009; NIST
	and operations capabilities to establish variable barriers across	SP 800-53
	multiple layers and dimensions of the organization.	Revision 4
Defensive Design	Design techniques that explicitly protect supply chain	
	elements from future attacks or adverse events. Defensive	
	design addresses the technical, behavioral, and organizational	
	activities. It is intended to create options that preserve the	
	integrity of the mission and system function and its	
	nerformance to the end user or consumer of the supply chain	
	element	

Degradation	A decline in quality or performance; the process by which the	
	decline is brought about.	
Developer	A general term that includes: (i) developers or manufacturers	NIST SP 800-53
	of information systems, system components, or information	Revision 4
	system services; (ii) systems integrators; (iii) vendors; and (iv)	
	product resellers. Development of systems, components, or	
	services can occur internally within organizations (i.e., in-	
	house development) or through external entities.	
External	A provider of external information system services to an	NIST 800-53 Rev 4
(information	organization through a variety of consumer-producer	
systems) Service	relationships including but not limited to: joint ventures;	
Provider	business partnerships; outsourcing arrangements (i.e., through	
	contracts, interagency agreements, lines of business	
	arrangements); licensing agreements; and/or supply chain	
	exchanges.	
Element	ICT system element member of a set of elements that	
	constitutes a system.	
Element	A series of operations performed in the making or treatment	
Processes	of an element: performing operations on elements/data.	
Enhanced	An overlay which adds controls, enhancements or additional	
Overlav	guidance to security control baselines in order to highlight or	
	address needs specific to the purpose of the overlay. (See	
	"overlav.")	
Federal	The Federal Acquisition Regulations System is established for	48 CFR
Acquisition	the codification and publication of uniform policies and	
Regulation (FAR)	procedures for acquisition by all executive agencies	
Federal	A standard for adoption and use by federal departments and	NIST SP 800-64
Information	agencies that has been developed within the Information	
Processing	Technology Laboratory and published by the National Institute	
Standards	of Standards and Technology, a part of the U.S. Department of	
	Commerce. A FIPS covers some topic in information	
	technology in order to achieve a common level of quality or	
	some level of interoperability.	
High Impact	The loss of confidentiality, integrity, or availability that could	FIPS 199; CNSSI-
0 1	be expected to have a severe or catastrophic adverse effect on	4009
	organizational operations, organizational assets, individuals.	
	other organizations, or the national security interests of the	
	United States: (i.e., 1) causes a severe degradation in mission	
	capability to an extent and duration that the organization is	
	able to perform its primary functions, but the effectiveness of	
	the functions is significantly reduced: 2) results in major	
	damage to organizational assets: 3) results in major	
	loss: or 4) results in severe or catastrophic harm to individuals	
	involving loss of life or serious life threatening injuries)	
ICT Supply Chain	Linked set of resources and processes between acquirers	ISO 28001
	integrators, and suppliers that begins with the design of ICT	adapted
		uuupicu

ICT SCRM Control	products and services and extends through development, sourcing, manufacturing, handling and delivery of ICT products and services to the acquirer. Note: An ICT supply chain can include vendors, manufacturing facilities, logistics providers, distribution centers, distributors, wholesalers, and other organizations involved in the manufacturing, processing, design and development, handling and delivery of the products, or service providers involved in the operation, management, and delivery of the services. Means of managing ICT supply chain risk, including policies,	ISO/IEC 27000,
	which can be of administrative, technical, management, or legal nature.	αυαρτεύ
ICT Supply Chain Compromise	An ICT supply chain compromise is an occurrence within the ICT supply chain whereby an adversary jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits. An ICT supply chain compromise can occur anywhere within the system development life cycle of the product or service. NOTE: System includes physical or electronic system or network of organizations, people, technology, activities, information, and resources. It also includes system or network components. In the context of ICT supply chain, system encompasses both the system that traverses the supply chain and organization's ICT supply chain infrastructure. NOTE: ICT supply chain is system transforming natural resources, raw materials, and components into a finished ICT product or service from supplier to the end customer. NOTE: Development life cycle in general includes design, manufacturing, production, distribution, acquisition, installation, operations, maintenance, and decommissioning.	
ICT Supply Chain Infrastructure	The integrated set of components (hardware, software and processes) within the federal agency's organizational boundary that compose the environment in which a system is developed or manufactured, tested, deployed, maintained, and retired/decommissioned.	
ICT Supply Chain Logistics	The care, housing, and movement of ICT, including materials and components (hardware and software).	
ICT Supply Chain Risk	Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.	NIST SP 800-53 Rev 3: FIPS 200, adapted

ICT Supply Chain	The process of identifying, assessing, and mitigating the risks	
Risk	associated with the global and distributed nature of ICT	
Management	product and service supply chains.	
Identity	The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity	CNSSI No. 4009
	from any other entity.	
Industrial	The portion of internal security that refers to the protection of	NISPOM, adapted
Security	industrial installations, resources, utilities, materials, and	
	classified information essential to protect from loss or damage.	
Information and	Encompasses the capture, storage, retrieval, processing,	ANSDIT, adapted
Communications	display, representation, presentation, organization,	,
Technologies	management, security, transfer, and interchange of data and	
(ICT)	information.	
Information	Measures that protect and defend information and	CNSSI No. 4009
Assurance (IA)	information systems by ensuring their availability, integrity,	
	authentication, confidentiality, and non-repudiation. These	
	measures include providing for restoration of information	
	systems by incorporating protection, detection, and reaction	
	capabilities.	
Likelihood	A weighted factor based on a subjective analysis of the	CNSSI-4009
	probability that a given threat is capable of exploiting a given	
	vulnerability	100/150 45200
Life cycle	Evolution of a system, product, service, project, or other	ISO/IEC 15288
	numan-made entity from conception through retirement.	
Low Impact	The loss of confidentiality, integrity, or availability that could	CNSSI-4009
	be expected to have a limited adverse effect on organizational	
	operations, organizational assets, individuals, other	
	States (i.e., 1) causes a degradation in mission canability to an	
	states (i.e., 1) causes a degradation in mission capability to an	
	primary functions, but the effectiveness of the functions is	
	noticeably reduced: 2) results in minor damage to	
	organizational assets: 3) results in minor financial loss: or 4)	
	results in minor harm to individuals).	
Market research	Collecting and analyzing information about capabilities within	48 CFR
	the market to satisfy agency needs.	
Moderate Impact	The loss of confidentiality, integrity, or availability that could	CNSSI-4009
	be expected to have a serious adverse effect on organizational	
	operations, organizational assets, individuals, other	
	organizations, or the national security interests of the United	
	States (i.e., 1) causes a significant degradation in mission	
	capability to an extent and duration that the organization is	
	able to perform its primary functions, but the effectiveness of	
	the functions is significantly reduced; 2) results in significant	

· · · · · · · · · · · · · · · · · · ·		
	damage to organizational assets; 3) results in significant financial loss; or 4) results in significant harm to individuals that does not involve loss of life or serious life-threatening injuries).	
Modular Contracting	Under modular contracting, an executive agency's need for a system is satisfied in successive acquisitions of interoperable increments. Each increment complies with common or commercially accepted standards applicable to information technology so that the increments are compatible with other increments of information technology comprising the system.	U.S. Code Title 41
Organizational Users	An organizational employee or an individual the organization deems to have equivalent status of an employee including, for example, contractor, guest researcher, individual detailed from another organization.	NIST SP 800-53 Revision 4
Overlay	A set of security controls, control enhancements, supplemental guidance, and other supporting information, that is intended to complement (and further refine) security control baselines to provide greater ability to appropriately tailor security requirements for specific technologies or product groups, circumstances and conditions, and/or operational environments. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.	NIST SP 800-53 Revision 4 (adapted)
Procurement	(See "acquisition.")	48 CFR
Provenance	For ICT SCRM, the records describing the possession of, and changes to, components, component processes, information, systems, organization, and organizational processes. Provenance enables all changes to the baselines of components, component processes, information, systems, organizations, and organizational processes, to be reported to specific actors, functions, locales, or activities.	
Red Team/Blue Team Approach	A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. 1. The group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team).	CNSSI 4009

	Typically, the Blue Team and its supporters must defend	
	against real or simulated attacks 1) over a significant period of	
	time, 2) in a representative operational context (e.g., as part of	
	an operational exercise) and 3) according to rules established	
	and monitored with the help of a neutral group refereeing the	
	simulation or oversise (i.e., the White Team)	
	2. The term Dive Teem is also used for defining a group of	
	2. The term blue ream is also used for defining a group of	
	individuals that conduct operational network vulnerability	
	evaluations and provide mitigation techniques to customers	
	who have a need for an independent technical review of their	
	network security posture. The Blue Team identifies security	
	threats and risks in the operating environment, and in	
	cooperation with the customer, analyzes the network	
	environment and its current state of security readiness. Based	
	on the Blue Team findings and expertise, they provide	
	recommendations that integrate into an overall community	
	security solution to increase the customer's cyber security	
	readiness posture. Often times a Blue Team is employed by	
	itself or prior to a Red Team employment to ensure that the	
	customer's networks are as secure as possible before having	
	the Red Team test the systems.	
Risk Framing	The set of assumptions, constraints, risk tolerances, and	NIST SP 800-39
	priorities/trade-offs that shape an organization's approach for	
	managing risk	
Risk	The process of managing risks to organizational operations	NIST SP 800-53;
Management	(including mission, functions, image, reputation),	NIST SP 800-53A;
	organizational assets, individuals, other organizations, and the	NIST SP 800-37,
	Nation, resulting from the operation of an information system.	adapted
	and includes: (i) the conduct of a risk assessment: (ii) the	
	implementation of a risk mitigation strategy: and (iii)	
	employment of techniques and procedures for the monitoring	
	of the security state of the information system	
Dick Mitigation	Drioritizing avaluating and implementing the appropriate rick	
RISK WILIBALION	reducing controls (countermoscures recommended from the	CN331-4009
	reducing controls/countermeasures recommended from the	
	risk management process.	
Secondary	An unofficial, unauthorized, or unintended distribution	
market	channel.	
Security Control	The set of assumptions, constraints, risk tolerances, and	NIST SP 800-53;
	priorities/trade-offs that shape an organization's approach for	800-37; 800-53A;
	managing risk	800-60; FIPS 200;
		FIPS 199; CNSSI-
		4009
Sources Sought	A synopsis posted by a government agency that states they are	FAR, Subpart 7.3
Notice	seeking possible sources for a project. It is not a solicitation for	and OMB Circular
	work, nor is it a request for proposal.	A-76

Statement of	The SOW details what the developer must do in the	NIST SP 800-64
Work (SOW)	performance of the contract. Documentation developed under	
	the contract, for example, is specified in the SOW. Security	
	assurance requirements, which detail many aspects of the	
	processes the developer follows and what evidence must be	
	provided to assure the organization that the processes have	
	been conducted correctly and completely, may also be	
	specified in the SOW.	
Supplier	Organization or individual that enters into an agreement with	ISO/IEC 15288,
	the acquirer or integrator for the supply of a product or	adapted, and
	service. This includes all suppliers in the supply chain.	adapted from
		definition of
	Includes (i) developers or manufacturers of information	"developer" from
	systems, system components, or information system services;	NIST SP 800-53
	(ii) vendors; and (iii) product resellers.	Revision 4
Supply Chain	Descriptions or depictions of supply chains, including the	
Мар	physical and logical flow of goods, information, processes, and	
	money, upstream and downstream through a supply chain.	
	They may include supply chain nodes, locations, delivery	
	paths, or transactions.	
System	A combination of interacting elements organized to achieve	ISO/IEC
,	one or more stated purposes.	15288:2008
System	Those organizations that provide customized services to the	
Integrator	federal agency acquire including custom development, test,	
0	operations, and maintenance.	
System	The justified confidence that the system functions as intended	NDIA 2008
Assurance	and is free of exploitable vulnerabilities, either intentionally or	
	unintentionally designed or inserted as part of the system at	
	any time during the life cycle.	
System	The scope of activities associated with a system, encompassing	NIST SP 800-34;
Development Life	the system's initiation, development and acquisition,	CNSSI-4009
Cycle (SDLC)	implementation, operation and maintenance, and ultimately	
	its disposal that instigates another system initiation.	
System	An organization that customizes (e.g., combines, adds,	NIST IR 7622,
Integrator	optimizes) components, systems, and corresponding	adapted
	processes. The integrator function can also be performed by	
	acquirer.	
System Owner	Person or organization having responsibility for the	CNSSI-4009
	development, procurement, integration, modification,	
	operation, and maintenance, and/or final disposition of an	
	information system.	
Threat	Any circumstance or event with the potential to adversely	NIST SP 800-53;
	impact organizational operations (including mission, functions,	NIST SP 800-53A;
	image, or reputation), organizational assets, individuals, other	NIST SP 800-27;
	organizations, or the Nation through an information system	NIST SP 800-60;
	via unauthorized access, destruction, disclosure, modification	NIST SP 800-37;
	of information, and/or denial of service.	CNSSI-4009

Threat	Process of formally evaluating the degree of threat to an	
Assessment/	information system or enterprise and describing the nature of	000_52A
Analysis	the threat	000-33A
Threat Event	An event or situation that has the potential for causing	
Threat Event	An event of situation that has the potential for causing	Rovision 1
Thurst Course	Cither (1) intent and mathed to reacted at the intentional	
Inreat Source	Either (1) Intent and method targeted at the intentional	NIST 800-30 Rev.
	exploitation of a vulnerability, or (2) a situation and method	1
	that may accidentally trigger a vulnerability.	
Threat Scenario	A set of discrete threat events, associated with a specific	NIST 800-30
	threat source or multiple threat sources, partially ordered in	Revision 1
	time.	
Trust	The confidence one element has in another, that the second	Software
	element will behave as expected.	Assurance in
		Acquisition:
		Mitigating Risks to
		the Enterprise,
		NDU, and October
		22, 2008.
Validation	Confirmation (through the provision of strong, sound,	ISO 9000
	objective evidence) that requirements for a specific intended	
	use or application have been fulfilled.	
Verification	Confirmation, through the provision of objective evidence.	CNSSI-4009, ISO
	that specified requirements have been fulfilled (e.g., an	9000. adapted
	entity's requirements have been correctly defined or an	
	entity's attributes have been correctly presented; or a	
	procedure or function performs as intended and leads to the	
	expected outcome)	
Vetted Supplier	A supplier with whom the organization is comfortable doing	
vetted Supplier	husiness. This level of comfort is usually achieved through	
	developing an organization defined set of supply shain criteria	
	developing an organization-defined set of supply chain criteria	
)/icibility/clos	And then verting suppliers against those chiefla.	
	A property of openness and accountability throughout the	ISU/IEC 2/030-3
(ransparency)	supply chain.	Draft, adapted
Vulnerability	Weakness in an information system, system security	NIST SP 800-53:
Vanierability	procedures internal controls or implementation that could be	NIST SP 800-53A
	exploited or triggered by a threat source	NIST SP 800-37
		NIST SP 800-00,
		EIDS 200
Vulnorability	Systematic examination of an information system or product	
Accossmont	to determine the adequacy of security measures, identify	CNSSI 4000
735535110111	courity deficiencies, provide data from which to prodict the	CN331-4003
	security deficiencies, provide data from which to predict the	
	effectiveness of proposed security measures, and confirm the	
	adequacy of such measures after implementation.	

APPENDIX B

ACRONYMS

AO	Authorizing Official
APT	Advanced Persistent Threat
BIA	Business Impact Analysis
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operating Officer
СРО	Chief Privacy Officer
CMVP	Cryptographic Module Validation Program
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COTS	Commercial Off-The-Shelf
СТО	Chief Technology Officer
CUI	Controlled Unclassified Information
CVE	Common Vulnerability Enumeration
CWE	Common Weakness Enumeration
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
FAR	Federal Acquisition Regulation
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act

GOTS	Government Off-The-Shelf
HAZMAT	Hazardous Materials
HR	Human Resources
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
ICT	Information and Communication Technology
IDE	Integrated Development Environment
IEC	International Electrotechnical Commission
IP	Internet Protocol/Intellectual Property
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Information Technology
ITL	Information Technology Laboratory (NIST)
NSA	National Security Agency
NASPO	North American Security Products Organization
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
NSTISSI	National Security Telecommunications and Information System Security Instruction
OEM	Original Equipment Manufacturer
OMB	Office of Management and Budget
OPSEC	Operations Security
OTS	Off-The-Shelf
O-TTPS	Open Trusted Technology Provider Standard
OWASP	Open Web Application Security Project
PACS	Physical Access Control System
PIV	Personal Identity Verification

PKI	Public Key Infrastructure
QA/QC	Quality Assurance/Quality Control
R&D	Research and Development
RMF	Risk Management Framework
SAFECode	Software Assurance Forum for Excellence in Code
SCRM	Supply Chain Risk Management
SDLC	System Development Life cycle
SLA	Service-Level Agreement
SOA	Service-Oriented Architecture
SP	Special Publication (NIST)
U.S.	United States (of America)
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

1 APPENDIX C

2 **REFERENCES**

3	
4	

5

American National Standards Institute/ North American Security Products Organization. "ANSI / NASPO Security Assurance Standard," 2008.

Boyens, Jon, Celia Paulsen, Nadya Bartol, Stephanie A. Shankles, and Rama Moorthy. *NIST IR 7622: Notional Supply Chain Risk Management Practices for Federal Information Systems.* NIST Interagency Report. Gaithersburg, MD: National Institute of Standards
 and Technology, October 2012.

10 http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf.

- 11Committee on National Security Systems. National Information Assurance (IA) Glossary, April1226, 2010. http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf.
- 13 "Common Criteria Evaluation & Validation Scheme." *National Information Assurance* 14 *Partnership.* Accessed April 18, 2014. https://www.niap 15 ccevs.org/index.cfm?&CFID=22586532&CFTOKEN=1db2682b670970ec-AC9C5029 16 EFAB-F518-8334AF0904052438.
- 17 "Federal Acquisition Regulation (FAR) Home Page." *Acquisition Central*. Accessed April 18, 2014. https://acquisition.gov/far/.
- "FIPS-200-Final-March.pdf." Accessed April 19, 2014.
 http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.
- 21 "FIPS-PUB-199-Final.pdf." Accessed February 24, 2014.
 22 http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.
- Gardner, John T., and Martha C. Cooper. "STRATEGIC SUPPLY CHAIN MAPPING
 APPROACHES." *Journal of Business Logistics* 24, no. 2 (September 1, 2003): 37–64.
 doi:10.1002/j.2158-1592.2003.tb00045.x.
- Homeland Security System Engineering and Development Institute. *Information Communication Technology (ICT) Supply Chain Exploit Frame of Reference*, March 2013.
- International Organization for Standardization. *Quality Management Systems: Requirements*, April 2013.
- 30 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46486.
- 31 ______. Specification for Security Management Systems for the Supply Chain, April 2013.
 32 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44641.
- International Organization for Standardization/International Electrotechnical Commission.
 DRAFT Information Technology Security Techniques Information Security for Supplier Relationships, April 2013.
- 36 ——. Information Technology Security Techniques Code of Practice for Information
 37 Security Controls, n.d. Accessed July 2, 2013.
- 38 ______. Information Technology Security Techniques Information Security Management
 39 Systems Overview and Vocabulary, n.d. Accessed July 2, 2013.
- 40 ——. Information Technology Security Techniques Information Security Management
 41 Systems Requirements, n.d. Accessed July 2, 2013.

42 43	
44 45	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=4356 4.
46 47	
48 49 50 51	Joint Task Force Transformation Initiative. <i>Guide for Applying the Risk Management Framework</i> <i>to Federal Information Systems: A Security Life Cycle Approach</i> . Special Publication. National Institute of Standards and Technology, February 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.
52 53 54 55	
56 57 58	 <i>NIST SP 800-30r1: Guide for Conducting Risk Assessments</i>. NIST Special Publication. National Institute of Standards and Technology, September 2012. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.
59 60 61 62	 NIST SP 800-53r4: Security and Privacy Controls for Federal Information Systems and Organizations. NIST Special Publication. National Institute of Standards and Technology, April 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
63 64 65	Minimum Security Requirements for Federal Information and Information Systems. Federal Information Processing Standard (FIPS). National Institute of Standards and Technology, March 2006.
66 67 68 69	Polydys, Mary L., and Stan Wisseman. Software Assurance in Acquisition: Mitigating Risks to the Enterprise. A Reference Guide for Security-Enhanced Software Acquisition and Outsourcing. DoD & DHS SwA Acquisition Working Group, October 22, 2008. https://buildsecurityin.us-cert.gov/sites/default/files/SwA_in_Acquisition_102208.pdf.
70 71 72	Software Assurance Forum for Excellence in Code (SAFECode). <i>The Software Supply Chain Integrity Framework, Defining Risks and Responsibilities for Securing Software in the Global Supply Chain</i> , July 21, 2009.
73 74 75 76	Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain. Software Assurance Forum for Excellence in Code (SAFECode), June 14, 2010. http://www.safecode.org/publications/SAFECode_Software_Integrity_Controls0610.pdf.
77 78 79 80	Standards for Security Categorization of Federal Information and Information Systems. Federal Information Processing Standard (FIPS) 199. National Institute of Standards and Technology, February 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB- 199-final.pdf.
81 82	The Open Group. <i>Mitigating Tainted and Counterfeit Products</i> . Open Trusted Technology Provider Standard (O-TTPS), April 2013.
83 84 85	U.S. Department of Defense. <i>Critical Program Information (CPI) Protection Within the Department of Defense</i> . Department of Defense Instruction (DoDI), December 28, 2010. http://www.dtic.mil/whs/directives/corres/pdf/520039p.pdf.
86	. National Industrial Security Program Operating Manual (NISPOM), March 28, 2013.

- 87 88 U.S. Department of Homeland Security. *DHS Sensitive Systems Policy Directive 4300A*, March 14, 2011. http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf.

89

1 APPENDIX D

2 ICT SCRM CONTROL SUMMARY

3

4 This appendix lists the ICT SCRM controls in this publication and maps them to their 5 corresponding NIST SP 800-53 Revision 4 controls as appropriate. Table 3-1 indicates those 6 controls that are defined in NIST SP 800-53Revision 4 as "High Baseline" requirements. Some 7 ICT SCRM controls were added to this baseline in order to create a baseline for ICT SCRM. 8 Additionally, because ICT SCRM is an organization-wide activity that requires selection and 9 implementation of controls at the organization, mission, and system levels (Tiers 1, 2, and 3 of 10 the organizational hierarchy according to NIST SP 800-39), Table 3-1 indicates the 11 organizational hierarchy tiers in which the controls should be implemented. The table highlights

ICT SCRM controls and enhancements not in NIST SP 800-53Revision 4 in red.

- 12 13
- 14
- 15
- 16

Table D-1:	ICT SCRM	Control	Summarv
			o a y

NIST SP 800- 161 SCRM CNTL NO.	800-53 REV. 4 CNTL NO.	CONTROL NAME	800-53 REV. 4 HIGH BASELINE	SCRM BASELINE	TIERS		
		CONTROL ENHANCEMENT NAME			1	2	3
SCRM_AC-1	AC-1	ACCESS CONTROL POLICY AND PROCEDURES	х	х	х	Х	х
SCRM_AC-2	AC-2	ACCOUNT MANAGEMENT	х	Х		Х	х
SCRM_AC-3	AC-3	ACCESS ENFORCEMENT	Х	Х		Х	х
SCRM_AC- 3(1)	AC-3 (8)	ACCESS ENFORCEMENT REVOCATION OF ACCESS AUTHORIZATIONS		х		х	x
SCRM_AC- 3(2)	AC-3 (9)	ACCESS ENFORCEMENT CONTROLLED RELEASE		Х		х	х
SCRM_AC-4	AC-4	INFORMATION FLOW ENFORCEMENT	х	Х		Х	х
SCRM_AC- 4(1)	AC-4 (6)	INFORMATION FLOW ENFORCEMENT METADATA		Х		Х	х
SCRM_AC- 4(2)	AC-4 (17)	INFORMATION FLOW ENFORCEMENT DOMAIN AUTHENTICATION				х	х
SCRM_AC- 4(3)	AC-4 (19)	INFORMATION FLOW ENFORCEMENT VALIDATION OF METADATA				х	х
SCRM_AC- 4(4)	AC-4 (21)	INFORMATION FLOW ENFORCEMENT PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS					x
SCRM_AC-5	AC-5	SEPARATION OF DUTIES	х	Х		Х	х
(SCRM_AC-6)	(AC-6)	(LEAST PRIVILEGE)	(X)	(N/A)			
SCRM_AC- 6(1)	AC-6(6)	LEAST PRIVILEGE PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS		х		х	х
SCRM_AC-7	AC-17	REMOTE ACCESS	х	Х		Х	х
SCRM_AC- 7(1)	AC-17 (6)	REMOTE ACCESS PROTECTION OF INFORMATION		Х		Х	х
SCRM_AC-8	AC-18	WIRELESS ACCESS	Х	Х	Х	Х	х
SCRM_AC-9	AC-19	ACCESS CONTROL FOR MOBILE DEVICES	х	Х		Х	х

NIST SP 800- 161 SCRM CNTL NO.	800-53 REV. 4 CNTL NO.	CONTROL NAME	800-53 REV. 4 HIGH BASELINE	SCRM	TIERS			
		CONTROL ENHANCEMENT NAME		BASELINE	1	2	3	
SCRM_AC-10	AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	Х	Х	х	х	x	
SCRM_AC- 10(1)	AC-20 (1)	USE OF EXTERNAL INFORMATION SYSTEMS LIMITS ON AUTHORIZED USE	х	Х		х	x	
SCRM_AC- 10(2)	AC-20 (3)	USE OF EXTERNAL INFORMATION SYSTEMS / NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES				x	x	
SCRM_AC-11	AC-21	INFORMATION SHARING	Х	Х	Х	Х		
SCRM_AC-12	AC-22	PUBLICLY ACCESSIBLE CONTENT	Х	Х		Х	х	
SCRM_AC-13	AC-24	ACCESS CONTROL DECISIONS			Х	Х	х	
SCRM_AT-1	AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	х	х	х	х		
(SCRM_AT-2)	(AT-3)	(ROLE-BASED SECURITY TRAINING)	(X)	(N/A)				
SCRM_AT- 2(1)	AT-3 (2)	SECURITY TRAINING PHYSICAL SECURITY CONTROLS		X		х		
SCRM_AU-1	AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	х	Х	х	х	x	
SCRM_AU-2	AU-2	AUDIT EVENTS	Х	Х	Х	Х	х	
SCRM_AU-3	AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING	х	х		х	х	
SCRM_AU- 3(2)	AU-6 (9)	AUDIT REVIEW, ANALYSIS, AND REPORTING CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES		X			x	
SCRM_AU-4	AU-10	NON-REPUDIATION	Х	X			х	
SCRM_AU- 4(1)	AU-10(1)	NON-REPUDIATION ASSOCIATION OF IDENTITIES		X		х		
SCRM_AU- 4(2)	AU-10 (2)	NON-REPUDIATION / VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY		X		х	x	
SCRM_AU- 4(3)	AU-10 (3)	NON-REPUDIATION / CHAIN OF CUSTODY		X		х	х	
SCRM_AU-5	AU-12	AUDIT GENERATION	X	X		Х	Х	
SCRM_AU-6	AU-13	MONITORING FOR INFORMATION DISCLOSURE		X		х	х	
SCRM_AU-7	AU-16	CROSS-ORGANIZATIONAL AUDITING		X		х	х	
SCRM_AU- 7(1)	AU-16 (2)	CROSS-ORGANIZATIONAL AUDITING SHARING OF AUDIT INFORMATION		X		х	x	
SCRM_CA-1	CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES	x	х	x	х	х	
SCRM_CA-2	CA-2	SECURITY ASSESSMENTS	Х	Х		х	х	

NIST SP 800- 161 SCPM	800-53 REV. 4	CONTROL NAME	800-53 REV. 4 HIGH BASELINE	SCRM	TIERS			
CNTL NO.	CNTL NO.	CONTROL ENHANCEMENT NAME		BASELINE	1	2	3	
SCRM_CA- 2(1)	CA-2 (2)	SECURITY ASSESSMENTS SPECIALIZED ASSESSMENTS	х	х			x	
SCRM_CA- 2(2)	CA-2 (3)	SECURITY ASSESSMENTS EXTERNAL ORGANIZATIONS		Х			х	
SCRM_CA-3	CA-3	SYSTEM INTERCONNECTIONS	х	х			х	
SCRM_CA- 3(1)	CA-3 (3)	SYSTEM INTERCONNECTIONS / UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS					x	
SCRM_CA- 3(2)	CA-3 (4)	SYSTEM INTERCONNECTIONS / CONNECTIONS TO PUBLIC NETWORKS					х	
SCRM_CA- 3(3)	CA-3 (5)	SYSTEM INTERCONNECTIONS / RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS	х	х			х	
SCRM_CA-4	CA-5	PLAN OF ACTION AND MILESTONES	х	Х		х	х	
SCRM_CA-5	CA-6	SECURITY AUTHORIZATION	х	Х	х	Х	х	
SCRM_CA-6	CA-7	CONTINUOUS MONITORING	х	Х	х	х	х	
SCRM_CA- 6(1)	CA-7 (3)	CONTINUOUS MONITORING TREND ANALYSES		Х			х	
SCRM_CM-1	СМ-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	Х	х	х	х	х	
SCRM_CM-2	CM-2	BASELINE CONFIGURATION	Х	Х		Х	х	
SCRM_CM- 2(1)	CM-2 (1)	BASELINE CONFIGURATION / REVIEWS AND UPDATES	х	х		Х	х	
SCRM_CM- 2(2)	CM-2 (6)	BASELINE CONFIGURATION DEVELOPMENT AND TEST ENVIRONMENTS		х		х	x	
SCRM_CM-3	СМ-3	CONFIGURATION CHANGE CONTROL	Х	Х		Х	х	
SCRM_CM-4	CM-4	SECURITY IMPACT ANALYSIS	Х	Х			х	
SCRM_CM-5	CM-5	ACCESS RESTRICTIONS FOR CHANGE	Х	Х		Х	х	
SCRM_CM- 5(1)	CM-5 (1)	ACCESS RESTRICTIONS FOR CHANGE AUTOMATED ACCESS ENFORCEMENT / AUDITING	х	х			x	
SCRM_CM- 5(2)	CM-5 (2)	ACCESS RESTRICTIONS FOR CHANGE REVIEW SYSTEM CHANGES	х	х		х	х	
SCRM_CM- 5(3)	CM-5 (3)	ACCESS RESTRICTIONS FOR CHANGE SIGNED COMPONENTS	х	х			х	
SCRM_CM- 5(4)	CM-5 (6)	ACCESS RESTRICTIONS FOR CHANGE / LIMIT LIBRARY PRIVILEGES		х			х	
SCRM_CM-6	CM-6	CONFIGURATION SETTINGS	Х	Х		Х	х	
SCRM_CM- 6(1)	CM-6 (1)	CONFIGURATION SETTINGS AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION	Х	х			х	
SCRM_CM- 6(2)	CM-6 (2)	CONFIGURATION SETTINGS RESPOND TO UNAUTHORIZED CHANGES	X	х			х	
SCRM_CM-7	CM-7	LEAST FUNCTIONALITY	Х	Х			Х	
NIST SP 800- 161 SCRM	800-53 REV. 4	CONTROL NAME	800-53 REV. 4	SCRM	TIE	FIERS		
--------------------------	---------------	--	---------------	----------	-----	-------	---	--
CNTL NO.	CNTL NO.	CONTROL ENHANCEMENT NAME	HIGH BASELINE	BASELINE	1	2	3	
SCRM_CM- 7(1)	CM-7 (4)	LEAST FUNCTIONALITY UNAUTHORIZED SOFTWARE / BLACKLISTING		х		Х	х	
SCRM_CM- 7(2)	CM-7 (5)	LEAST FUNCTIONALITY AUTHORIZED SOFTWARE / WHITELISTING	х	х			х	
SCRM_CM-8	CM-8	INFORMATION SYSTEM COMPONENT INVENTORY	х	х		Х	х	
SCRM_CM- 8(1)	CM-8 (1)	INFORMATION SYSTEM COMPONENT INVENTORY / UPDATES DURING INSTALLATIONS / REMOVALS	х	Х			х	
SCRM_CM- 8(2)	CM-8 (2)	INFORMATION SYSTEM COMPONENT INVENTORY AUTOMATED MAINTENANCE	х	х			х	
SCRM_CM- 8(3)	CM-8 (4)	INFORMATION SYSTEM COMPONENT INVENTORY ACCOUNTABILITY INFORMATION	x	х			х	
SCRM_CM- 8(4)	CM-8 (6)	INFORMATION SYSTEM COMPONENT INVENTORY ASSESSED CONFIGURATIONS / APPROVED DEVIATIONS		х			х	
SCRM_CM- 8(5)	CM-8 (7)	INFORMATION SYSTEM COMPONENT INVENTORY CENTRALIZED REPOSITORY		х			х	
SCRM_CM- 8(6)	CM-8 (8)	INFORMATION SYSTEM COMPONENT INVENTORY / AUTOMATED LOCATION TRACKING		х		х	х	
SCRM_CM- 8(7)	CM-8 (9)	INFORMATION SYSTEM COMPONENT INVENTORY / ASSIGNMENT OF COMPONENTS TO SYSTEMS		х			х	
SCRM_CM-9	СМ-9	CONFIGURATION MANAGEMENT PLAN	Х	Х		Х	Х	
SCRM_CM- 9(1)	СМ-9 (1)	CONFIGURATION MANAGEMENT PLAN ASSIGNMENT OF RESPONSIBILITY		х		Х	х	
(SCRM_CM- 10)	(CM-10)	(SOFTWARE USAGE RESTRICTIONS)	(X)	(N/A)				
SCRM_CM- 10(1)	CM-10(1)	SOFTWARE USAGE RESTRICTIONS OPEN SOURCE SOFTWARE		х		х	х	
SCRM_CM-11	CM-11	USER-INSTALLED SOFTWARE	Х	Х		Х	Х	
SCRM_CP-1	CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES	х	х	х	х	Х	
SCRM_CP-2	CP-2	CONTINGENCY PLAN	х	Х			Х	
SCRM_CP-2(1)	CP-2 (7)	CONTINGENCY PLAN / COORDINATE WITH EXTERNAL SERVICE PROVIDERS		х			х	
SCRM_CP-2(2)	CP-2 (8)	CONTINGENCY PLAN IDENTIFY CRITICAL ASSETS	х	х			х	
SCRM_CP-3	СР-6	ALTERNATE STORAGE SITE	Х	Х		Х	Х	
SCRM_CP-4	CP-7	ALTERNATE PROCESSING SITE	Х	Х		Х	Х	
(SCRM_CP-5)	(CP-8)	(TELECOMMUNICATIONS SERVICES)	(X)	(N/A)				
SCRM_CP-5(1)	CP-8 (3)	TELECOMMUNICATIONS SERVICES SEPARATION OF PRIMARY / ALTERNATE PROVIDERS	х	х		х	х	

NIST SP 800-	800-53 REV. 4	CONTROL NAME	800-53 REV. 4	SCRM	TIE	ERS	
CNTL NO.	CNTL NO.	CONTROL ENHANCEMENT NAME	HIGH BASELINE	BASELINE	1	2	3
SCRM_CP-5(2)	CP-8 (4)	TELECOMMUNICATIONS SERVICES PROVIDER CONTINGENCY PLAN	Х	х		х	х
SCRM_IA-1	IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	Х	х	х	х	Х
SCRM_IA-2	IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	х	х	х	х	х
SCRM_IA-3	IA-4	IDENTIFIER MANAGEMENT	Х	Х		Х	Х
SCRM_IA-3(1)	IA-4 (6)	IDENTIFIER MANAGEMENT / CROSS- ORGANIZATION MANAGEMENT		х	х	х	Х
SCRM_IA-4	IA-5	AUTHENTICATOR MANAGEMENT	Х	Х			Х
SCRM_IA-4(1)	IA-5 (5)	AUTHENTICATOR MANAGEMENT CHANGE AUTHENTICATORS PRIOR TO DELIVERY		х			Х
SCRM_IA-4(2)	IA-5 (9)	AUTHENTICATOR MANAGEMENT CROSS- ORGANIZATION CREDENTIAL MANAGEMENT		х			Х
SCRM_IA-5	IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	Х	х		х	Х
				-			
SCRM_IR-1	IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	х	х	Х	х	Х
(SCRM_IR-2)	(IR-4)	(INCIDENT HANDLING)	(X)	(N/A)			
SCRM_IR-2(1)	IR-4 (10)	INCIDENT HANDLING SUPPLY CHAIN COORDINATION		х		х	
(SCRM_IR-3)	(IR-6)	(INCIDENT REPORTING)	(X)	(N/A)			
SCRM_IR-3(1)	IR-6 (3)	INCIDENT REPORTING / COORDINATION WITH SUPPLY CHAIN		х			х
SCRM_IR-4	IR-9	INFORMATION SPILLAGE RESPONSE		Х			Х
SCRM_MA-1	MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES	Х	х	Х	Х	Х
(SCRM_MA- 2)	(MA-2)	(CONTROLLED MAINTENANCE)	(X)	(N/A)			
SCRM_MA- 2(1)	MA-2 (2)	CONTROLLED MAINTENANCE AUTOMATED MAINTENANCE ACTIVITIES	Х	х			х
SCRM_MA-3	MA-3	MAINTENANCE TOOLS	Х	Х		Х	Х
SCRM_MA- 3(1)	MA-3 (1)	MAINTENANCE TOOLS INSPECT TOOLS	х	х			Х
SCRM_MA- 3(2)	MA-3 (2)	MAINTENANCE TOOLS INSPECT MEDIA	Х	Х			Х
SCRM_MA- 3(3)	MA-3 (3)	MAINTENANCE TOOLS PREVENT UNAUTHORIZED REMOVAL	Х	х			Х
SCRM_MA-4	MA-4	NONLOCAL MAINTENANCE	Х	Х		Х	Х
SCRM_MA- 4(1)	MA-4 (2)	NONLOCAL MAINTENANCE / DOCUMENT NONLOCAL MAINTENANCE	Х	Х		х	х

NIST SP 800- 161 SCRM	800-53 REV. 4	CONTROL NAME	800-53 REV. 4	SCRM	TIE	TIERS		
CNTL NO.	CNTL NO.	CONTROL ENHANCEMENT NAME	HIGH BASELINE	BASELINE	1	2	3	
SCRM_MA-5	MA-5	MAINTENANCE PERSONNEL	Х	Х		Х	Х	
SCRM_MA-6	MA-6	TIMELY MAINTENANCE	Х	Х			х	
SCRM_MA-7	-	MAINTENANCE MONITORING AND INFORMATION SHARING	N/A	х			х	
SCRM_MP-1	MP-1	MEDIA PROTECTION POLICY AND PROCEDURES	Х	Х	Х	х		
SCRM_MP-2	MP-5	MEDIA TRANSPORT	Х	Х	Х	Х		
SCRM_MP-3	MP-6	MEDIA SANITIZATION	Х	Х		Х	х	
SCRM_PE-1	PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	Х	х	х	х	х	
SCRM_PE-2	PE-3	PHYSICAL ACCESS CONTROL	Х	Х		Х	Х	
SCRM_PE-2(1)	PE-3 (5)	PHYSICAL ACCESS CONTROL TAMPER PROTECTION		Х		х	Х	
SCRM_PE-3	PE-6	MONITORING PHYSICAL ACCESS	Х	Х			х	
SCRM_PE-4	PE-16	DELIVERY AND REMOVAL	Х	Х			х	
SCRM_PE-5	PE-17	ALTERNATE WORK SITE	Х	Х			Х	
SCRM_PE-6	PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS	Х	х	х	х	х	
SCRM_PE-7	PE-20	ASSET MONITORING AND TRACKING		Х		х	Х	
SCRM_PL-1	PL-1	SECURITY PLANNING POLICY AND PROCEDURES	Х	Х	х			
SCRM_PL-2	PL-2	SYSTEM SECURITY PLAN	Х	Х			х	
SCRM_PL-2(1)	PL-2 (3)	SYSTEM SECURITY PLAN / PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	х	х		x		
SCRM_PL-3	PL-8	INFORMATION SECURITY ARCHITECTURE	Х	Х		х	Х	
SCRM_PL-3(1)	PL-8 (2)	INFORMATION SECURITY ARCHITECTURE SUPPLIER DIVERSITY		х		х	х	
				-				
SCRM_PM-1	PM-1	INFORMATION SECURITY PROGRAM PLAN		Х	Х	х	Х	
SCRM_PM-2	PM-2	SENIOR INFORMATION SECURITY OFFICER		х	х	х	х	
SCRM_PM-3	PM-3	INFORMATION SECURITY RESOURCES		Х	Х	х	Х	
SCRM_PM-4	PM-11	MISSION/BUSINESS PROCESS DEFINITION		Х	Х	х	Х	
SCRM_PM-5	PM-16	THREAT AWARENESS PROGRAM		Х	Х	Х	Х	

NIST SP 800- 161 SCRM	800-53 REV. 4	CONTROL NAME	800-53 REV. 4	SCRM	TIE	ERS			
CNTL NO.	CNTL NO.	CONTROL ENHANCEMENT NAME	HIGH BASELINE	BASELINE	1	2	3		
SCRM_PS-1	PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	Х	Х	х	х	х		
SCRM_PS-2	PS-6	ACCESS AGREEMENTS	х	х		х			
SCRM_PS-3	PS-7	THIRD-PARTY PERSONNEL SECURITY	Х	Х		Х			
SCRM_PV-1	-	PROVENANCE POLICY AND PROCEDURES	N/A		Х	Х	Х		
SCRM_PV-2	-	TRACKING PROVENANCE AND DEVELOPING A BASELINE	N/A			х	x		
SCRM_PV-2 (1)	-	TRACKING PROVENANCE AND DEVELOPING A BASELINE / AUTOMATED AND REPEATABLE PROCESSES	N/A				x		
SCRM_PV-3	-	AUDITING ROLES RESPONSIBLE FOR PROVENANCE	N/A			x	X		
SCRM_RA-1	RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	Х	Х	х	х	х		
SCRM_RA-2	RA-2	SECURITY CATEGORIZATION	Х	Х	Х	Х	Х		
SCRM_RA-3	RA-3	RISK ASSESSMENT	X X		Х	Х	Х		
SCRM_SA-1	SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	Х	Х	х	х	х		
SCRM_SA-2	SA-2	ALLOCATION OF RESOURCES	Х	х	Х	Х			
SCRM_SA-3	SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	Х	х	Х	Х	Х		
SCRM_SA-4	SA-4	ACQUISITION PROCESS	Х	х	Х	Х	Х		
SCRM_SA- 4(1)	SA-4 (5)	ACQUISITION PROCESS SYSTEM / COMPONENT / SERVICE CONFIGURATIONS		Х			х		
SCRM_SA- 4(2)	SA-4 (7)	ACQUISITION PROCESS NIAP-APPROVED PROTECTION PROFILES				х	х		
SCRM_SA-5	SA-5	INFORMATION SYSTEM DOCUMENTATION	Х	Х			Х		
SCRM_SA-6	SA-8	SECURITY ENGINEERING PRINCIPLES	Х	Х	Х	Х	Х		
(SCRM_SA-7)	(SA-9)	(EXTERNAL INFORMATION SYSTEM SERVICES)	(X)	(N/A)					
SCRM_SA- 7(1)	SA-9 (1)	EXTERNAL INFORMATION SYSTEMS RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS		Х		х	х		
SCRM_SA- 7(2)	SA-9 (3)	EXTERNAL INFORMATION SYSTEMS ESTABLISH / MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS		Х	х	х	х		
SCRM_SA- 7(3)	SA-9 (4)	EXTERNAL INFORMATION SYSTEMS CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS		Х			x		
SCRM_SA- 7(4)	SA-9 (5)	EXTERNAL INFORMATION SYSTEMS PROCESSING, STORAGE, AND SERVICE LOCATION		Х			х		

NIST SP 800- 161 SCRM	800-53 REV. 4	CONTROL NAME	800-53 REV. 4	SCRM	TIE	FIERS				
CNTL NO.	CNTL NO.	CONTROL ENHANCEMENT NAME	HIGH BASELINE	BASELINE	1	2	3			
SCRM_SA-8	SA-10	DEVELOPER CONFIGURATION MANAGEMENT	х	x		x	x			
SCRM_SA-9	SA-11	DEVELOPER SECURITY TESTING AND EVALUATION	Х	Х	х	х	х			
SCRM_SA-10	SA-12	SUPPLY CHAIN PROTECTION	х	х	х	х	х			
SCRM_SA- 10(1)	SA-12 (1)	SUPPLY CHAIN PROTECTION ACQUISITION STRATEGIES / TOOLS / METHODS		х	х	х	x			
SCRM_SA- 10(2)	SA-12 (2)	SUPPLY CHAIN PROTECTION / SUPPLIER REVIEWS		Х		х	х			
SCRM_SA- 10(3)	SA-12 (5)	SUPPLY CHAIN PROTECTION LIMITATION OF HARM		Х		х	х			
SCRM_SA- 10(4)	SA-12 (7)	SUPPLY CHAIN PROTECTION / ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE		Х		х	х			
SCRM_SA- 10(5)	SA-12 (8)	SUPPLY CHAIN PROTECTION USE OF ALL- SOURCE INTELLIGENCE				х	x			
SCRM_SA- 10(6)	SA-12 (9)	SUPPLY CHAIN PROTECTION OPERATIONS SECURITY		Х		х	х			
SCRM_SA- 10(7)	SA-12 (10)	SUPPLY CHAIN PROTECTION / VALIDATE AS GENUINE AND NOT ALTERED		х		х	х			
SCRM_SA- 10(8)	SA-12 (11)	SUPPLY CHAIN PROTECTION / PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS				x	x			
SCRM_SA- 10(9)	SA-12 (12)	SUPPLY CHAIN PROTECTION / INTER- ORGANIZATIONAL AGREEMENTS		х		х	х			
SCRM_SA- 10(10)	SA-12 (13)	SUPPLY CHAIN PROTECTION / CRITICAL INFORMATION SYSTEM COMPONENTS		х		х	х			
SCRM_SA- 10(11)	SA-12 (14)	SUPPLY CHAIN PROTECTION / IDENTITY AND TRACEABILITY		Х		х	х			
SCRM_SA- 10(12)	SA-12 (15)	SUPPLY CHAIN PROTECTION PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES				х	х			
SCRM_SA-11	SA-14	CRITICALITY ANALYSIS		Х		х	х			
SCRM_SA-12	SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS	х	х		х	х			
SCRM_SA- 12(1)	SA-15 (3)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS / CRITICALITY ANALYSIS		х		х	x			
SCRM_SA- 12(2)	SA-15 (4)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS / THREAT MODELING / VULNERABILITY ANALYSIS		х		х	х			
SCRM_SA- 12(3)	SA-15 (8)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS REUSE OF THREAT / VULNERABILITY INFORMATION		х			x			
SCRM_SA-13	SA-16	DEVELOPER-PROVIDED TRAINING	Х	Х		Х	Х			
SCRM_SA-14	SA-17	DEVELOPER SECURITY ARCHITECTURE AND DESIGN	Х	Х		х	х			
SCRM_SA-15	SA-18	TAMPER RESISTANCE AND DETECTION		Х	х	Х	х			
SCRM_SA- 15(1)	SA-18 (1)	TAMPER RESISTANCE AND DETECTION MULTIPLE PHASES OF SDLC		x		х	x			

NIST SP 800- 161 SCRM	800-53 REV. 4	CONTROL NAME	800-53 REV. 4	SCRM	TIE	TIERS		
CNTL NO.	CNTL NO.	CONTROL ENHANCEMENT NAME	HIGH BASELINE	BASELINE	1	2	3	
SCRM_SA- 15(2)	SA-18 (2)	TAMPER RESISTANCE AND DETECTION / INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES		х		x	x	
SCRM_SA- 15(3)	-	TAMPER RESISTANCE AND DETECTION RETURN POLICY	N/A	Х		x	x	
SCRM_SA-16	SA-19	COMPONENT AUTHENTICITY		Х		х	х	
SCRM_SA- 16(1)	SA-19 (1)	COMPONENT AUTHENTICITY ANTI- COUNTERFEIT TRAINING		Х		х	х	
SCRM_SA- 16(2)	SA-19 (2)	COMPONENT AUTHENTICITY CONFIGURATION CONTROL FOR COMPONENT SERVICE / REPAIR		х		x	х	
SCRM_SA- 16(3)	SA-19 (3)	COMPONENT AUTHENTICITY COMPONENT DISPOSAL		Х		х	х	
SCRM_SA- 16(4)	SA-19 (4)	COMPONENT AUTHENTICITY ANTI- COUNTERFEIT SCANNING		х		х	х	
SCRM_SA-17	SA-20	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS				х	х	
SCRM_SA-18	SA-21	DEVELOPER SCREENING		Х		Х	х	
SCRM_SA- 18(1)	SA-21 (1)	DEVELOPER SCREENING / VALIDATION OF SCREENING		х		х	x	
SCRM_SA-19	SA-22	UNSUPPORTED SYSTEM COMPONENTS		х		х	х	
SCRM_SA- 19(1)	SA-22 (1)	UNSUPPORTED SYSTEM COMPONENTS ALTERNATIVE SOURCES FOR CONTINUED SUPPORT		х		х	х	

SCRM_SC-1	SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	Х	х	х	х	х
SCRM_SC-2	SC-4	INFORMATION IN SHARED RESOURCES	Х	Х		Х	х
SCRM_SC-3	SC-5	DENIAL OF SERVICE PROTECTION	Х	Х		Х	
SCRM_SC-3(1)	SC-5 (2)	DENIAL OF SERVICE PROTECTION / EXCESS CAPACITY / BANDWIDTH / REDUNDANCY				х	
SCRM_SC-4	SC-7	BOUNDARY PROTECTION	х	Х		Х	
SCRM_SC-4(1)	SC-7 (13)	BOUNDARY PROTECTION / ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS					х
SCRM_SC-4(2)	SC-7 (19)	BOUNDARY PROTECTION BLOCKS COMMUNICATION FROM NON- ORGANIZATIONALLY CONFIGURED HOSTS					x
SCRM_SC-5	SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	х	х		Х	х
SCRM_SC-6	SC-18	MOBILE CODE	х	Х			х
SCRM_SC-6(1)	SC-18 (2)	MOBILE CODE ACQUISITION / DEVELOPMENT / USE		х			х
SCRM_SC-7	SC-27	PLATFORM-INDEPENDENT APPLICATIONS				Х	x
SCRM_SC-8	SC-28	PROTECTION OF INFORMATION AT REST	Х	Х		Х	Х
SCRM_SC-9	SC-29	HETEROGENEITY		Х		х	х

NIST SP 800- 161 SCPM	800-53 REV. 4	CONTROL NAME	800-53 REV. 4	SCRM	TIE	FIERS		
CNTL NO.	CNTL NO.	CONTROL ENHANCEMENT NAME	HIGH BASELINE	BASELINE	1	2	3	
SCRM_SC-10	SC-30	CONCEALMENT AND MISDIRECTION					х	
SCRM_SC- 10(1)	SC-30 (2)	CONCEALMENT AND MISDIRECTION RANDOMNESS				х	х	
SCRM_SC- 10(2)	SC-30 (3)	CONCEALMENT AND MISDIRECTION / CHANGE PROCESSING / STORAGE LOCATIONS				х	х	
SCRM_SC- 10(3)	SC-30 (4)	CONCEALMENT AND MISDIRECTION MISLEADING INFORMATION				x	x	
SCRM_SC- 10(4)	SC-30 (5)	CONCEALMENT AND MISDIRECTION / CONCEALMENT OF SYSTEM COMPONENTS				х	x	
SCRM_SC-11	SC-36	DISTRIBUTED PROCESSING AND STORAGE				х	х	
(SCRM_SC- 12)	(SC-37)	(OUT-OF-BAND CHANNELS)		(N/A)				
SCRM_SC- 12(1)	SC-37 (1)	OUT-OF-BAND CHANNELS ENSURE DELIVERY / TRANSMISSION				х	х	
SCRM_SC-13	SC-38	OPERATIONS SECURITY		Х		х	х	
SCRM_SI-1	SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	х	х	х	x	x	
SCRM_SI-2	SI-2	FLAW REMEDIATION	Х	Х		х	х	
SCRM_SC-2(1)	SI-2 (5)	FLAW REMEDIATION AUTOMATIC SOFTWARE / FIRMWARE UPDATES		х		x		
SCRM_SI-3	SI-4	INFORMATION SYSTEM MONITORING	Х	Х	х	х	Х	
SCRM_SI-3(1)	SI-4 (17)	INFORMATION SYSTEM MONITORING INTEGRATED SITUATIONAL AWARENESS				х	х	
SCRM_SI-3(2)	SI-4 (19)	INFORMATION SYSTEM MONITORING INDIVIDUALS POSING GREATER RISK		х		х	x	
SCRM_SI-4	SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	х	Х		х	х	
SCRM_SI-5	SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	х	Х		х	х	
SCRM_SI-5(1)	SI-7 (14)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / BINARY OR MACHINE EXECUTABLE CODE	Х	х		х	х	
SCRM_SI-5(2)	SI-7 (15)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / CODE AUTHENTICATION		х			х	
SCRM_SI-6	SI-12	INFORMATION HANDLING AND RETENTION	Х	Х			х	

2 NIST SP 800-53 ICT SCRM-RELEVANT CONTROLS

3

12

4 This appendix provides a list of the information security controls from NIST Special Publication 5 800-53 Revision 4 that are directly relevant and apply to supply chain security. The list is 6 categorized alphabetically by existing information security control families. The specific controls 7 within those families are ordered numerically. Note: Control families Program Management (PM) 8 and Planning (PL) are listed separately, as they are considered an oversight activity and ordered 9 as such in NIST SP 800-53 Revision 4. The controls in this publication are linked to the Chapter 10 3 supply chain risk management (SCRM) guidance to provide an expanded description and frame 11 of reference to the SCRM guidance.

13 FAMILY: ACCESS CONTROL

14	AC-1	ACCES	S CONTROL POLICY AND PRO	CEDURES	[Back to SCRM Control]
15		Control:	The organization:		
16 17		a. De rol	evelops, documents, and disservelops]:	minates to [Assignment: organi	zation-defined personnel or
18 19 20		1.	An access control policy tha management commitment, compliance; and	t addresses purpose, scope, ro coordination among organizat	les, responsibilities, ional entities, and
21 22		2.	Procedures to facilitate the access controls; and	implementation of the access	control policy and associated
23		b. Re	eviews and updates the current	•	
24		1.	Access control policy [Assig	nment: organization-defined fr	requency]; and
25		2.	Access control procedures [Assignment: organization-defi	ned frequency].
26 27 28 29 30 31 32 33 34 35 36		Supplem effectiv Policy policies level m be inclu- be repr proced system policy a <u>Control</u>	nental Guidance: This control ad we implementation of selected and procedures reflect applica s, standards, and guidance. Se hay make the need for system- uded as part of the general infe- resented by multiple policies re- ures can be established for the s, if needed. The organization and procedures. Related contre <u>Enhancements:</u> None.	ddresses the establishment of p security controls and control en ble federal laws, Executive Ore curity program policies and pro- specific policies and procedure ormation security policy for org effecting the complex nature of security program in general ar al risk management strategy is ol: PM-9.	blicy and procedures for the nhancements in the AC family. ders, directives, regulations, ocedures at the organization s unnecessary. The policy can ganizations or conversely, can 'certain organizations. The id for particular information a key factor in establishing
37		Referen	ces: NIST Special Publication	ns 800-12, 800-100.	
38		Priority a	and Baseline Allocation:		
20		P1	LOW AC-1	MOD AC-1	HIGH AC-1

39

[Back to SCRM Control]

41	<u>Con</u>	trol: The organization:
42 43 44	a.	Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];
45	b.	Assigns account managers for information system accounts;
46	c.	Establishes conditions for group and role membership;
47 48	d.	Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
49 50	e.	Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
51 52	f.	Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
53	g.	Monitors the use of, information system accounts;
54	h.	Notifies account managers:
55		1. When accounts are no longer required;
56		2. When users are terminated or transferred; and
57		3. When individual information system usage or need-to-know changes;
58	i.	Authorizes access to the information system based on:
59		1. A valid access authorization;
60		2. Intended system usage; and
61 62		 Other attributes as required by the organization or associated missions/business functions;
63 64	j.	Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and
65 66	k.	Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85	Sup grou serv org syst con acc attri auth orig con acc gran the resp	<u>plemental Guidance</u> : Information system account types include, for example, individual, shared, up, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and vice. Some of the account management requirements listed above can be implemented by anizational information systems. The identification of authorized users of the information tem and the specification of access privileges reflects the requirements in other security trols in the security plan. Users requiring administrative privileges on information system ounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, sion/business owner, or chief information security officer) responsible for approving such ounts and privileged access. Organizations may choose to define access privileges or other ibutes by account, by type of account, or a combination of both. Other attributes required for norizing access include, for example, restrictions on time-of-day, day-of-week, and point-of- gin. In defining other account attributes, organizations consider system-related requirements , scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time e differences, customer requirements, remote access to support travel requirements). Failure to sider these factors could affect information system availability. Temporary and emergency ounts are accounts intended for short-term use. Organizations establish temporary accounts as a to f normal account activation procedures when there is a need for short-term accounts without demand for immediacy in account activation. Organizations establish emergency accounts in ponse to crisis situations and with the need for rapid account activation. Therefore, emergency
86	acc	ount activation may bypass normal account authorization processes. Emergency and temporary

87 accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used 88 for special tasks defined by organizations or when network resources are unavailable). Such 89 accounts remain available and are not subject to automatic disabling or removal dates. Conditions 90 for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or 91 temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. 92 Some types of information system accounts may require specialized training. Relate control: AC-93 3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-94 6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13. 95 References: None. 96 Priority and Baseline Allocation: P1 LOW AC-2 MOD AC-2 (1) (2) (3) (4) HIGH AC-2 (1) (2) (3) (4) (5) (12) (13) 97 98 AC-3 ACCESS ENFORCEMENT [Back to SCRM Control]

- 100Control: The information system enforces approved authorizations for logical access to information101and system resources in accordance with applicable access control policies.
- 102 Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, 103 attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access 104 control matrices, cryptography) control access between active entities or subjects (i.e., users or 105 processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, 106 domains) in information systems. In addition to enforcing authorized access at the information 107 system level and recognizing that information systems can host many applications and services in 108 support of organizational missions and business operations, access enforcement mechanisms can 109 also be employed at the application and service level to provide increased information security. 110 Relate control: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, 111 AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3.
- 112
113AC-3 (8)ACCESS ENFORCEMENT / REVOCATION OF ACCESS
AUTHORIZATIONS[BACK TO SCRM CONTROL]114The information system enforces the revocation of access authorizations resulting from

immediate revocation is necessary.

116organization-defined rules governing the timing of revocations of access authorizations].117118119120120121121122123123123126127128129120120121121122123123123124125126127128129120121121122123123124125126127128129120121121122123123124125125126127128129129120121121122123123124125125126127128129129120121121122123123124125126127128129129120121121122123123124125126<tr

changes to the security attributes of subjects and objects based on [Assignment:

 126
 AC-3 (9)
 ACCESS ENFORCEMENT / CONTROLLED RELEASE
 [BACK TO SCRM CONTROL]

 127
 The information system does not release information outside of the established system boundary unless:
 128

 129
 a. The receiving [Assignment: organization-defined information system or system component] provides [Assignment: organization-defined security safeguards]; and

99

115

124

b. ([Assignment: organization-defined security safeguards] are used to validate the appropriateness of the information designated for release.

134 Supplemental Guidance: Information systems can only protect organizational information within the 135 confines of established system boundaries. Additional security safeguards may be needed to 136 ensure that such information is adequately protected once it is passed beyond the established 137 information system boundaries. Examples of information leaving the system boundary include 138 transmitting information to an external information system or printing the information on one of 139 its printers. In cases where the information system is unable to make a determination of the 140 adequacy of the protections provided by entities outside its boundary, as a mitigating control, 141 organizations determine procedurally whether the external information systems are providing 142 adequate security. The means used to determine the adequacy of the security provided by external 143 information systems include, for example, conducting inspections or periodic testing, establishing 144 agreements between the organization and its counterpart organizations, or some other process. The 145 means used by external entities to protect the information received need not be the same as those 146 used by the organization, but the means employed are sufficient to provide consistent adjudication 147 of the security policy to protect the information. This control enhancement requires information 148 systems to employ technical or procedural means to validate the information prior to releasing it to 149 external systems. For example, if the information system passes information to another system 150 controlled by another organization, technical means are employed to validate that the security 151 attributes associated with the exported information are appropriate for the receiving system. 152 Alternatively, if the information system passes information to a printer in organization-controlled 153 space, procedural means can be employed to ensure that only appropriately authorized individuals 154 gain access to the printer. This control enhancement is most applicable when there is some policy 155 mandate (e.g., law, Executive Order, directive, or regulation) that establishes policy regarding 156 access to the information, and that policy applies beyond the realm of a particular information 157 system or organization. 158

159 <u>References</u>: None.

Priority and Baseline Allocation:

P1	LOW AC-3	MOD AC-3	HIGH AC-3
----	----------	----------	-----------

162

164

161

131

132

133

163	AC-4	INFORMATION FLOW ENFORCEMENT

[Back to SCRM Control]

165Control: The information system enforces approved authorizations for controlling the flow of166information within the system and between interconnected systems based on [Assignment:167organization-defined information flow control policies].

168 Supplemental Guidance: Information flow control regulates where information is allowed to 169 travel within an information system and between information systems (as opposed to who is 170 allowed to access the information) and without explicit regard to subsequent accesses to that 171 information. Flow control restrictions include, for example, keeping export-controlled information 172 from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from 173 within the organization, restricting web requests to the Internet that are not from the internal web 174 proxy server, and limiting information transfers between organizations based on data structures 175 and content. Transferring information between information systems representing different security 176 domains with different security policies introduces risk that such transfers violate one or more 177 domain security policies. In such situations, information owners/stewards provide guidance at 178 designated policy enforcement points between interconnected systems. Organizations consider 179 mandating specific architectural solutions when required to enforce specific security policies.

180 181 182 183 184	Er sy in att	forcement includes, for example: (i) prohibiting information transfer stems (i.e., allowing access only); (ii) employing hardware mechanis formation flows; and (iii) implementing trustworthy regarding mecha ributes and security labels.	rs between interconnected sms to enforce one-way anisms to reassign security
185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201	On to in co oc tu sy fil do m flo ne en gu te SO	ganizations commonly employ information flow control policies and control the flow of information between designated sources and dest dividuals, and devices) within information systems and between inter- ntrol is based on the characteristics of the information and/or the info- curs, for example, in boundary protection devices (e.g., gateways, ro- nnels, firewalls) that employ rule sets or establish configuration settin- stem services, provide a packet-filtering capability based on header i tering capability based on message content (e.g., implementing key w cument characteristics). Organizations also consider the trustworthir echanisms (i.e., hardware, firmware, and software components) that we enforcement. Control enhancements 3 through 22 primarily addre eds which focus on more advanced filtering techniques, in-depth ana forcement mechanisms implemented in cross-domain products, for e ards. Such capabilities are generally not available in commercial offi- chnology products. Related controls: AC-3, AC-17, AC-19, AC-21, 6 2-5, SC-7, SC-18.	d enforcement mechanisms tinations (e.g., networks, rconnected systems. Flow ormation path. Enforcement outers, guards, encrypted ngs that restrict information information, or message- word searches or using ness of filtering/inspection are critical to information ess cross-domain solution alysis, and stronger flow example, high-assurance -the-shelf information CM-6, CM-7, SA-8, SC-2,
201 202	Control En	nancements:	
203	AC-4(6)	INFORMATION FLOW ENFORCEMENT METADATA	[BACK TO SCRM CONTROL]
204 205		The information system enforces information flow control base organization-defined metadata].	ed on [Assignment:
200 207 208 209 210 211 212 213 214 215		<u>Supplemental Guidance</u> : Metadata is information used to describe Metadata can include structural metadata describing data structure and semantics) or descriptive metadata describing data contents (e number). Enforcing allowed information flows based on metadata effective flow control. Organizations consider the trustworthiness data accuracy (i.e., knowledge that the metadata values are correct data integrity (i.e., protecting against unauthorized changes to met of metadata to the data payload (i.e., ensuring sufficiently strong b appropriate levels of assurance). Related controls: AC-16, SI-7.	e the characteristics of data. es (e.g., data format, syntax, e.g., age, location, telephone enables simpler and more of metadata with regard to t with respect to the data), adata tags), and the binding binding techniques with
216	AC-4 (17)	INFORMATION FLOW ENFORCEMENT DOMAIN AUTHENTICATION	[BACK TO SCRM CONTROL]
217 218 219 220		The information system uniquely identifies and authenticates spoints by [Selection (one or more): organization, system, applied information transfer.	source and destination ation, individual] for
221 222 223 224 225 226 227		<u>Supplemental Guidance</u> : Attribution is a critical component of a soperations. The ability to identify source and destination points for information systems, allows the forensic reconstruction of events are encourages policy compliance by attributing policy violations to so organizations/individuals. Successful domain authentication require labels distinguish among systems, organizations, and individuals is sending, receiving, or disseminating information. Related controls	security concept of r information flowing in when required, and pecific res that information system nvolved in preparing, : IA-2, IA-3, IA-4, IA-5.
228	AC-4 (19)	INFORMATION FLOW ENFORCEMENT / VALIDATION OF METADATA	[BACK TO SCRM CONTROL]

229 230 231			The information system, when domains, applies the same sec payloads.	n transferring information bet curity policy filtering to metad	tween different security ata as it applies to data
232 233 234 235 236 237 238			Supplemental Guidance: This c data to which the metadata appl data payloads (i.e., only the dat make such distinctions, conside part of the payload. All informa applies) is subject to filtering an	control enhancement requires the lies. Some organizations disting a to which the metadata is bound ering metadata and the data to we ation (including metadata and the nd inspection.	e validation of metadata and the uish between metadata and d). Other organizations do not hich the metadata applies as e data to which the metadata
239 240	AC-4 (21)		INFORMATION FLOW ENFORCEM.	ENT PHYSICAL / LOGICAL	
241			SEPARATION OF INFORMATION FL	LOWS	[BACK TO SCRM CONTROL]
242 243 244			The information system separ [Assignment: organization-def [Assignment: organization-def	rates information flows logical fined mechanisms and/or techn fined required separations by ty	ly or physically using <i>iques</i>] to accomplish <i>pes of information</i>].
245 246 247 248 249			<u>Supplemental Guidance</u> : Enfor protection by ensuring that info flow control by transmission pa information include, for examp requests and responses, and inf	rcing the separation of information prmation is not commingled white aths perhaps not otherwise achies le, inbound and outbound common promation of differing security ca	on flows by type can enhance le in transit and by enabling vable. Types of separable nunications traffic, service ategories.
250		<u>Refe</u>	rences: Web: ucdmo.gov.		
251		Prior	ity and Baseline Allocation:		
252		P1	LOW Not Selected	MOD AC-4	HIGH AC-4
253	AC-5	SEPA	ARATION OF DUTIES		[Back to SCRM Control]
254		Cont	rol: The organization:		
255		a.	Separates [Assignment: organiz	zation-defined duties of individu	als];
256		b.	Documents separation of duties	s of individuals; and	
257		c.	Defines information system acc	cess authorizations to support se	paration of duties.
258 259 260 261 262 263 264 265		Supp privi dutic func func perso cont	<u>elemental Guidance</u> : Separation o ileges and helps to reduce the ri- es includes, for example: (i) div tions among different individual tions with different individuals agement, quality assurance and onnel administering access con- trols: AC-3, AC-6, PE-3, PE-4,	f duties addresses the potential f sk of malevolent activity withou iding mission functions and info ils and/or roles; (ii) conducting i (e.g., system management, prog testing, and network security); a trol functions do not also admini PS-2.	for abuse of authorized at collusion. Separation of prmation system support nformation system support gramming, configuration and (iii) ensuring security ister audit functions. Related
266		<u>Cont</u>	rol Enhancements: None.		
267		Refe	rences: None.		
268		Prior	ity and Baseline Allocation:		
		P1	LOW Not Selected	MOD AC-5	HIGH AC-5
269					

270	AC-6	LEAST PRIVILEGE		[Back to SCRM Control]
271 272 273		<u>Control</u> : The organization employ accesses for users (or processes a assigned tasks in accordance with	ts the principle of least privilege cting on behalf of users) which organizational missions and bu	, allowing only authorized are necessary to accomplish usiness functions.
274 275 276 277 278 279 280		Supplemental Guidance: Organizat systems. The principle of least pri that the processes operate at privious organizational missions/business processes, roles, and information Organizations also apply least pri- organizational information system	ions employ least privilege for s ivilege is also applied to inform lege levels no higher than neces functions. Organizations consid system accounts as necessary, to ivilege to the development, implins. Related controls: AC-2, AC-	pecific duties and information ation system processes, ensuring sary to accomplish required er the creation of additional o achieve least privilege. ementation, and operation of 3, AC-5, CM-6, CM-7, PL-2.
281 282	AC-6(6)	LEAST PRIVILEGE PRIVILEGEL USERS	O ACCESS BY NON-ORGANIZATIONA	L [BACK TO SCRM CONTROL]
283 284 285 286		The organization prohibits pri- users. Supplemental Guidance: Relate	vileged access to the information and control: IA-8.	system by non-organizational
287 288 289		<u>References</u> : None. Priority and Baseline Allocation:		
		P1 LOW Not Selected	MOD AC-6 (1) (2) (5) (9) (10)	HIGH AC-6 (1) (2) (3) (5) (9) (10)
290				
291	AC-17	REMOTE ACCESS		[Back to SCRM Control]
292				
293		Control: The organization:		
294 295		a. Establishes and documents u implementation guidance for	sage restrictions, configuration/	connection requirements, and wed; and
296		b. Authorizes remote access to	the information system prior to	allowing such connections.
297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313		Supplemental Guidance: Remote ac processes acting on behalf of use Remote access methods include, often employ encrypted virtual prover remote connections. The use however, the use of VPNs, when employing appropriate encryption provide sufficient assurance to the internal networks. Still, VPN con- does not enhance the availability affect the organizational capability malicious code. Remote access con- servers or systems designed for p- allowing remote access without s- may use interconnection security agreements are not required by the addressed in AC-3. Related contra-	ccess is access to organizational rs) communicating through exte for example, dial-up, broadband rivate networks (VPNs) to enhar e of encrypted VPNs does not m adequately provisioned with app n techniques for confidentiality a e organization that it can effect innections traverse external networ of remote connections. Also, VI ty to adequately monitor networ ontrols apply to information syst ublic access. This control address pecifying the formats for such a agreements to authorize remote tis control. Enforcing access rest ols: AC-2, AC-3, AC-18, AC-19	information systems by users (or rnal networks (e.g., the Internet). , and wireless. Organizations nee confidentiality and integrity ake the access non-remote; propriate security controls (e.g., and integrity protection) may vely treat such connections as orks, and the encrypted VPN PNs with encrypted tunnels can k communications traffic for tems other than public web sses authorization prior to uthorization. While organizations access connections, such crictions for remote connections is 9, AC-20, CA-3, CA-7, CM-8,
314		IA-2, IA-3, IA-8, MA-4, PE-17,	PL-4, SC-10, SI-4.	, .,,,

315		Control Enhancements:		
316	AC-17(6)	REMOTE ACCESS / PROTE	ECTION OF INFORMATION	[BACK TO SCRM CONTROL]
317 318 319		The organization ensume chanisms from una Supplemental Guidance	ures that users protect informa authorized use and disclosure. <u>e</u> : Related controls: AT-2, AT-3	s, PS-6.
320 221		<u>References</u> : NIST Special	Publications 800-46, 800-77, 800	0-113, 800-114, 800-121.
321		Priority and Baseline Allocation	<u>::</u>	
		P1 LOW AC-17	MOD AC-17 (1) (2) (3) (4)	HIGH AC-17 (1) (2) (3) (4)
322				
323	AC-18	WIRELESS ACCESS		[Back to SCRM Control]
324		Control: The organization:		
325 326		a. Establishes usage restri guidance for wireless a	ictions, configuration/connectior	requirements, and implementation
327		b. Authorizes wireless ac	cess to the information system p	rior to allowing such connections.
328 329 330 331		Supplemental Guidance: Wire (UHF/VHF), 802.11x, and EAP/TLS, PEAP), which p controls: AC-2, AC-3, AC-	eless technologies include, for ex Bluetooth. Wireless networks us rovide credential protection and 17, AC-19, CA-3, CA-7, CM-8,	cample, microwave, packet radio e authentication protocols (e.g., mutual authentication. Related IA-2, IA-3, IA-8, PL-4, SI-4.
332 333		<u>References</u> : NIST Special P	Publications 800-48, 800-94, 800	-97.
334		Priority and Baseline Allocation	Ľ	
		P1 LOW AC-18	MOD AC-18 (1)	HIGH AC-18 (1) (4) (5)
335	AC-19	ACCESS CONTROL FOR MO	BILE DEVICES	[Back to SCRM Control]
336		Control: The organization:		
337 338		a. Establishes usage restri implementation guidan	ictions, configuration requirement the for organization-controlled m	nts, connection requirements, and nobile devices; and
339		b. Authorizes the connect	ion of mobile devices to organiz	ational information systems.
340 341 342 343 344 345 346 347 348 349 350 351 352		Supplemental Guidance: A m such that it can easily be ca physical connection (e.g., w removable or removable da devices may also include vo to capture information, and Examples include smart phy with a single individual and degree of proximity can van processing, storage, and tra merely a subset of desktop device. Due to the large van	obile device is a computing devi rried by a single individual; (ii) is virelessly transmit or receive info ta storage; and (iv) includes a se pice communication capabilities, /or built-in features for synchron ones, E-readers, and tablets. Mol I the device is usually in close pr ry depending upon on the form fa nsmission capability of the mobi systems, depending upon the nat- riety of mobile devices with diffe	ice that: (i) has a small form factor is designed to operate without a ormation); (iii) possesses local, non- lf-contained power source. Mobile , on-board sensors that allow the device izing local data with remote locations. bile devices are typically associated oximity to the individual; however, the actor and size of the device. The le device may be comparable to or source and intended purpose of the erent technical characteristics and

357 358 359 360 361 362 363 364 365		primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled. Related controls: AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4.					
366		References: OMB Memorandum 06-16; NIST Special Publications 800-114, 800-124, 800-164.					
367		Priority and Baseline Allocation:					
		P1 LOW AC-19 MOD AC-19 (5) HIGH AC-19 (5)					
368							
369	AC-20	USE OF EXTERNAL INFORMATION SYSTEMS [Back to SCRM Control]					
370 371 372		<u>Control</u> : The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:					
373		a. Access the information system from external information systems; and					
374 375		b. Process, store, or transmit organization-controlled information using external information systems.					
376 377 378 379 380 381 382 383 384 385 386 387 388		<u>Supplemental Guidance</u> : External information systems are information systems or components of information systems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External information systems include, for example: (i) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of organizations. This control also addresses the use of external information systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational information systems.					
389 390 391 392 393 394 395		For some external information systems (i.e., information systems operated by other federal agencies, including organizations subordinate to those agencies), the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. Information systems within these organizations would not be considered external. These situations occur when, for example, there are pre-existing sharing/trust agreements (either implicit or explicit) established between federal agencies or organizations subordinate to those agencies.					

updating virus protection software, scanning for critical software updates and patches, conducting

395organizations subordinate to those agencies, or when such trust agreements are specified by396applicable laws, Executive Orders, directives, or policies. Authorized individuals include, for397example, organizational personnel, contractors, or other individuals with authorized access to398organizational information systems and over which organizations have the authority to impose399rules of behavior with regard to system access. Restrictions that organizations impose on400authorized individuals need not be uniform, as those restrictions may vary depending upon the401trust relationships between organizations. Therefore, organizations may choose to impose different402security restrictions on contractors than on state, local, or tribal governments.

403 404 405 406 407 408 409 410 411 412 413 414	This control does not apply to the use of external information systems to access public interfaces to organizational information systems (e.g., individuals accessing federal information through www.usa.gov). Organizations establish terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum: types of applications that can be accessed on organizational information that can be processed, stored, or transmitted on external information systems. If terms and conditions with the owners of external information systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems. Related controls: AC-3, AC-17, AC-19, CA-3, PL-4, SA-9.	
415 416	AC-20(1) USE OF EXTERNAL INFORMATION SYSTEMS LIMITS ON AUTHORIZED USE [BACK TO SCRM CONTROL]	
417 418 419 420 421 422	 The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: (a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or 	
423	(b) Retains approved information system connection or processing agreements with	
424 425 426 427 428 429 430 431 432	the organizational entity hosting the external information system. <u>Supplemental Guidance</u> : This control enhancement recognizes that there are circumstances where individuals using external information systems (e.g., contractors, coalition partners) need to access organizational information systems. In those situations, organizations need confidence that the external information systems contain the necessary security safeguards (i.e., security controls), so as not to compromise, damage, or otherwise harm organizational information systems. Verification that the required security controls have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the confidence level required by organizations. Related control: CA-2.	
433 434	AC-20(3) USE OF EXTERNAL INFORMATION SYSTEMS NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES [BACK TO SCRM CONTROL]	
435 436 437 438	The organization [<i>Selection: restricts; prohibits</i>] the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information.	
439 440 441 442 443 444 445 444 445 446 447 448 449 450 451	<u>Supplemental Guidance</u> : Non-organizationally owned devices include devices owned by other organizations (e.g., federal/state agencies, contractors) and personally owned devices. There are risks to using non-organizationally owned devices. In some cases, the risk is sufficiently high as to prohibit such use. In other cases, it may be such that the use of non-organizationally owned devices is allowed but restricted in some way. Restrictions include, for example: (i) requiring the implementation of organization-approved security controls prior to authorizing such connections; (ii) limiting access to certain types of information, services, or applications; (iii) using virtualization techniques to limit processing and storage activities to servers or other system components provisioned by the organization; and (iv) agreeing to terms and conditions for usage. For personally owned devices, organizations consult with the Office of the General Counsel regarding legal issues associated with using such devices in operational environments, including, for example, requirements for conducting forensic analyses during investigations after an incident.	
1 5 0		

<u>References</u>: FIPS Publication 199. 452

453		Priority and Baseline Allocation:						
		P1	LOW AC-20	MOD AC-20 (1) (2)	HIGH AC-20 (1) (2)			
454								
455	AC-21	INFO	RMATION SHARING		[Back to SCRM Control]			
456								
457		Contr	rol: The organization:					
458 459 460 461		a. F a f	a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and					
462 463		b. E a	b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.					
464 465 466 467 468 469 470		Supp mann inforr progr the pa indivi categ	<u>Supplemental Guidance</u> : This control applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, classified information related to special access programs or compartments) based on some formal or administrative determination. Depending on the particular information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment. Related control: AC-3.					
471		Refer	rences: None.					
472		Prior	ity and Baseline Allocati	ion:				
		P2	LOW Not Selected	MOD AC-21	HIGH AC-21			
 473 474 475 476 	AC-22	PUBL	ICLY ACCESSIBLE CONT	ſENT	[Back to SCRM Control]			
477 478		 a. Designates individuals authorized to post information onto a publicly accessible information system; 						
479 480		b. T	Frains authorized individ conpublic information;	luals to ensure that publicly ac	cessible information does not contain			
481 482		c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and						
483 484		d. Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered.						
485 486 487 488 489 490 491		Supp regula inform contra gener non-co AC-4	lemental Guidance: In a ations, standards, and/or mation (e.g., information ol addresses information al public, typically with organization information I, AT-2, AT-3, AU-13.	accordance with federal laws, I guidance, the general public in protected under the Privacy A systems that are controlled by out identification or authentica systems is covered by organiz	Executive Orders, directives, policies, s not authorized access to nonpublic Act and proprietary information). This / the organization and accessible to the ation. The posting of information on zational policy. Related controls: AC-3,			
492		Contr	col Enhancements: Non	ne.				

493		References: None.			
494		Priority and Baseline Allocation:			
495		P3 LOW AC-22	MOD AC-22	HIGH AC-22	
496 497	AC-24	ACCESS CONTROL DECISIONS		[Back to SCRM Control]	
498 499		<u>Control</u> : The organization establishe <i>access control decisions</i>] are applied	s procedures to ensure [Assignation of the state of the s	<i>nent: organization-defined</i> access enforcement.	
500 501 502 503 504 505 506		<u>Supplemental Guidance</u> : Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses. In contrast, access enforcement occurs when information systems enforce access control decisions. While it is very common to have access control decisions and access enforcement implemented by the same entity, it is not required and it is not always an optimal implementation choice. For some architectures and distributed information systems, different entities may perform access control decisions and access enforcement			
507					
508		References: None.			
509		Priority and Baseline Allocation:			
		P0 LOW Not Selected	MOD Not Selected	HIGH Not Selected	
510					

511 FAMILY: AWARENESS AND TRAINING

512	AT-1	SECU	IRITY AWARENESS AND TRA	INING POLICY AND PROCEDURES	[Back to SCRM Control]		
513		Conti	rol: The organization:				
514 515		a. I <i>r</i>	Develops, documents, and d roles]:	isseminates to [Assignment: organ	ization-defined personnel or		
516 517 518		1	 A security awareness an responsibilities, manage and compliance; and 	nd training policy that addresses pu ement commitment, coordination an	rpose, scope, roles, mong organizational entities,		
519 520		2	2. Procedures to facilitate and associated security	the implementation of the security awareness and training controls; ar	awareness and training policy		
521		b. Reviews and updates the current:					
522 523		1	 Security awareness and and 	training policy [Assignment: organ	vization-defined frequency];		
524 525		2	2. Security awareness and <i>frequency</i>].	training procedures [Assignment:	organization-defined		
526 527 528 529 530 531 532 533 534 535		Supp effect Polic polic level be ind be rep proce system	lemental Guidance: This co tive implementation of sele y and procedures reflect ap- ies, standards, and guidance may make the need for syst cluded as part of the genera presented by multiple polici edures can be established fo ms, if needed. The organiza y and procedures. Related c	ontrol addresses the establishment of cted security controls and control e plicable federal laws, Executive Or e. Security program policies and pro- tem-specific policies and procedure l information security policy for or res reflecting the complex nature of r the security program in general an tional risk management strategy is ontrol: PM-9.	of policy and procedures for the nhancements in the AT family. ders, directives, regulations, ocedures at the organization as unnecessary. The policy can ganizations or conversely, can certain organizations. The nd for particular information a key factor in establishing		
536		Contr	rol Enhancements: None.				
537		Refer	rences: NIST Special Publi	cations 800-12, 800-16, 800-50, 80	0-100.		
538		Prior	ity and Baseline Allocation	:			
		P1	LOW AT-1	MOD AT-1	HIGH AT-1		
539							
540	AT-3	ROLE	E BASED SECURITY TRAININ	G			
541	AT-3 (2) S	SECURI	TY TRAINING PHYSICAL SECU	IRITY CONTROLS	[BACK TO SCRM CONTROL]		
542 543 544		i o	The organization provides initial and [<i>Assignment: or</i> operation of physical secu	[Assignment: organization-define ganization-defined frequency] tra rity controls.	ed personnel or roles] with ining in the employment and		
545 546 547 548 549		2 c g r t	Supplemental Guidance: Ph control devices, physical int guards (deployment and ope roles and responsibilities as raining. Related controls: P	aysical security controls include, for rusion alarms, monitoring/surveilla erating procedures). Organizations is sociated with physical security cont E-2, PE-3, PE-4, PE-5.	r example, physical access ince equipment, and security identify personnel with specific trols requiring specialized		
550 551		<u>Refer</u> 50.	rences: C.F.R. Part 5 Subpa	urt C (5 C.F.R. 930.301); NIST Spe	cial Publications 800-16, 800-		
552		Prior	ity and Baseline Allocation	:			

P1 LOW AT-3	MOD AT-3	HIGH AT-3
-------------	----------	-----------

554 FAMILY: AUDIT AND ACCOUNTABILITY

555	AU-1	AUDIT A	AND ACCOUNTABILITY POLIC	Y AND PROCEDURES	[Back to SCRM Control]
556		Control	: The organization:		
557 558		a. Der role	velops, documents, and dissered list of the set of the	minates to [Assignment: organi	zation-defined personnel or
559 560 561		1.	An audit and accountability management commitment, c and	policy that addresses purpose, coordination among organizatio	scope, roles, responsibilities, onal entities, and compliance;
562 563		2. Procedures to facilitate the implementation of the audit and accountability policy associated audit and accountability controls; and			
564		b. Rev	views and updates the current		
565		1.	Audit and accountability po	licy [Assignment: organization	-defined frequency]; and
566		2.	Audit and accountability pro	ocedures [Assignment: organize	ation-defined frequency].
567 568 569 570 571 572 573 574 575 576 577 578 579		 <u>Supplemental Guidance</u>: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. <u>Control Enhancements:</u> None. <u>References:</u> NIST Special Publications 800-12, 800-100. 			
		P1 I	OW AU-1	MOD AU-1	HIGH AU-1
580 581					
582	AU-2	AUDIT H	EVENTS		[Back to SCRM Control]
583 584 585 586 587 588 589		Control a. Det [As b. Coorela eve	: The organization: termines that the information signment: organization-defin ordinates the security audit fu ated information to enhance n ents;	system is capable of auditing th ed auditable events]; unction with other organizationanutual support and to help guide	he following events: al entities requiring audit- e the selection of auditable
590 591		c. Pro the	vides a rationale for why the -fact investigations of securit	auditable events are deemed to y incidents; and	be adequate to support after-
592 593 594 595		d. Det [As in A eve	termines that the following ex signment: organization-defin AU-2 a.) along with the frequent [.	vents are to be audited within the ed audited events (the subset of ency of (or situation requiring)	te information system: f the auditable events defined auditing for each identified

$\begin{array}{c} 596\\ 597\\ 598\\ 599\\ 600\\ 601\\ 602\\ 603\\ 604\\ 605\\ 606\\ 607\\ 608\\ 609\\ 610\\ 611\\ 612\\ 613\\ 614\\ 615\\ 616\\ 617 \end{array}$		the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of <i>auditable</i> events that are <i>audited</i> at a given point in time. For example, organizations may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures. Related controls: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4. <u>References</u> : NIST Special Publication 800-92; Web: csrc.nist.gov/pcig/cig.html,				
618 619		<u>References</u> : NIST Special Publication 800-92; Web: csrc.nist.gov/pcig/cig.html, idmanagement.gov.				
620		Priori	ity and Baseline Allocation:			
		P1	LOW AU-2	MOD AU-2 (3)	HIGH AU-2 (3)	
621 622 623	A11 6		T DEVIEW ANALVSIS AND I	FEADTINC	[Back to SCRM Control]	
624	AC-0	Contr	rol: The organization:		Dack to BERM Control	
625		Conu				
623 626 627		a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and				
628		b. R	Reports findings to [Assignn	ent: organization-defined person	nel or roles].	
629 630 631 632 633 634 635 636 637 638 639 640		Suppl auditi of acc settin physi- the in to org securi inforr system	lemental Guidance: Audit r ing performed by organizati count usage, remote access, igs, system component inver ical access, temperature and information system boundarie ganizational entities that inc ity group/department. If org mation or unable to conduct	eview, analysis, and reporting cov ons including, for example, auditin wireless connectivity, mobile devi- ntory, use of maintenance tools and humidity, equipment delivery and es, use of mobile code, and use of lude, for example, incident respon anizations are prohibited from rev such activities (e.g., in certain nat whe carried out by other organization	rers information security-related ng that results from monitoring ice connection, configuration d nonlocal maintenance, removal, communications at VoIP. Findings can be reported se team, help desk, information iewing and analyzing audit ional security applications or tions granted such authority.	
641		IA-3, SI-4,	ed controls: AC-2, AC-3, A IA-5, IR-5, IR-6, MA-4, M SI-7.	C-6, AC-17, AT-3, AU-7, AU-16, P-4, PE-3, PE-6, PE-14, PE-16, R	, CA-7, CM-5, CM-10, CM-11, A-5, SC-7, SC-18, SC-19, SI-3,	

642
643AU-6 (9) AUDIT REVIEW, ANALYSIS, AND REPORTING / CORRELATION WITH
INFORMATION FROM NONTECHNICAL SOURCES

644 645		The organization correlates in information to enhance organization to enhance	nformation from nontechnic nization-wide situational awa	al sources with audit areness.				
646 647 648 649 650 651 652 653 654 655 656		<u>Supplemental Guidance</u> : Nontechnical sources include, for example, human resources records documenting organizational policy violations (e.g., sexual harassment incidents, improper use of organizational information assets). Such information can lead organizations to a more directed analytical effort to detect potential malicious insider activity. Due to the sensitive nature of the information available from nontechnical sources, organizations limit access to such information to minimize the potential for the inadvertent release of privacy-related information to individuals that do not have a need to know. Thus, correlation of information from nontechnical sources with audit information generally occurs only when individuals are suspected of being involved in a security incident. Organizations obtain legal advice prior to initiating such actions. Related control: AT-2.						
657		References: None.						
658		Priority and Baseline Allocation:						
		P1 LOW AU-6	MOD AU-6 (1) (3)	HIGH AU-6 (1) (3) (5) (6)				
659								
660	AU-10	NON-REPUDIATION		[Back to SCRM Control]				
661 662 663		Control: The information system p individual) falsely denying having p covered by non-repudiation].	rotects against an individual (c performed [Assignment: organ	or process acting on behalf of an nization-defined actions to be				
664 665 666 667 668 669 670 671 672 673 674		Supplemental Guidance: Types of ind example, creating information, send indicating concurrence or signing a claims by: (i) authors of not having transmitted messages; (iii) receivers having signed documents. Non-repu- originated from a particular individ- email, signing a contract, approving Organizations obtain non-repudiatio (e.g., digital signatures, digital mess SC-17, SC-23.	lividual actions covered by not ling and receiving messages, a contract). Non-repudiation pro- authored particular documents s of not having received messa udiation services can be used t ual, or if an individual took sp g a procurement request) or rec on services by employing vario sage receipts). Related control	n-repudiation include, for approving information (e.g., otects individuals against later s; (ii) senders of not having ages; or (iv) signatories of not o determine if information ecific actions (e.g., sending an ceived specific information. ous techniques or mechanisms s: SC-12, SC-8, SC-13, SC-16,				
675								
676		Control Enhancements:						
677	AU-10 (1)) NON-REPUDIATION ASSOCIATION OF A	IDENTITIES	[BACK TO SCRM CONTROL]				
678 679 680		The information system: a. Binds the identity of [Assignment: organiz	the information producer wattion-defined strength of bind	ith the information to <i>ding</i>]; and				
681 682		b. Provides the means f	for authorized individuals to rmation.	determine the identity of the				
683 684 685 686 687 688		Supplemental Guidance: provide organizational per information in the event of the strength of the binding on the security category of AC-4, AC-16.	This control enhancement suppresented with the means to ident f an information transfer. Orgation between the information prod f the information and relevant	borts audit requirements that tify who produced specific inizations determine and approve fucer and the information based risk factors. Related controls:				

689 690	AU-10 (2) NON-REPUDI. IDENTIT	ATION VALIDATE BIND Y	ING OF INFORMATION PROD	UCER [BACK TO SCRM CONTROL]	
691		The inf	formation system:			
692 693	(a) Validates the binding of the information producer identity to the information at [Assignment: organization-defined frequency]; and					
694 695	(b) Performs [Assignment: organization-defined actions] in the event of a validation error.					
696 697 698 699 700		Suppler between the use user rec	mental Guidance: Thin n production and revie of cryptographic chec quests or generated au	is control enhancement pro ew. The validation of bind eksums. Organizations det tomatically. Related contr	events the modification of information ings can be achieved, for example, by ermine if validations are in response to ols: AC-3, AC-4, AC-16.	
701	AU-10 (3) NON-REPUDI	ATION CHAIN OF CUST	TODY	[BACK TO SCRM CONTROL]	
702 703 704		The inf establis	formation system ma shed chain of custody	intains reviewer/release y for all information revi	r identity and credentials within the ewed or released.	
705 706 707 708 709 710 711 712 713 714	<u>Supplemental Guidance</u> : Chain of custody is a process that tracks the movement of evidence through its collection, safeguarding, and analysis life cycle by documenting each person who handled the evidence, the date and time it was collected or transferred, and the purpose for the transfer. If the reviewer is a human or if the review function is automated but separate from the release/transfer function, the information system associates the identity of the reviewer of the information to be released with the information and the information label. In the case of human reviews, this control enhancement provides organizational officials the means to identify who reviewed and released the information. In the case of automated reviews, this control enhancement ensures that only approved review functions are employed. Related					
715 716		References:	None.			
717		Priority and	Baseline Allocation:			
		P2 LOW	Not Selected	MOD Not Selected	HIGH AU-10	
718						
719	AU-12	AUDIT GENI	ERATION		[Back to SCRM Control]	
720		<u>Control</u> : The	e information system:			
721 722	a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components];					
723 724		b. Allows events a	[Assignment: organiz are to be audited by sp	<i>pation-defined personnel o</i> pecific components of the	<i>r roles</i>] to select which auditable information system; and	
725		c. Generat	tes audit records for th	ne events defined in AU-2	d. with the content defined in AU-3.	
726 727 728 729		Supplementa components These event generating a	<u>I Guidance</u> : Audit reco . The list of audited e s are typically a subsecudit records. Related	ords can be generated from vents is the set of events for et of all events for which the controls: AC-3, AU-2, AU	many different information system or which audits are to be generated. ne information system is capable of J-3, AU-6, AU-7.	
730		References:	None.			
731		Priority and B	aseline Allocation:			

		P1	LOW AU-12	MOD AU-12	HIGH AU-12 (1) (3)		
732							
733							
734	AU-13	MONI	TORING FOR INFORMATION D	ISCLOSURE	[Back to SCRM Control]		
735 736 737		Contr and/o unaut	<u>ol</u> : The organization monitors <i>r information sites</i>] [Assignment horized disclosure of organizat	[Assignment: organization-defint: organization-defined frequention information.	ined open source information ncy] for evidence of		
738 739		Suppl Relate	lemental Guidance: Open sour ed controls: PE-3, SC-7.	ce information includes, for exa	mple, social networking sites.		
740 741		Refer	ences: None.				
742		<u>Priori</u>	ity and Baseline Allocation:				
		P0	LOW Not Selected	MOD Not Selected	HIGH Not Selected		
743							
744	AU-16	CROS	S-ORGANIZATIONAL AUDITING	, ,	[Back to SCRM Control]		
745 746 747 748		<u>Contr</u> [Assigninform	<u>ol</u> : The organization employs gnment: organization-defined a nation is transmitted across org	[Assignment: organization-defined and it information] among extern ganizational boundaries.	<i>ned methods</i>] for coordinating al organizations when audit		
749 750 751 752 753 754 755 756		Supplemental Guidance: When organizations use information systems and/or services of external organizations, the auditing capability necessitates a coordinated approach across organizations. For example, maintaining the identity of individuals that requested particular services across organizational boundaries may often be very difficult, and doing so may prove to have significant performance ramifications. Therefore, it is often the case that cross-organizational auditing (e.g., the type of auditing capability provided by service-oriented architectures) simply captures the identity of individuals issuing requests at the initial information system, and subsequent systems record that the requests emanated from authorized individuals. Related control: AU-6.					
757	AU-16(2)	CROSS	ORGANIZATIONAL AUDITING SH	ARING OF AUDIT INFORMATION	[BACK TO SCRM CONTROL]		
758 759 760 761 762		T c a	The organization provides cross- lefined organizations] based on [greements].	organizational audit information t Assignment: organization-defined	o [Assignment: organization- d cross-organizational sharing		
763 764 765 766 767 768 769	<u>Supplemental Guidance</u> : Because of the distributed nature of the audit information, cross- organization sharing of audit information may be essential for effective analysis of the auditing being performed. For example, the audit records of one organization may not provide sufficient information to determine the appropriate or inappropriate use of organizational information resources by individuals in other organizations. In some instances, only the home organizations of individuals have the appropriate knowledge to make such determinations, thus requiring the sharing of audit information among organizations.						
770							
771		<u>Refer</u>	ences: None.				
112		Priori	ty and Baseline Allocation:				

DO	LOW N (CL / L	MOD N (CL / L	
PO	LOW Not Selected	MOD Not Selected	HIGH Not Selected

773 FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION

774 775	CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES Back to SCRM Cont					
776		Control: The organization:					
777 778		a. Develops, documents, and disseminates to [Assignment: organization-defined person or roles]:					
779 780 781			1. A security assessment a responsibilities, manage entities, and compliance	and authorization policy that ad ement commitment, coordinatione; and	dresses purpose, scope, roles, on among organizational		
782 783 784			2. Procedures to facilitate authorization policy and and	the implementation of the secu d associated security assessmen	rity assessment and authorization controls;		
785		b.	Reviews and updates the cur	rrent:			
786 787			1. Security assessment and <i>frequency</i>]; and	d authorization policy [Assignn	nent: organization-defined		
788 789			2. Security assessment and <i>frequency</i>].	d authorization procedures [Ass	ignment: organization-defined		
790 791 792 793 794 795 796 797 798 799 800 801 802		 <u>Supplemental Guidance</u>: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. <u>Control Enhancements:</u> None. References: NIST Special Publications 800-12, 800-37, 800-53A, 800-100. 					
002							
803		PI LO	UW CA-I	MOD CA-I	HIGH CA-1		
804	CA-2	SECURIT	Y ASSESSMENTS		[Back to SCRM Control]		
803 806		Control:	The organization:				
807		a. Dev	elops a security assessment	plan that describes the scope of	the assessment including:		
808		1.	Security controls and control	ol enhancements under assessme	ent;		
809		2.	Assessment procedures to b	e used to determine security co	ntrol effectiveness; and		
810		3.	Assessment environment, as	ssessment team, and assessmen	t roles and responsibilities;		
811 812		b. Asso [Ass	esses the security controls in signment: organization-defin	the information system and its <i>ed frequency</i>] to determine the	environment of operation extent to which the controls		

813 814	are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
815	c. Produces a security assessment report that documents the results of the assessment; and
816 817	d. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles].
818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838	<u>Supplemental Guidance</u> : Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from Appendix F (main catalog) and Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The FISMA requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives.
839 840 841 842 843 844 845 846 845 846 847 848 849 850 851	To satisfy annual assessment requirements, organizations can use assessment results from the following sources: (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Subsequent to initial authorizations and in accordance with OMB policy, organizations assess security control assessments in accordance with organizations establish the frequency for ongoing security control assessments in accordance with organizational continuous monitoring strategies. Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4.
852	Control Enhancements:
853	CA-2 (2) SECURITY ASSESSMENTS / SPECIALIZED ASSESSMENTS [BACK TO SCRM CONTROL]
854 855 856 857 858 859 860	The organization includes as part of security control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [Assignment: organization-defined other forms of security assessment]].
861 862 863	<u>Supplemental Guidance</u> : Organizations can employ information system monitoring, insider threat assessments, malicious user testing, and other forms of testing (e.g., verification and validation) to improve readiness by exercising organizational capabilities and indicating

864 865 866 867 868 869	current performance levels as a means of focusing actions to improve security. Organizations conduct assessment activities in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can incorporate vulnerabilities uncovered during assessments into vulnerability remediation processes. Related controls: PE-3, SI-2.							
870	CA-2 (3) SECURITY ASSESSMENTS EXTERNAL ORGANIZATIONS [BACK TO SCRM CONTROL]							1
871 872 873 874 875 876	The organization accepts the results of an assessment of [Assignment: organization- defined information system] performed by [Assignment: organization-defined external organization] when the assessment meets [Assignment: organization-defined requirements].						n	
877 878 879 880 881 882 883 883 884 885	<u>Supplemental Guidance</u> : Organizations may often rely on assessments of specific information systems by other (external) organizations. Utilizing such existing assessments (i.e., reusing existing assessment evidence) can significantly decrease the time and resources required for organizational assessments by limiting the amount of independent assessment activities that organizations need to perform. The factors that organizations may consider in determining whether to accept assessment results from external organizations can vary. Determinations for accepting assessment results can be based on, for example, past assessment experiences one organization has had with another organization, the reputation that organizations have with regard to assessments, the level of detail of supporting assessment documentation provided, or mandates imposed upon organizations by federal legislation, policies, or directives						r	
886 887		<u>Refere</u> 800-3	ences: Executive Order 1 9, 800-53A, 800-115, 800	3587 0-137	; FIPS Publication 19	9; NIST S	pecial Publications 800-37,	
888		Priority	and Baseline Allocation:					
889		P2	LOW CA-2		MOD CA-2 (1)		HIGH CA-2 (1) (2)	
890	CA-3	SYSTE	M INTERCONNECTIONS				[Back to SCRM Control	<u>L</u>
891 892		<u>Contr</u>	ol: The organization:					
893 894		a. A th	uthorizes connections f arough the use of Interc	rom t onne	he information syste ction Security Agree	em to othe ements;	er information systems	
895 896		b. D re	ocuments, for each inte equirements, and the na	rconi iture	nection, the interface of the information c	e characte ommunica	eristics, security ated; and	
897 898		c. R	eviews and updates Inte efined frequency].	ercon	nection Security Ag	reements	[Assignment: organization-	
899 900 901 902 903 904 905 906 907 908		Supple system conne- may b securi organi conne- author Instea- system	emental Guidance: This ns (i.e., system interconnections such as email and e introduced when inform ty requirements and secur- zations. Authorizing offi- ctions and the appropriate izing official, organization d, organizations can desc ns in their respective secu-	contro ection websi natior rity co cials o cials o e cont cons do ribe t urity p	ol applies to dedicated as) and does not apply ite browsing. Organiz a systems are connect ontrols, both within o determine the risk ass trols employed. If inte o not need to develop he interface character plans. If interconnectin	d connection to transitu ations care ed to other rganization pociated wite erconnection Interconnection istics betwo	ons between information ory, user-controlled efully consider the risks that r systems with different ns and external to ith information system ng systems have the same ection Security Agreements. veen those interconnecting s have different authorizing	

909 910 911 912 913 914 915 916 917 918		officials within the same organizatio Agreements or describe the interface respective systems. Organizations m information into formal contracts, es agencies and nonfederal (i.e., private information systems sharing the sam aerial vehicles, and medical devices) preoperational testing. Such connect subject to additional security control 16, CA-7, IA-3, SA-9, SC-7, SI-4.	n, organizations can either deve e characteristics between system ay also incorporate Interconnec pecially for interconnections es e sector) organizations. Risk cor e networks. For certain technolo , there may be specialized conn ions may require Interconnectio s. Related controls: AC-3, AC-4	elop Interconnection Security is in the security plans for the tion Security Agreement tablished between federal asiderations also include ogies (e.g., space, unmanned ections in place during on Security Agreements and be 4, AC-20, AU-2, AU-12, AU-			
919		Control Enhancements:					
920 921	CA-3 (3)	SYSTEM INTERCONNECTIONS UN SECURITY SYSTEM CONNECTIONS	CLASSIFIED NON-NATIONAL	[BACK TO SCRM CONTROL]			
922 923 924 925		The organization prohibits the unclassified, non-national secu [Assignment; organization-defi	e direct connection of an [Assignation of an [Assignation of an and the set of the set o	<i>gnment: organization-defined</i> work without the use of e].			
926 927 928 929 930		<u>Supplemental Guidance:</u> Organ (e.g., the Internet). Approved bo communications (i.e., informatio and external networks. This con storing, or transmitting Controll	izations typically do not have coundary protection devices (e.g., on flows) between unclassified to trol enhancement is required for ed Unclassified Information (Cl	ontrol over external networks , routers, firewalls) mediate non-national security systems r organizations processing, UI).			
931							
932 933	CA-3 (4)	SYSTEM INTERCONNECTIONS COI NETWORKS	NNECTIONS TO PUBLIC	[BACK TO SCRM CONTROL]			
934 935		The organization prohibits the <i>information system</i>] to a public	e direct connection of an [<i>Assi</i> a e network.	gnment: organization-defined			
936 937		<u>Supplemental Guidance:</u> A pub including, for example, the Inter	lic network is any network acceret and organizational extranet	essible to the general public s with public access.			
938 939	CA-3 (5)	SYSTEM INTERCONNECTIONS RES SYSTEM CONNECTIONS	TRICTIONS ON EXTERNAL	[BACK TO SCRM CONTROL]			
940 941 942		The organization employs [Selection: allow-all, deny-by-exception; deny-all, permit-by- exception] policy for allowing [Assignment: organization-defined information systems] to connect to external information systems.					
943 944 945 946 947 948		<u>Supplemental Guidance:</u> Organ external domains (e.g., websites connectivity: (i) allow-all, deny two policies); or (ii) deny-all, al the two policies). For either poli acceptable. Related control: CM	<u>Supplemental Guidance:</u> Organizations can constrain information system connectivity to external domains (e.g., websites) by employing one of two policies with regard to such connectivity: (i) allow-all, deny by exception, also known as <i>blacklisting</i> (the weaker of the two policies); or (ii) deny-all, allow by exception, also known as <i>whitelisting</i> (the stronger of the two policies). For either policy, organizations determine what exceptions, if any, are acceptable. Related control: CM-7				
949		References: FIPS Publication 199; N	IST Special Publication 800-47				
950		Priority and Baseline Allocation:					
		P1 LOW CA-3	MOD CA-3 (5)	HIGH CA-3 (5)			
951							

953		Control: The organization:					
954 955 956 957		a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and					
958 959 960		b.	Updates existing plan of based on the findings fro continuous monitoring a	action om sector ctivitie	and milestones [<i>Assignme</i> urity controls assessments, es.	ent: organ , security	nization-defined frequency] impact analyses, and
961 962 963		<u>Supp</u> autho Relat	blemental Guidance: Plan prization packages and ar ted controls: CA-2, CA-7	ns of a re subjo ', CM-	ction and milestones are ke ect to federal reporting req 4, PM-4.	ey docum juirement	nents in security is established by OMB.
964		Refer	ences: OMB Memorand	um 02-	-01; NIST Special Publica	tion 800-	37.
965		Priori	ty and Baseline Allocation:				
		P3	LOW CA-5		MOD CA-5	H	IGH CA-5
966							
967	CA-6	SECU	JRITY AUTHORIZATION				[Back to SCRM Control]
968 969		Cont	rol: The organization:				
970 971		 a. Assigns a senior-level executive or manager as the authorizing official for the information system; 					
972 973		b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and					
974		c.	Updates the security auth	orizati	on [Assignment: organiza	tion-defir	ned frequency].
975 976 977 978 979 980 981 982 983 984 985 986 987 988 987 988 989 990 991 992 993 994 995		<u>Supplemental Guidance</u> : Security authorizations are official management decisions, conveyed through authorization decision documents, by senior organizational officials or executives (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security controls. Authorizing officials provide budgetary oversight for organizational information systems or assume responsibility for the mission/business operations supported by those systems. The security authorization process is an inherently federal responsibility and therefore, authorizing officials must be federal employees. Through the security authorization process, authorizing officials assume responsibility and are accountable for security risks associated with the operation and use of organizational information systems. Accordingly, authorizing officials are in positions with levels of authority commensurate with understanding and accepting such information security-related risks. OMB policy requires that organizations conduct ongoing authorizations of information systems by implementing continuous monitoring programs. Continuous monitoring programs can satisfy three-year reauthorization packages (i.e., security plans, security sates of organization and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation. To reduce the administrative cost of security reauthorization, authorizating officials use the results of organization and environments of operation.					
996 997		reauthorization decisions. Related controls: CA-2, CA-7, PM-9, PM-10. Control Enhancements: None.					

<u>References</u>: OMB Circular A-130; OMB Memorandum 11-33; NIST Special Publications 800-37, 800-137. Priority and Baseline Allocation:

1000

MOD CA-6

HIGH CA-6

[Back to SCRM Control]

1001 CA-7 CONTINUOUS MONITORING

LOW CA-6

P2

- 1002 1003 Control: 1004 a. The organization develops a continuous monitoring strategy and implements a 1005 continuous monitoring program that includes: 1006 Establishment of [Assignment: organization-defined metrics] to be monitored; b. 1007 c Establishment of [Assignment: organization-defined frequencies] for monitoring and 1008 [Assignment: organization-defined frequencies] for assessments supporting such 1009 monitoring; 1010 d. Ongoing security control assessments in accordance with the organizational continuous 1011 monitoring strategy; 1012 e. Ongoing security status monitoring of organization-defined metrics in accordance with 1013 the organizational continuous monitoring strategy; 1014 Correlation and analysis of security-related information generated by assessments and f. 1015 monitoring; 1016 Response actions to address results of the analysis of security-related information; and g. 1017 Reporting the security status of organization and the information system to h. 1018 [Assignment: organization-defined personnel or roles] [Assignment: organization-1019 defined frequency]. 1020 Supplemental Guidance: Continuous monitoring programs facilitate ongoing awareness of threats, 1021 vulnerabilities, and information security to support organizational risk management decisions. The 1022 terms *continuous* and *ongoing* imply that organizations assess/analyze security controls and 1023 information security-related risks at a frequency sufficient to support organizational risk-based 1024 decisions. The results of continuous monitoring programs generate appropriate risk response 1025 actions by organizations. Continuous monitoring programs also allow organizations to maintain 1026 the security authorizations of information systems and common controls over time in highly 1027 dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, 1028 and technologies. Having access to security-related information on a continuing basis through 1029 reports/dashboards gives organizational officials the capability to make more effective and timely 1030 risk management decisions, including ongoing security authorization decisions. Automation 1031 supports more frequent updates to security authorization packages, hardware/software/firmware 1032 inventories, and other system information. Effectiveness is further enhanced when continuous 1033 monitoring outputs are formatted to provide information that is specific, measurable, actionable, 1034 relevant, and timely. Continuous monitoring activities are scaled in accordance with the security 1035 categories of information systems. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-1036 9. RA-5. SA-11. SA-12. SI-2. SI-4. 1037 1038 Control Enhancements:
- 1039 CA-7 (3) CONTINUOUS MONITORING / TREND ANALYSES

[BACK TO SCRM CONTROL]

1040The organization employs trend analyses to determine if security control1041implementations, the frequency of continuous monitoring activities, and/or the types of

1042 1043	activities used in the continuous monitoring process need to be modified based on empirical data.						
1044 1045 1046 1047 1048 1049	Supplemental Guidance: Tre information regarding the typ across the federal governmer vulnerabilities in information from multiple security contro findings from Inspectors Ger	<u>Supplemental Guidance</u> : Trend analyses can include, for example, examining recent threat information regarding the types of threat events that have occurred within the organization or across the federal government, success rates of certain types of cyber attacks, emerging vulnerabilities in information technologies, evolving social engineering techniques, results from multiple security control assessments, the effectiveness of configuration settings, and findings from Inspectors General or auditors.					
1050 1051	<u>References</u> : OMB Memorandum 11-3 137; US-CERT Technical Cyber Secu	<u>References</u> : OMB Memorandum 11-33; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800- 137; US-CERT Technical Cyber Security Alerts; DoD Information Assurance Vulnerability Alerts.					
1052 1053	2 Priority and Baseline Allocation:						
	P2 LOW CA-/	MOD $CA-7(1)$	$\Pi O \Pi C A - I (1)$				

1055 FAMILY: CONFIGURATION MANAGEMENT

1056	CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	[Back to SCRM Control]					
1057 1058		Control: The organization:						
1059 1060		a. Develops, documents, and disseminates to [<i>Assignment: organization-defined personnel or roles</i>]:						
1061 1062 1063		1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and						
1064 1065		2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and						
1066		b. Reviews and updates the current:						
1067		1. Configuration management policy [Assignment: organization	on-defined frequency]; and					
1068		2. Configuration management procedures [Assignment: organ	ization-defined frequency].					
1069 1070 1071 1072 1073 1074 1075 1076 1077 1078		<u>Supplemental Guidance</u> : This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CM family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing						
1079		Control Enhancements: None.						
1080		References: NIST Special Publications 800-12, 800-100.						
1081		Priority and Baseline Allocation:						
		P1 LOW CM-1 MOD CM-1	HIGH CM-1					
1082								
1083	CM-2	BASELINE CONFIGURATION	[Back to SCRM Control]					
1084								
1085 1086		<u>Control</u> : The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.						
1087 1088 1089 1090 1091 1092 1093 1094 1095 1096 1097		<u>Supplemental Guidance</u> : This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of						

1098 1099	information systems reflect the current enterprise architecture. Related controls: CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7.						
$\begin{array}{c}1100\\1101\end{array}$	Control Enhancements:						
1102	СМ-2 (1)	BASE	LINE CONFIGURATION REVIEWS A	ND UPDATES	[BACK TO SCRM CONTROL]		
1103							
1104			The organization reviews and u	pdates the baseline configuratio	n of the information system:		
1105			(a) [Assignment: organization	-defined frequency];			
1106			(b) When required due to [Ass	ignment organization-defined ci	rcumstances]; and		
1107 1108			(c) As an integral part of infor <u>Supplemental Guidance</u> : Related of	mation system component instation solution component instation control: CM-5.	lations and upgrades.		
1109 1110	СМ-2 (6)		BASELINE CONFIGURATION / DEV ENVIRONMENTS	ELOPMENT AND TEST	[BACK TO SCRM CONTROL]		
1111 1112 1113 1114			The organization maintains a development and test environ baseline configuration.	baseline configuration for inf ments that is managed separa	ormation system tely from the operational		
1115 1116 1117 1118 1119 1120 1121 1122 1123 1124 1125	<u>Supplemental Guidance</u> : Establishing separate baseline configurations for development, testing, and operational environments helps protect information systems from unplanned/unexpected events related to development and testing activities. Separate baseline configurations allow organizations to apply the configuration management that is most appropriate for each type of configuration. For example, management of operational configurations typically emphasizes the need for stability, while management of development/test configurations requires greater flexibility. Configurations in the test environment mirror the configurations in the operational environment to the extent practicable so that the results of the testing are representative of the proposed changes to the operational systems. This control enhancement requires separate configurations but not necessarily separate physical environments. Related controls: CM-4. SC-3. SC-7.						
1120		Refe Prior	erences: NIST Special Publication 8 rity and Baseline Allocation:	00-128.			
					T1		
1100		P1	LOW CM-2	MOD CM-2 (1) (3) (7)	HIGH CM-2 (1) (2) (3) (7)		
1128							
1129	CM-3	CON	FIGURATION CHANGE CONTRO	L	[Back to SCRM Control]		
1130		Control: The organization:					
1131		a. Determines the types of changes to the information system that are configuration-controlled;					
1132 1133		b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;					
1134		c.	Documents configuration change	ge decisions associated with the	information system;		
1135		d.	Implements approved configura	ation-controlled changes to the i	nformation system;		
1136 1137		e.	Retains records of configuratio [Assignment: organization-defi	n-controlled changes to the informed time period];	rmation system for		
1140 g. Coordinates and provides oversight for configuration change control acti 1141 [Assignment: organization-defined configuration change control learner 1142 board] that convenes [Selection (one or more): [Assignment: organization] 1143 Supplemental Guidance: Configuration change conditions]. 1144 Supplemental Guidance: Configuration change conditions, config 1145 involve the systematic proposal, justification, implementation, testing, review 1146 control includes changes to baseline configuration settings for information systems, changes to configuration settings for information experting systems, applications, firewalls, routers, and mobile devices), unsoft 1150 changes to information systems include, for example, Configuration develo 1151 changes or ganizational information systems and the auditing activities 1152 najor upgrades, organizational information systems and the auditing activities 1153 major upgrades, organizational information systems and the auditing activities 1154 on the Configuration Control Boards. Auditing of changes includes activities 1155 major upgrades, organizational information systems and the auditing activities 1156 implement such changes. Related controls: CM-2, CM-4, CM-5, CM-6, CM-1 1157 12. 1158 References: N	ht for configuration change control activities through <i>d configuration change control element (e.g., committee,</i> <i>one or more):</i> [Assignment: organization-defined frequency]; <i>d configuration change conditions</i>]]. In change controls for organizational information systems feation, implementation, testing, review, and disposition of em upgrades and modifications. Configuration change onfigurations for components and configuration items of guration settings for information technology products (e.g., alls, routers, and mobile devices), unscheduled/unauthorized inerabilities. Typical processes for managing configuration le, for example, Configuration Control Boards that approve <i>v</i> development information systems or systems undergoing er including representatives from development organizations Auditing of changes includes activities before and after formation systems and the auditing activities required to irols: CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI- 128. <u>MOD CM-3 (2)</u> <u>HIGH CM-3 (1) (2)</u> <u>IBack to SCRM Control</u>] nanges to the information system to determine potential mentation. nal personnel with information security responsibilities (e.g., nformation System Security Officers, Information System ystem Security Engineers) conduct security impact analyses. t analyses possess the necessary skills/technical expertise to stems and the associated security ramifications. Security ple, reviewing security plans to understand security control sign documentation to understand control implementation the controls. Security plans to understand security control sign documentation to understand control implementation the controls. Security plans to understand security Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, 128.						
---	---						
1144 Supplemental Guidance: Configuration change controls for organizational in involve the systems, including system upgrades and modifications. Config control includes changes to baseline configurations for components and confi information systems, changes to configurations for components and confistence operating systems, applications, firewalls, routers, and mobile devices), unset changes, and changes to remediate vulnerabilities. Typical processes for mamon operating systems, or new development information systems or singer upgrades, organizations consider including representatives from development information systems or singer upgrades, organizations and the auditing acti implement such changes. Related controls: CM-2, CM-4, CM-5, CM-6, CM-1157 1151 changes are made to organization 800-128. 1152 Priority and Baseline Allocation: 1160 CM-4 1161 CM-4 1162 Control: The organization analyzes changes to the information system to det security impacts prior to change implementation. 1163 References: NIST Special Publication BOC CM-3 (2) HIGH C 1164 SECURITY IMPACT ANALYSIS 1165 Information system Administrators, Information System Security Officers, Ir Security Images to information systems and the associated security analyses requires induced, for example, reviewing security Officers, Ir Security Managers, and Information System Security Information systems and the associated security officers, Ir Security Managers, and Information System Security Information to understand cont analyze the changes to rinformation systems and the associated security officers, Ir Secur	n change controls for organizational information systems feation, implementation, testing, review, and disposition of em upgrades and modifications. Configuration change onfigurations for components and configuration items of guration settings for information technology products (e.g., alls, routers, and mobile devices), unscheduled/unauthorized inerabilities. Typical processes for managing configuration le, for example, Configuration Control Boards that approve a development information systems or systems undergoing reincluding representatives from development organizations Auditing of changes includes activities before and after formation systems and the auditing activities required to trols: CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-128. MOD CM-3 (2) HIGH CM-3 (1) (2) IBack to SCRM Control] nanges to the information system to determine potential mentation. all personnel with information security responsibilities (e.g., formation System Security Officers, Information System ystem Security Engineers) conduct security impact analyses. analyses possess the necessary skills/technical expertise to stems and the associated security ramifications. Security ple, reviewing security plans to understand security control sign documentation to understand control implementation the controls. Security impact analyses may also include d the impact of the changes and to determine if additional / impact analyses are scaled in accordance with the security Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, 128.						
P1 LOW Not Selected MOD CM-3 (2) HIGH CI 1160 1160 1161 CM-4 SECURITY IMPACT ANALYSIS 1162 Control: The organization analyzes changes to the information system to deto security impacts prior to change implementation. 1163 Supplemental Guidance: Organizational personnel with information security Information System Administrators, Information System Security Officers, Ir Security Managers, and Information System Security Engineers) conduct securit/analyze the changes to information systems and the associated security ramifing impact analysis may include, for example, reviewing security plans to understand cont and how specific changes might affect the controls. Security impact analyses assessments of risk to better understand the impact of the changes and to dete security controls are required. Security impact analyses are scaled in accordar categories of the information systems. Related controls: CA-2, CA-7, CM-3, SA-10, SI-2. 1176 References: NIST Special Publication 800-128. 1177 Priority and Baseline Allocation: 12 LOW CM-4 MOD CM-4 1178	MOD_CM-3 (2) HIGH_CM-3 (1) (2) [Back to SCRM Control] nanges to the information system to determine potential ementation. nal personnel with information security responsibilities (e.g., nformation System Security Officers, Information System ystem Security Engineers) conduct security impact analyses. tanalyses possess the necessary skills/technical expertise to stems and the associated security ramifications. Security uple, reviewing security plans to understand security control esign documentation to understand control implementation the controls. Security impact analyses may also include d the impact of the changes and to determine if additional / impact analyses are scaled in accordance with the security Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, 128.						
1160 1160 1160 1161 CM-4 SECURITY IMPACT ANALYSIS 1161 CM-4 SECURITY IMPACT ANALYSIS 1162 Control: The organization analyzes changes to the information system to deta security impacts prior to change implementation. 1163 Supplemental Guidance: Organizational personnel with information security Information System Administrators, Information System Security Officers, Ir Security Managers, and Information System Security Engineers) conduct securits analyze the changes to information systems and the associated security ramifi impact analysis may include, for example, reviewing security plans to understand cont and how specific changes might affect the controls. Security impact analyses assessments of risk to better understand the impact of the changes and to dete security controls are required. Security impact analyses are scaled in accordar categories of the information systems. Related controls: CA-2, CA-7, CM-3, SA-10, SI-2. 1176 References: NIST Special Publication 800-128. 1177 Priority and Baseline Allocation: 1178 P2	[Back to SCRM Control] hanges to the information system to determine potential mentation. hal personnel with information security responsibilities (e.g., hformation System Security Officers, Information System ystem Security Engineers) conduct security impact analyses. t analyses possess the necessary skills/technical expertise to stems and the associated security ramifications. Security uple, reviewing security plans to understand security control sign documentation to understand control implementation the controls. Security impact analyses may also include id the impact of the changes and to determine if additional / impact analyses are scaled in accordance with the security Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, 128.						
1161 CM-4 SECURITY IMPACT ANALYSIS 1162 Control: The organization analyzes changes to the information system to deta security impacts prior to change implementation. 1163 Supplemental Guidance: Organizational personnel with information security Information System Administrators, Information System Security Officers, Ir Security Managers, and Information System Security Engineers) conduct securite the changes to information systems and the associated security ramifi impact analyses may include, for example, reviewing security plans to understree requirements and reviewing system design documentation to understand control and how specific changes might affect the controls. Security impact analyses assessments of risk to better understand the impact of the changes and to dete security controls are required. Security impact analyses are scaled in accordan categories of the information systems. Related controls: CA-2, CA-7, CM-3, SA-10, SI-2. 1176 References: NIST Special Publication 800-128. 1177 Priority and Baseline Allocation: 1178 MOD CM-4	IBack to SCRM Control manges to the information system to determine potential mentation. al personnel with information security responsibilities (e.g., nformation System Security Officers, Information System ystem Security Engineers) conduct security impact analyses. t analyses possess the necessary skills/technical expertise to stems and the associated security ramifications. Security uple, reviewing security plans to understand security control sign documentation to understand control implementation the controls. Security impact analyses may also include d the impact of the changes and to determine if additional impact analyses are scaled in accordance with the security Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, 128.						
1162 Control: The organization analyzes changes to the information system to deta security impacts prior to change implementation. 1164 Supplemental Guidance: Organizational personnel with information security Information System Administrators, Information System Security Officers, Ir Security Managers, and Information System Security Engineers) conduct securits impact analyze the changes to information systems and the associated security ramifi impact analysis may include, for example, reviewing security plans to understand control and how specific changes might affect the controls. Security impact analyses assessments of risk to better understand the impact of the changes and to dete security controls are required. Security impact analyses are scaled in accordar categories of the information systems. Related controls: CA-2, CA-7, CM-3, SA-10, SI-2. 1176 References: NIST Special Publication 800-128. 1177 Priority and Baseline Allocation: 1178 MOD CM-4	hanges to the information system to determine potential ementation. hal personnel with information security responsibilities (e.g., nformation System Security Officers, Information System ystem Security Engineers) conduct security impact analyses. t analyses possess the necessary skills/technical expertise to stems and the associated security ramifications. Security uple, reviewing security plans to understand security control sign documentation to understand control implementation the controls. Security impact analyses may also include d the impact of the changes and to determine if additional / impact analyses are scaled in accordance with the security Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, 128.						
1164Supplemental Guidance: Organizational personnel with information security Information System Administrators, Information System Security Officers, In Security Managers, and Information System Security Engineers) conduct secu- Individuals conducting security impact analyses possess the necessary skills/t analyze the changes to information systems and the associated security ramifi impact analysis may include, for example, reviewing security plans to unders requirements and reviewing system design documentation to understand cont and how specific changes might affect the controls. Security impact analyses assessments of risk to better understand the impact of the changes and to dete security controls are required. Security impact analyses are scaled in accordan categories of the information systems. Related controls: CA-2, CA-7, CM-3, SA-10, SI-2.1176References: NIST Special Publication 800-128.1177Priority and Baseline Allocation:11781178	nal personnel with information security responsibilities (e.g., nformation System Security Officers, Information System ystem Security Engineers) conduct security impact analyses. t analyses possess the necessary skills/technical expertise to stems and the associated security ramifications. Security uple, reviewing security plans to understand security control esign documentation to understand control implementation the controls. Security impact analyses may also include d the impact of the changes and to determine if additional / impact analyses are scaled in accordance with the security Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, 128.						
P2 LOW CM-4 MOD CM-4 HIGH CM 1178							
1178	MOD CM-4 HIGH CM-4 (1)						
1179 CM-5 ACCESS RESTRICTIONS FOR CHANGE [Bac	[Back to SCRM Control]						

1181 1182	<u>Control</u> : restriction	The organization defines, documents, approves, and en as associated with changes to the information system.	nforces physical and logical access
1183 1184 1185 1186 1187 1188 1189 1190 1191 1192 1193	Suppleme informati Therefore systems f maintain support a restriction physical a abstract la informati making u	ntal Guidance: Any changes to the hardware, softwar on systems can potentially have significant effects on to , organizations permit only qualified and authorized in or purposes of initiating changes, including upgrades a records of access to ensure that configuration change of ter-the-fact actions should organizations discover any is for change also include software libraries. Access re- and logical access controls (see AC-3 and PE-3), work uyers (e.g., changes implemented into third-party inter on systems), and change windows (e.g., changes occur nauthorized changes easy to discover). Related control	e, and/or firmware components of the overall security of the systems. ndividuals to access information and modifications. Organizations control is implemented and to unauthorized changes. Access estrictions include, for example, flow automation, media libraries, faces rather than directly into only during specified times, ls: AC-3, AC-6, PE-3.
1194	Control En	nancements:	
1195 1196	CM-5 (1) ACCESS RES ENFO	TRICTIONS FOR CHANGE AUTOMATED ACCESS RCEMENT / AUDITING	[BACK TO SCRM CONTROL]
1197	The i	nformation system enforces access restrictions and suppo	orts auditing of the enforcement
1198	action Suppl	IS. emental Guidance: Related controls: AU-2, AU-12, AU-6, CM	<i>I</i> -3, CM-6.
1200	CM-5 (2) ACCESS RES	TRICTIONS FOR CHANGE REVIEW SYSTEM CHANGES	[BACK TO SCRM CONTROL]
1201 1202 1203	The frequ unau	organization reviews information system changes [/ ency] and [Assignment: organization-defined circum thorized changes have occurred.	Assignment: organization-defined nstances] to determine whether
1204 1205 1206 1207	<u>Supp</u> the sp by or CM-1	<u>lemental Guidance</u> : Indications that warrant review of becific circumstances justifying such reviews may be of ganizations during the configuration change process. I B, CM-5, PE-6, PE-8.	f information system changes and obtained from activities carried out Related controls: AU-6, AU-7,
1208	СМ-5 (3) АССЕ	SS RESTRICTIONS FOR CHANGE SIGNED COMPONENTS	[BACK TO SCRM CONTROL]
1209 1210 1211	The softw softw digit	nformation system prevents the installation of [Ass are and firmware components] without verification ally signed using a certificate that is recognized and	<i>ignment: organization-defined</i> that the component has been l approved by the organization.
1212 1213 1214 1215 1216 1217 1218	Supp unles firmv syste comp organ contr	lemental Guidance: Software and firmware components s signed with recognized and approved certificates incovere vare version updates, patches, service packs, device dr m (BIOS) updates. Organizations can identify applical onents by type, by specific items, or a combination of sizational verification of such signatures, is a method co ols: CM-7, SC-13, SI-7.	its prevented from installation clude, for example, software and ivers, and basic input output ble software and firmware both. Digital signatures and of code authentication. Related
1219	CM-5 (6) ACCESS RES	TRICTIONS FOR CHANGE LIMIT LIBRARY PRIVILEGES	[BACK TO SCRM CONTROL]
1220			
1221	The	organization limits privileges to change software re	sident within software libraries.
1222	<u>Supp</u>	lemental Guidance: Software libraries include privile	ged programs. Related control:
1223	AC-2		
1224	References	<u>y:</u> None.	
1225	Priority and	Baseline Allocation:	

		P1 LOW Not Selected	MOD CM-5	HIGH CM-5 (1) (2) (3)
1226				
1227	CM-6	CONFIGURATION SETTINGS		[Back to SCRM Control]
1228 1229		Control: The organization:		
1230 1231 1232 1233		a. Establishes and documents conf employed within the information <i>configuration checklists</i>] that re- requirements;	iguration settings for information n system using [<i>Assignment: or</i>] flect the most restrictive mode of	on technology products ganization-defined security consistent with operational
1234		b. Implements the configuration se	ettings;	
1235 1236 1237		c. Identifies, documents, and appro [Assignment: organization-defined organization-defined operational	oves any deviations from establi- ned information system component al requirements]; and	ished configuration settings for <i>ents</i>] based on [<i>Assignment</i> :
1238 1239		d. Monitors and controls changes t policies and procedures.	o the configuration settings in a	ccordance with organizational
1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1250 1251 1252 1253		Supplemental Guidance: Configurat hardware, software, or firmware com posture and/or functionality of the sy related configuration settings can be (e.g., database, electronic mail, author input/output devices (e.g., scanners, routers, gateways, voice and data sw operating systems, middleware, and impacting the security state of inform other security control requirements. settings; (ii) account, file, directory p protocols, services, and remote conn configuration settings and subsequer established settings become part of t	ion settings are the set of param ponents of the information syst ystem. Information technology p defined include, for example, n entication, web, proxy, file, don copiers, and printers), network itches, wireless access points, n applications. Security-related p nation systems including the pa Security-related parameters inclu- permission settings; and (iii) set ections. Organizations establish atly derive specific settings for i he systems configuration baseli	neters that can be changed in tem that affect the security products for which security- nainframe computers, servers nain name), workstations, components (e.g., firewalls, etwork appliances, sensors), arameters are those parameters rameters required to satisfy lude, for example: (i) registry tings for functions, ports, n organization-wide nformation systems. The ne.
1254 1255 1256 1257 1258 1259 1260 1261 1262 1263 1264 1265 1266 1267		Common secure configurations (also and hardening guides, security refere recognized, standardized, and establis for specific information technology p information system components to m can be developed by a variety of org product developers, manufacturers, w other organizations in the public and United States Government Configura CM-6 and other controls such as AC (SCAP) and the defined standards w provide an effective method to unique establishes federal policy on configur controls: AC-19, CM-2, CM-3, CM-	preferred to as security configurence guides, security technical i ished benchmarks that stipulate platforms/products and instructi- neet operational requirements. C anizations including, for examp- vendors, consortia, academia, in private sectors. Common secur- ation Baseline (USGCB) which -19 and CM-7. The Security Co- ithin the protocol (e.g., Commo- nely identify, track, and control ration requirements for federal 7, SI-4.	ration checklists, lockdown mplementation guides) provide secure configuration settings ons for configuring those Common secure configurations le, information technology dustry, federal agencies, and re configurations include the affects the implementation of ontent Automation Protocol n Configuration Enumeration) configuration settings. OMB information systems. Related
1268		Control Enhancements:		
1269				
1270 1271	СМ-6 (1)	CONFIGURATION SETTINGS AUTO APPLICATION / VERIFICATION	MATED CENTRAL MANAGEMENT /	[BACK TO SCRM CONTROL]

1272 1273 1274 1275 1276		The organization employs a configuration settings for [A components].	Automated mechanisms to centr Assignment: organization-define ated controls: CA-7, CM-4.	cally manage, apply, and verify ed information system
1277 1278	СМ-6 (2)	CONFIGURATION SETTINGS / RE CHANGES	SPOND TO UNAUTHORIZED	[BACK TO SCRM CONTROL]
1279 1280 1281		The organization employs [, respond to unauthorized ch <i>settings</i>].	Assignment: organization-defin anges to [Assignment: organiza	ed security safeguards] to ation-defined configuration
1282 1283 1284 1285		<u>Supplemental Guidance</u> : Res include, for example, alerting configuration settings, or in e Related controls: IR-4, SI-7.	ponses to unauthorized changes designated organizational perso xtreme cases, halting affected in	to configuration settings can nnel, restoring established formation system processing.
1286 1287		References: OMB Memoranda 07-11, nvd.nist.gov, checklists.nist.gov, www.	07-18, 08-22; NIST Special Publicat nsa.gov.	ions 800-70, 800-128; Web:
1288		Priority and Baseline Allocation:		
		P1 LOW CM-6	MOD CM-6	HIGH CM-6 (1) (2)
1290 1291 1292	CM-7	LEAST FUNCTIONALITY Control: The organization:		[Back to SCRM Control]
1293		a Configures the information sy	vstem to provide only essential c	anabilities [.] and
1294 1295 1296		 b. Prohibits or restricts the use of [Assignment: organization-deservices]. 	of the following functions, ports, <i>efined prohibited or restricted fu</i>	protocols, and/or services: nctions, ports, protocols, and/or
1297 1298 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1310 1311 1312 1313		Supplemental Guidance: Informat services. Some of the functions ar essential organizational operation convenient to provide multiple ser- increases risk over limiting the ser- organizations limit component fur- web servers, but not both). Organ systems or individual components services are candidates for elimina- auto-execute, and file sharing). Or and logical ports/protocols (e.g., U Transfer Protocol) on information unauthorized transfer of informati scanning tools, intrusion detection firewalls and host-based intrusion functions, ports, protocols, and se <u>Control Enhancements:</u>	tion systems can provide a wide ad services, provided by default, s (e.g., key missions, functions). rvices from single information sy rvices provided by any one comp actionality to a single function pa- izations review functions and ser a of information systems, to deter ation (e.g., Voice Over Internet H rganizations consider disabling u Jniversal Serial Bus, File Transfe systems to prevent unauthorized on, or unauthorized tunneling. Con and prevention systems, and en detection systems to identify an rvices. Related controls: AC-6, C	variety of functions and may not be necessary to support Additionally, it is sometimes ystem components, but doing so ponent. Where feasible, er device (e.g., email servers or vices provided by information rmine which functions and Protocol, Instant Messaging, mused or unnecessary physical er Protocol, and Hyper Text d connection of devices, organizations can utilize network d-point protections such as d prevent the use of prohibited CM-2, RA-5, SA-5, SC-7.
1314 1315	СМ-7 (4)	LEAST FUNCTIONALITY UNAUT BLACKLISTING	HORIZED SOFTWARE /	[BACK TO SCRM CONTROL]

1316 1317		The organization:
1318 1319		(a) Identifies [Assignment: organization-defined software programs not authorized to execute on the information system];
1320 1321		(b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and
1322 1323		(c) Reviews and updates the list of unauthorized software programs [Assignment: organization-defined frequency].
1324 1325 1326 1327 1328		<u>Supplemental Guidance</u> : The process used to identify software programs that are not authorized to execute on organizational information systems is commonly referred to as <i>blacklisting</i> . Organizations can implement CM-7 (5) instead of this control enhancement if whitelisting (the stronger of the two policies) is the preferred approach for restricting software program execution. Related controls: CM-6, CM-8, PM-5.
1329	СМ-7 (5)	LEAST FUNCTIONALITY AUTHORIZED SOFTWARE / WHITELISTING
1330		The organization:
1331 1332		(a) Identifies [Assignment: organization-defined software programs authorized to execute on the information system];
1333 1334		(b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and
1335 1336		(c) Reviews and updates the list of authorized software programs [Assignment: organization-defined frequency].
1337 1338 1339 1340 1341 1342		<u>Supplemental Guidance</u> : The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as <i>whitelisting</i> . In addition to whitelisting, organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution or at system startup. Related controls: CM-2, CM-6, CM-8, PM-5, SA-10, SC-34, SI-7.
1343		References: DoD Instruction 8551.01.
1344		Priority and Baseline Allocation:
		P1 LOW CM-7 MOD CM-7 (1) (2) (4) HIGH CM-7 (1) (2) (5)
1345		
1346	CM-8	INFORMATION SYSTEM COMPONENT INVENTORY [Back to SCRM Control]
1347 1348		Control: The organization:
1349		a. Develops and documents an inventory of information system components that:
1350		1. Accurately reflects the current information system;
1351		2. Includes all components within the authorization boundary of the information system;
1352		3. Is at the level of granularity deemed necessary for tracking and reporting; and
1353 1354		4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and
1355 1356		b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].

1357 1358 1359 1360 1361 1362 1363 1364 1365 1366	S cc su ir ir ir sc cc fc cc	upplemental Guidance: Organizations may choose to implement omponent inventories that include components from all organizations inch situations, organizations ensure that the resulting inventorial formation required for proper component accountability (e.g., information system owner). Information deemed necessary for en- aformation system components includes, for example, hardware offware license information, software version numbers, compon- omponents or devices, machine names and network addresses. or example, manufacturer, device type, model, serial number, a pontrols: CM-2, CM-6, PM-5.	ent centralized information system zational information systems. In es include system-specific information system association, effective accountability of e inventory specifications, nent owners, and for networked Inventory specifications include, nd physical location. Related
1367	<u>C</u>	ontrol Enhancements:	
1368 1369	CM-8 (1) INI	FORMATION SYSTEM COMPONENT INVENTORY UPDATES DURING INSTALLATIONS / REMOVALS	[BACK TO SCRM CONTROL]
1370 1371 1372		The organization updates the inventory of information s integral part of component installations, removals, and i	system components as an information system updates.
1373 1374	СМ-8 (2)	INFORMATION SYSTEM COMPONENT INVENTORY / AUTOMATED MAINTENANCE	[BACK TO SCRM CONTROL]
1375 1376 1377 1378 1379 1380 1381 1382 1383 1384		The organization employs automated mechanisms to hele complete, accurate, and readily available inventory of in <u>Supplemental Guidance</u> : Organizations maintain information feasible. Virtual machines, for example, can be difficult to re- not visible to the network when not in use. In such cases, or date, complete, and accurate an inventory as is deemed reass can be satisfied by the implementation of CM-2 (2) for organitor information system component inventory and baseline confi- control: SI-7.	Ip maintain an up-to-date, aformation system components. on system inventories to the extent monitor because such machines are ganizations maintain as up-to- onable. This control enhancement anizations that choose to combine iguration activities. Related
1385 1386	СМ-8 (4)	INFORMATION SYSTEM COMPONENT INVENTORY ACCOUNTABILITY INFORMATION	[BACK TO SCRM CONTROL]
1387 1388 1389 1390 1391 1392 1393 1394 1395		The organization includes in the information system cor a means for identifying by [Selection (one or more): nam responsible/accountable for administering those compor <u>Supplemental Guidance</u> : Identifying individuals who are be for administering information system components helps to be components are properly administered and organizations ca action is required (e.g., component is determined to be the s component needs to be recalled/replaced, or component needs	nponent inventory information , <i>e; position; role</i>], individuals nents. oth responsible and accountable ensure that the assigned n contact those individuals if some source of a breach/compromise, eds to be relocated).
1396 1397	СМ-8 (б)	INFORMATION SYSTEM COMPONENT INVENTORY ASSESSED CONFIGURATIONS / APPROVED DEVIATIONS	[BACK TO SCRM CONTROL]
1398 1399 1400 1401		The organization includes assessed component configurations to current deployed configurations in the info inventory.	ations and any approved ormation system component

1402 1403 1404 1405		Supplemental Guidance: T established by organization have been assessed to deten approved deviations from e	his control enhancement focuses as for information system compor- rmine compliance with the require established configuration settings.	on configuration settings nents, the specific components that ed configuration settings, and any Related controls: CM-2, CM-6.
1406 1407	СМ-8 (7)	INFORMATION SYSTEM COMI REPOSITORY	PONENT INVENTORY CENTRALIZED	[BACK TO SCRM CONTROL]
1408 1409 1410		The organization provide system components.	s a centralized repository for th	e inventory of information
1411 1412 1413 1414 1415 1416 1417 1418 1419		Supplemental Guidance: C system component invento systems. Centralized repos opportunities for efficienci firmware assets. Such repo and responsible individuals are otherwise in need of mi inventories include system. (e.g., information system a	Organizations may choose to impl ries that include components from itories of information system com- es in accounting for organizations sitories may also help organizations of system components that have itigation actions. Organizations en- specific information required for ssociation, information system ov	ement centralized information all organizational information apponent inventories provide al hardware, software, and ons rapidly identify the location been compromised, breached, or asure that the resulting centralized proper component accountability wner).
1420 1421	СМ-8 (8)	INFORMATION SYSTEM COM LOCATION TRACKING	PONENT INVENTORY AUTOMATED	[BACK TO SCRM CONTROL]
1422 1423 1424		The organization employ system components by ge	s automated mechanisms to sup ographic location.	port tracking of information
1425 1426 1427 1428 1429		Supplemental Guidance: T information system compo capability may also help or individuals of system comp need of mitigation actions.	The use of automated mechanisms nents can increase the accuracy o ganizations rapidly identify the lo ponents that have been compromi	to track the location of f component inventories. Such ocation and responsible sed, breached, or are otherwise in
1430 1431	СМ-8 (9)	INFORMATION SYSTEM COMF COMPONENTS TO SYSTEMS	ONENT INVENTORY ASSIGNMENT O	F [BACK TO SCRM CONTROL]
1432 1433		The organization:		
1434 1435		(a) Assigns [Assignment: to an information sys	organization-defined acquired i tem; and	nformation system components]
1436 1437		(b) Receives an acknowle assignment.	edgement from the information	system owner of this
1438 1439 1440 1441		Supplemental Guidance: C system components (e.g., r controllers, and network de control: SA-4.	Organizations determine the criter nicroprocessors, motherboards, so evices) that are subject to this con	ia for or types of information oftware, programmable logic trol enhancement. Related
1442 1443		<u>References</u> : NIST Special Publicat Priority and Baseline Allocation:	ion 800-128.	
-		P1 LOW CM-8	MOD CM-8 (1) (3) (5)	HIGH CM-8 (1) (2) (3) (4) (5)

1445	СМ-9	CON	FIGURATION MANAGEMENT PLA	N	[Back to SCRM Control]
1446					
1447 1448		<u>Cont</u> plan	<u>rol</u> : The organization develops, for the information system that:	documents, and implements a	configuration management
1449		a.	Addresses roles, responsibilities,	, and configuration managemer	nt processes and procedures;
1450 1451		b .	Establishes a process for identify life cycle and for managing the c	ving configuration items throug configuration of the configurati	hout the system development on items;
1452 1453		c .	Defines the configuration items tunder configuration managemen	for the information system and t; and	places the configuration items
1454		d .	Protects the configuration manag	gement plan from unauthorized	disclosure and modification.
$\begin{array}{c} 1455\\ 1456\\ 1457\\ 1458\\ 1459\\ 1460\\ 1461\\ 1462\\ 1463\\ 1464\\ 1465\\ 1466\\ 1467\\ 1468\\ 1469\\ 1470\\ 1471\\ 1472\\ 1473\\ \end{array}$		Supp confi plans supp mana deve proce comp to de const temp subse appro and a impa infor mana confi to be	elemental Guidance: Configurati iguration management policies w s define detailed processes and p ort system development life cycl agement plans are typically deve lopment life cycle. The plans des esses, how to update configuration ponent inventories, how to contra- evelop, release, and update key de istent and timely development and plates can represent a master com- ets of the plan implemented on a oval processes include designation approving proposed changes to in the tanalyses prior to the impleme mation system items (hardware, aged. As information systems co iguration items may be identified to under configuration control. Re	ion management plans satisfy t while being tailored to individua rocedures for how configuration le activities at the information s loped during the development/ scribe how to move changes th on settings and baselines, how ol development, test, and opera ocuments. Organizations can e nd implementation of configura figuration management plan fo system by system basis. Confi on of key management stakeho nformation systems, and person ntation of changes to the syster software, firmware, and docum ntinue through the system deve and some existing configurati lated controls: CM-2, CM-3, C	he requirements in al information systems. Such on management is used to system level. Configuration acquisition phase of the system rough change management to maintain information system attional environments, and how mploy templates to help ensure attion management plans. Such r the organization at large with guration management lders responsible for reviewing nuel that conduct security ms. Configuration items are the nentation) to be configuration- elopment life cycle, new on items may no longer need 2M-4, CM-5, CM-8, SA-10.
1474		<u>Contr</u>	ol Enhancements:		
1475 1476	СМ-9 (1)		CONFIGURATION MANAGEMENT PL RESPONSIBILITY	AN / ASSIGNMENT OF	[BACK TO SCRM CONTROL]
1477 1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1489		Refer Priori	The organization assigns responses to organizational personal development. Supplemental Guidance: In the assigned within organizations, symanagement processes using performent degree of independence integration processes and configure or effective oversight. Tences: NIST Special Publication 800 ty and Baseline Allocation:	onsibility for developing the connel that are not directly investigation of dedicated configurate developers may be tasked exponnel who are not directly investigation of duties ensures that organization e between the information system and gement processes 0-128.	onfiguration management rolved in information system ion management teams d to develop configuration volved in system development ons establish and maintain a em development and to facilitate quality control and
		P1	LOW Not Selected	MOD CM-9	HIGH CM-9

1491	CM-10	SOFTWARE USAGE RESTRICTIONS		[Back to SCRM Control]
1492		Control: The organization:		
1493 1494		a. Uses software and associated d copyright laws;	ocumentation in accordance with	h contract agreements and
1495 1496		b. Tracks the use of software and control copying and distribution	associated documentation protection; and	cted by quantity licenses to
1497 1498 1499		c. Controls and documents the use capability is not used for the un of copyrighted work.	e of peer-to-peer file sharing tech authorized distribution, display,	hnology to ensure that this performance, or reproduction
1500 1501 1502		<u>Supplemental Guidance</u> : Software simple spreadsheets) or automated rorganizational needs. Related control	license tracking can be accomplenethods (e.g., specialized trackinols: AC-17, CM-8, SC-7.	ished by manual methods (e.g., ng applications) depending on
1503		Control Enhancements:		
1504 1505	СМ-10 (1)	SOFTWARE USAGE RESTRICTIONS [<u>BACK TO SCRM CONTROL]</u>	OPEN SOURCE SOFTWARE	
1506 1507 1508		The organization establishes the f [Assignment: organization-defined	ollowing restrictions on the us <i>restrictions</i>].	e of open source software:
1509 1510 1511 1512 1513 1514 1515		Supplemental Guidance: Open sour form. Certain software rights norma software license agreements that per From a security perspective, the ma organizations with the ability to exa licensing issues associated with ope derivative use of such software.	rece software refers to software the lly reserved for copyright holde rmit individuals to study, change jor advantage of open source soft mine the source code. However, n source software including, for	at is available in source code rs are routinely provided under e, and improve the software. ftware is that it provides , there are also various example, the constraints on
1516		References: None.		
1517		Priority and Baseline Allocation:		
		P2 LOW CM-10	MOD CM-10	HIGH CM-10
1518				
1519	CM-11	USER-INSTALLED SOFTWARE		[Back to SCRM Control]
1520		Control: The organization:		
1521 1522 1523 1524 1525		 a. Establishes [Assignment: organ by users; b. Enforces software installation p and c. Monitors policy compliance at 	<i>uization-defined policies</i>] govern policies through [<i>Assignment: or</i> [<i>Assignment: organization-defin</i>]	ing the installation of software ganization-defined methods];
1526 1527 1528 1529 1530 1531 1532 1533 1534		Supplemental Guidance: If provide software in organizational informati installed, organizations identify per Permitted software installations may software and downloading applicati software installations may include, software that organizations consider governing user-installed software m entity. Policy enforcement methods	d the necessary privileges, users ion systems. To maintain contro mitted and prohibited actions reg y include, for example, updates a ons from organization-approved for example, software with unkn potentially malicious. The poli- ay be organization-developed of include procedural methods (e.g	have the ability to install l over the types of software garding software installation. and security patches to existing "app stores." Prohibited nown or suspect pedigrees or cies organizations select r provided by some external g., periodic examination of user

1535 1536	accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both. Related controls: AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4.						
1537							
1538	Priority and Baseline Allocation:						
	P1	LOW CM-11	MOD CM-11	HIGH CM-11			

APPENDIX E	
------------	--

1539 FAMILY: CONTINGENCY PLANNING

1540	CP-1	CONTIN	GENCY PLANNING POLICY A	ND PROCEDURES	[Back to SCRM Control]		
1541		Control: The organization:					
1542 1543		a. Develops, documents, and disseminates to [<i>Assignment: organization-defined personnel or roles</i>]:					
1544 1545 1546		1.	A contingency planning pol management commitment, c and	icy that addresses purpose, sco coordination among organization	pe, roles, responsibilities, onal entities, and compliance;		
1547 1548		2.	Procedures to facilitate the i associated contingency plan	mplementation of the continge ning controls; and	ncy planning policy and		
1549		b. Rev	views and updates the current				
1550		1.	Contingency planning polic	y [Assignment: organization-d	efined frequency]; and		
1551		2.	Contingency planning proce	edures [Assignment: organizati	on-defined frequency].		
1553 1554 1555 1556 1557 1558 1559 1560 1561 1562 1563 1564		effective implementation of selected security controls and control enhancements in the CP family Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, car be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. <u>Control Enhancements:</u> None. <u>References</u> : Federal Continuity Directive 1; NIST Special Publications 800-12, 800-34, 800-100. Priority and Baseline Allocation:					
		P1 I	LOW CP-1	MOD CP-1	HIGH CP-1		
1565							
1566	CP-2	CONTIN	IGENCY PLAN [Back to SCH	<u>RM Control]</u>			
1567							
1568		<u>Control</u>	: The organization:				
1569		a. De	velops a contingency plan for	the information system that:			
1570 1571		1.	Identifies essential missions requirements;	and business functions and as	sociated contingency		
1572		2.	Provides recovery objective	s, restoration priorities, and me	etrics;		
1573 1574		3.	Addresses contingency roles information;	s, responsibilities, assigned ind	ividuals with contact		
1575 1576		4.	Addresses maintaining esset system disruption, compron	ntial missions and business fun nise, or failure;	ctions despite an information		
1577 1578		5.	Addresses eventual, full info security safeguards original	ormation system restoration wi ly planned and implemented; a	thout deterioration of the nd		

1579	6. Is reviewed and approved by [Assignment: organization-defined personnel or roles];
1580 1581	b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];
1582	c. Coordinates contingency planning activities with incident handling activities;
1583 1584	d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency];
1585 1586 1587	e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
1588 1589	f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and
1590	g. Protects the contingency plan from unauthorized disclosure and modification.
1591 1592 1593 1594 1595 1596 1597 1598 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1610	Supplemental Guidance: Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. Related controls: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11.
1611	Control Enhancements:
1612 1613	CP-2 (7) CONTINGENCY PLAN / COORDINATE WITH EXTERNAL SERVICE PROVIDERS [BACK TO SCRM CONTROL]
1614 1615 1616 1617	The organization coordinates its contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.
1617 1618 1619 1620 1621 1622	Supplemental Guidance: When the capability of an organization to successfully carry out its core missions/business functions is dependent on external service providers, developing a timely and comprehensive contingency plan may become more challenging. In this situation, organizations coordinate contingency planning activities with the external entities to ensure that the individual plans reflect the overall contingency needs of the organization. Related control: SA-9.
1623	CP-2 (8) CONTINGENCY PLAN / IDENTIFY CRITICAL ASSETS [BACK TO SCRM CONTROL]
1624	
1625	The organization identifies critical information system assets supporting essential
1626	missions and business functions.

1627 1628 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1640 1641		<u>Supplemental Guidance</u> : Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Organizations identify critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted during contingency operations. In addition, the identification of critical information assets facilitates the prioritization of organizational resources. Critical information system assets include technical and operational aspects. Technical aspects include, for example, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures). Organizational program protection plans can provide assistance in identifying critical assets. Related controls: SA-14, SA-15.				
1642		Priority and Baseline Allocation:				
		P1 LOW CP-2 MOD CP-2 (1) (3) (8) HIGH CP-2 (1) (2) (3) (4) (5) (8)				
1643						
1644	CP-6	ALTERNATE STORAGE SITE [Back to SCRM Control]				
1645						
1646		Control: The organization:				
1647 1648		a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and				
1649 1650		b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.				
1651 1652 1653 1654 1655 1656 1657 1658		<u>Supplemental Guidance</u> : Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2, CP-7, CP-9, CP-10, MP-4.				
1659		References: NIST Special Publication 800-34.				
1000		Priority and Baseline Allocation:				
		P1 LOW Not Selected MOD CP-6 (1) (3) HIGH CP-6 (1) (2) (3)				
1661						
1662	CP-7	ALTERNATE PROCESSING SITE [Back to SCRM Control]				
1663		Control: The organization:				
1664 1665 1666 1667 1668		a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [<i>Assignment: organization-defined information system operations</i>] for essential missions/business functions within [<i>Assignment: organization-defined time period</i> <i>consistent with recovery time and recovery point objectives</i>] when the primary processing capabilities are unavailable;				

capabilities are unavailable;

1669 1670 1671		b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and						
1672 1673		c.	c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.					
1674 1675 1676 1677 1678 1679 1680 1681 1682 1683		Sup prir that agre and pers requ disr CP-	Supplemental Guidance: Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available. Items covered by alternate processing site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination for the transfer/assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6.					
1684		Refe	erences: NIST Special Publication 80	0-34.				
1685		<u>Prio</u>	rity and Baseline Allocation:					
		P1	LOW Not Selected	MOD CP-7 (1) (2) (3)	HIGH CP-7 (1) (2) (3) (4)			
1686 1687								
1688	CP-8	TEL	LECOMMUNICATIONS SERVICES		[Back to SCRM Control]			
1689								
1690 1691 1692 1693 1694		Cor agre ope defi the	<u>Control</u> : The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [<i>Assignment: organization-defined information system operations</i>] for essential missions and business functions within [<i>Assignment: organization-defined time period</i>] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.					
1695 1696 1697 1698 1699 1700 1701 1702 1703		<u>Supplemental Guidance</u> : This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary/alternate sites. Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits/lines or satellites in lieu of ground-based communications. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements. Related controls: CP-2, CP-6, CP-7.						
1704		Control Enhancements:						
1705								
1706 1707	CP-8 (3)		TELECOMMUNICATIONS SERVICES ALTERNATE PROVIDERS	SEPARATION OF PRIMARY /	[BACK TO SCRM CONTROL]			
1708 1709 1710 1711 1712 1713			The organization obtains alternate from primary service providers to <u>Supplemental Guidance</u> : Threats th in organizational assessments of failures, hostile cyber/physical a	e telecommunications services fr reduce susceptibility to the same hat affect telecommunications s risk and include, for example, ttacks, and errors of omission/o	om providers that are separated e threats. services are typically defined natural disasters, structural commission. Organizations			

1714 1715 1716 1717 1718		seek to reduce common susceptibilitie among telecommunications service pro- between services. Organizations may of where the service provider can provide separation needs addressed in the risk	s by, for example, minimi oviders and achieving suf consider using a single ser e alternate telecommunica assessment.	izing shared infrastructure ficient geographic separation rvice provider in situations ations services meeting the
1719	CP-8 (4)	TELECOMMUNICATIONS SERVICES PROV	IDER CONTINGENCY PLAN	[BACK TO SCRM CONTROL]
1720 1721		The organization:		
1722 1723		(a) Requires primary and alternate contingency plans;	e telecommunications ser	vice providers to have
1724 1725		(b) Reviews provider contingency p contingency requirements; and	lans to ensure that the p	olans meet organizational
1726 1727		(c) Obtains evidence of contingency <i>organization-defined frequency</i>].	y testing/training by pro	viders [Assignment:
1728 1729 1730 1731 1732 1733 1734		<u>Supplemental Guidance</u> : Reviews of p nature of such plans. In some situation sufficient evidence for organizations to service providers may also participate with the Department of Homeland Sec use these types of activities to satisfy e contingency plan reviews, testing, and	provider contingency plan as, a summary of provider o satisfy the review requir in ongoing disaster recov curity, state, and local gov evidentiary requirements a training.	as consider the proprietary contingency plans may be rement. Telecommunications ery exercises in coordination rernments. Organizations may related to service provider
1735 1736 1737		<u>References</u> : NIST Special Publication 800-34; N tsp.ncs.gov.	National Communications Sys	stems Directive 3-10; Web:
1738		Priority and Baseline Allocation:		
		P1 LOW Not Selected MOD	CP-8 (1) (2)	HIGH CP-8 (1) (2) (3) (4)
1 = 2 0				

1740 FAMILY: IDENTIFICATION AND AUTHENTICATION

1741 1742	IA-1	IDENTIFICATION AND AUTHENTICA PROCEDURES	TION POLICY AND	[Back to SCRM Control]			
1743		Control: The organization:					
1744 1745		a. Develops, documents, and disse <i>roles</i>]:	minates to [Assignment: organi	zation-defined personnel or			
1746 1747 1748		 An identification and auther responsibilities, management and compliance; and 	ntication policy that addresses p nt commitment, coordination ar	ourpose, scope, roles, nong organizational entities,			
1749 1750		2. Procedures to facilitate the and associated identification	implementation of the identificant and authentication controls; and	ation and authentication policy nd			
1751		b. Reviews and updates the curren	t:				
1752 1753		1. Identification and authentic and	ation policy [Assignment: organ	nization-defined frequency];			
1754 1755		2. Identification and authentic <i>frequency</i>].	ation procedures [Assignment: o	organization-defined			
1756 1757 1758 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769		Supplemental Guidance: This control ad effective implementation of selected Policy and procedures reflect applica policies, standards, and guidance. Se level may make the need for system- be included as part of the general inf be represented by multiple policies r procedures can be established for the systems, if needed. The organization policy and procedures. Related control Control Enhancements: None. <u>References</u> : FIPS Publication 20 800-76, 800-78, 800-100. <u>Priority and Baseline Allocation</u> :	dresses the establishment of pol security controls and control er able federal laws, Executive Orce curity program policies and pro- specific policies and procedure ormation security policy for orge effecting the complex nature of e security program in general an al risk management strategy is a rol: PM-9.	licy and procedures for the nhancements in the IA family. ders, directives, regulations, ocedures at the organization s unnecessary. The policy can ganizations or conversely, can certain organizations. The d for particular information a key factor in establishing 8 800-12, 800-63, 800-73,			
		P1 LOW IA-1	MOD IA-1	HIGH IA-1			
1770							
1771 1772	IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) [Back to SCRM Control]					
1773							
1774 1775		<u>Control</u> : The information system un processes acting on behalf of organiz	iquely identifies and authentica zational users).	tes organizational users (or			
1776 1777 1778 1779 1780 1780 1781 1782		Supplemental Guidance: Organizati deem to have equivalent status of en applies to all accesses other than: (i) 14; and (ii) accesses that occur throu authentication. Organizations may re (e.g., shared privilege accounts) or fe employ passwords, tokens, or biome	onal users include employees of pployees (e.g., contractors, gues accesses that are explicitly ider gh authorized use of group auth equire unique identification of in or detailed accountability of ind trics to authenticate user identif	r individuals that organizations t researchers). This control ntified and documented in AC- nenticators without individual ndividuals in group accounts ividual activity. Organizations ies, or in the case multifactor			

1783	authentication, or some combination thereof. Access to organizational information systems is
1784	defined as either local access or network access. Local access is any access to organizational
1785	information systems by users (or processes acting on behalf of users) where such access is
1786	obtained by direct connections without the use of networks. Network access is access to
1787	organizational information systems by users (or processes acting on behalf of users) where such
1788	access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type
1789	of network access that involves communication through external networks (e.g., the Internet).
1790	Internal networks include local area networks and wide area networks. In addition, the use of
1791	encrypted virtual private networks (VPNs) for network connections between organization-
1792	controlled endpoints and non-organization controlled endpoints may be treated as internal
1793	networks from the perspective of protecting the confidentiality and integrity of information
1794	traversing the network.
1795	Organizations can satisfy the identification and authentication requirements in this control by
1796	complying with the requirements in Homeland Security Presidential Directive 12 consistent with
1797	the specific organizational implementation plans. Multifactor authentication requires the use of
1798	two or more different factors to achieve authentication. The factors are defined as: (i) something
1799	you know (e.g. password personal identification number [PIN]); (ii) something you have (e.g.
1800	cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor
1801	solutions that require devices separate from information systems gaining access include, for
1802	example, hardware tokens providing time-based or challenge-response authenticators and smart
1803	cards such as the U.S. Government Personal Identity Verification card and the DoD common
1804	access card. In addition to identifying and authenticating users at the information system level
1805	(i.e., at logon), organizations also employ identification and authentication mechanisms at the
1806	application level, when necessary, to provide increased information security. Identification and
1807	authentication requirements for other than organizational users are described in IA-8. Related

1809
1810References:HSPD 12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special
Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web:
idmanagement.gov.

controls: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8.

1812 Priority and Baseline Allocation:

Р	21	LOW IA-2 (1) (12)	MOD IA-2 (1) (2) (3) (8) (11)	HIGH IA-2 (1) (2) (3) (4) (8) (9)
			(12)	(11) (12)

1813

1808

1814 IA-4 IDENTIFIER MANAGEMENT

[Back to SCRM Control]

1815 1816	Control: The organization manages information system identifiers by
1817 1818	 a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier;
1819	b. Selecting an identifier that identifies an individual, group, role, or device;
1820	c. Assigning the identifier to the intended individual, group, role, or device;
1821	d. Preventing reuse of identifiers for [Assignment: organization-defined time period]; and
1822	e. Disabling the identifier after [Assignment: organization-defined time period of inactivity].
1823 1824 1825 1826 1827	<u>Supplemental Guidance</u> : Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management
1828	activities of AC-2 use account names provided by IA-4. This control also addresses individual

1829 1830 1831 1832 1833		identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices. Related controls: AC-2, IA-2, IA-3, IA-5, IA-8, SC-37.					
1834		Cont	trol Enhancements:				
1835	IA-4 (6)		IDENTIFIER MANAGEMEN	T CROSS-ORGANIZATION	MANAGEMENT	<u> BACK TO SCR</u>	<u>M CONTROL]</u>
1836 1837			The organization coor organizations] for cros	dinates with [<i>Assignme</i> s-organization manage	<i>ent: organizatio</i> ement of identif	<i>n-defined external</i> fiers.	
1838 1839 1840 1841			Supplemental Guidance for organizations to app conducting cross-organi information.	: Cross-organization id ropriately identify indiv zation activities involvi	lentifier manage viduals, groups, i ing the processir	ment provides the c roles, or devices wh ng, storage, or trans	apability Ien mission of
1842							
1843		<u>Refe</u>	rences: FIPS Publication 2	01; NIST Special Publicatio	ons 800-73, 800-7	6, 800-78.	
1844		<u>Priori</u>	ity and Baseline Allocation:				
		P1	LOW IA-4	MOD IA-4		HIGH IA-4	
1845							
1846	IA-5	AUT	HENTICATOR MANAGEN	IENT		[Back to SCR	<u>M Control]</u>
1847							
1848		Cont	trol: The organization n	nanages information sys	stem authenticat	ors by:	
1849 1850		a.	Verifying, as part of the role, or device receiving	initial authenticator dis the authenticator;	stribution, the id	entity of the individ	lual, group,
1851		b.	Establishing initial auth	enticator content for aut	thenticators defi	ned by the organiza	ition;
1852		c.	Ensuring that authentica	tors have sufficient stre	ength of mechan	ism for their intend	ed use;
1853 1854		d.	d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;				
1855		e.	Changing default conter	nt of authenticators prior	r to information	system installation	.,
1856 1857		f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;					
1858 1859		g.	Changing/refreshing aut authenticator type];	henticators [Assignmen	t: organization-	defined time period	by
1860		h.	Protecting authenticator	content from unauthori	ized disclosure a	and modification;	
1861 1862		i.	Requiring individuals to protect authenticators; a	take, and having devic	es implement, s	pecific security safe	guards to
1863		j.	Changing authenticators	s for group/role account	s when member	ship to those accou	nts changes.
1864 1865 1866 1867 1868 1869		Supp biom the in pass defau authe	<u>elemental Guidance</u> : Ind netrics, PKI certificates, nitial password) as oppo word length). In many c ult authentication creder entication credentials ar	dividual authenticators i and key cards. Initial au used to requirements abc ases, developers ship in ntials to allow for initial e often well known, eas	include, for exar uthenticator con out authenticator formation system installation and ily discoverable	nple, passwords, to tent is the actual co r content (e.g., mini m components with configuration. Def , and present a sign	kens, ntent (e.g., mum factory àult ificant

1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1880 1881 1882 1883 1884 1885 1886		security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28.
1887 1888	IA-5 (5)	Control Ennancements: AUTHENTICATOR MANAGEMENT CHANGE AUTHENTICATORS PRIOR TO DELIVERY [BACK TO SCRM CONTROL]]
1889 1890 1891 1892 1893 1894 1895 1896 1897 1898 1899		The organization requires developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation. Supplemental Guidance: This control enhancement extends the requirement for organizations to change default authenticators upon information system installation, by requiring developers and/or installers to provide unique authenticators or change default authenticators for system components prior to delivery and/or installation. However, it typically does not apply to the developers of commercial off-the-shelve information technology products. Requirements for unique authenticators can be included in acquisition documents prepared by organizations when procuring information systems or system components.
1900 1901	IA-5 (9)	AUTHENTICATOR MANAGEMENT CROSS-ORGANIZATION CREDENTIAL MANAGEMENT[BACK TO SCRM CONTROL]
1902 1903 1904 1905 1906 1907 1908 1909		 The organization coordinates with [Assignment: organization-defined external organizations] for cross-organization management of credentials. <u>Supplemental Guidance</u>: Cross-organization management of credentials provides the capability for organizations to appropriately authenticate individuals, groups, roles, or devices when conducting cross-organization activities involving the processing, storage, or transmission of information. <u>References</u>: OMB Memoranda 04-04, 11-11; FIPS Publication 201; NIST Special Publications 800-73, 800-63, 800-76, 800-78, EICAM Roadmap and Implementation Guidance: Web: idmanagement dov
1910		Priority and Baseline Allocation:
1912		P1 LOW IA-5 (1) (11) MOD IA-5 (1) (2) (3) (11) HIGH IA-5 (1) (2) (3) (11)
1913	IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL

1914 USERS)

[Back to SCRM Control]

1915 1916	<u>Control</u> : The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).
1917 1918 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928	<u>Supplemental Guidance</u> : Non-organizational users include information system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to federal information systems with the need to protect and adequately mitigate risk. IA-2 addresses identification and authentication requirements for access to information systems by organizational users. Related controls: AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, DA-2, SA-12, SC-8.
1929 1930 1931 1932	<u>References</u> : OMB Memoranda 04-04, 11-11, 10-06-2011; FICAM Roadmap and Implementation Guidance; FIPS Publication 201; NIST Special Publications 800-63, 800-116; National Strategy for Trusted Identities in Cyberspace; Web: idmanagement.gov. <u>Priority and Baseline Allocation</u> :

	P1	LOW IA-8 (1) (2) (3) (4)	MOD IA-8 (1) (2) (3) (4)	HIGH IA-8 (1) (2) (3) (4)
1933				

1934 FAMILY: INCIDENT RESPONSE

1935	IR-1	INCIDE	ENT RESPONSE POLICY AND	PROCEDURES	[Back to SCRM Control]			
1936 1937		<u>Contro</u>	<u>l</u> : The organization:					
1938 1939		a. Develops, documents, and disseminates to [<i>Assignment: organization-defined personnel or roles</i>]:						
1940 1941 1942		1.	An incident response poli management commitmen and	cy that addresses purpose, scope, t, coordination among organizatio	roles, responsibilities, onal entities, and compliance;			
1943 1944		2.	Procedures to facilitate th incident response control	e implementation of the incident s; and	response policy and associated			
1945		b. Re	eviews and updates the curre	ent:				
1946		1.	Incident response policy	[Assignment: organization-define	d frequency]; and			
1947		2.	Incident response proced	ures [Assignment: organization-d	efined frequency].			
1948 1949 1950 1951 1952 1953 1954 1955 1956 1957		<u>Supplemental Guidance</u> : This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM 0						
1958		Contro	<u>l Enhancements:</u> None.					
1959		Referen	<u>nces:</u> NIST Special Publications	800-12, 800-61, 800-83, 800-100.				
1960		Priority :	and Baseline Allocation:					
10.64		P1	LOW IR-1	MOD IR-1	HIGH IR-1			
1961 1962	IR-4	INCIDE	ENT HANDLING					
1963		Contro	<u>l</u> : The organization:					
1964 1965		a. Im de	plements an incident handl tection and analysis, contain	ing capability for security inciden nment, eradication, and recovery;	ts that includes preparation,			
1966		b. Co	pordinates incident handling	activities with contingency plan	ning activities; and			
1967 1968		c. Inc pro	c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.					
1969 1970 1971 1972 1973 1974 1975		Supple on the suppor definiti Incider audit m reporte	mental Guidance: Organization capabilities of organization ted by those systems. There ion, design, and developmen nt-related information can b nonitoring, network monitor ed supply chain events. Effe	ations recognize that incident resp al information systems and the mi fore, organizations consider incident of mission/business processes a e obtained from a variety of source ring, physical access monitoring, ctive incident handling capability	onse capability is dependent ssion/business processes being ent response as part of the ind information systems. tes including, for example, user/administrator reports, and includes coordination among			

1976 1977 1978 1979		many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Relate control: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.					
1980 1981		Control Enhancements:					
1982	IR-4 (10)	INCIDENT HANDLING SUPPLY CH	IAIN COORDINATION	[BACK TO SCRM CONTROL]			
1983 1984		The organization coordinates with other organizations invol	incident handling activities in lved in the supply chain.	volving supply chain events			
1985 1986 1987 1988 1989 1990		Supplemental Guidance: Orgar example, system/product develo distributors, vendors, and resello compromises/breaches involvin products, development processe facilities.	nizations involved in supply cha opers, integrators, manufacturers ers. Supply chain incidents inclu- g information system componen- es or personnel, and distribution	in activities include, for s, packagers, assemblers, ude, for example, nts, information technology processes or warehousing			
1991		References: Executive Order 13587; NIS	ST Special Publication 800-61.				
1992		Priority and Baseline Allocation:					
1000		P1 LOW IR-4	MOD IR-4 (1)	HIGH IR-4 (1) (4)			
1993							
1994	IR-6	INCIDENT REPORTING					
1995		Control: The organization:					
1996 1997		a. Requires personnel to report sus response capability within [Assi	spected security incidents to the ignment: organization-defined to	organizational incident <i>ime period</i>]; and			
1998		b. Reports security incident inform	nation to [Assignment: organiza	tion-defined authorities].			
1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009		Supplemental Guidance: The intent requirements within an organization agencies and their subordinate organ the receipt of suspicious email comm types of security incidents reported, reporting authorities reflect applicab policies, standards, and guidance. C specifically exempted from such req Computer Emergency Readiness Te US-CERT Concept of Operations for IR-4, IR-5, IR-8.	of this control is to address both and the formal incident reportin nizations. Suspected security inc nunications that can potentially the content and timeliness of the ble federal laws, Executive Orde urrent federal policy requires that uirements) report security incid am (US-CERT) within specified or Federal Cyber Security Incide	h specific incident reporting ng requirements for federal idents include, for example, contain malicious code. The e reports, and the designated rs, directives, regulations, at all federal agencies (unless ents to the United States I time frames designated in the nt Handling. Related controls:			
2010		Control Enhancements:					
2011	IR-6 (3)	INCIDENT REPORTING COORDIN	ATION WITH SUPPLY CHAIN	[BACK TO SCRM CONTROL]			
2012 2013 2014 2015		The organization provides sec in the supply chain for inform to the incident.	curity incident information to aation systems or information	other organizations involved system components related			
2016 2017 2018 2019		<u>Supplemental Guidance</u> : Orgar example, system/product develo distributors, vendors, and resello compromises/breaches involvin	nizations involved in supply cha opers, integrators, manufacturers ers. Supply chain incidents inclu g information system componen	in activities include, for s, packagers, assemblers, ide, for example, nts, information technology			

2020 2021 2022 2023		r f g i	products, development processe acilities. Organizations determi gained from support by external nformation being released to ou	s or personnel, and distribution ne the appropriate information organizations with the potentia itside organizations of perhaps	processes or warehousing to share considering the value Il for harm due to sensitive questionable trustworthiness.		
2024		Refere	ences: NIST Special Publication 80	0-61: Web: www.us-cert.gov.			
2025		<u>Priorit</u>	y and Baseline Allocation:				
		P1	LOW IR-6	MOD IR-6 (1)	HIGH IR-6 (1)		
2026							
2027	IR-9	INFO	RMATION SPILLAGE RESPONSE		[Back to SCRM Control]		
2028							
2029		Contr	<u>col</u> : The organization responds	to information spills by:			
2030		a. I	dentifying the specific information	tion involved in the information	system contamination;		
2031 2032		b. A	Alerting [Assignment: organization not a method of communication not	tion-defined personnel or roles] associated with the spill;	of the information spill using		
2033		c. Isolating the contaminated information system or system component;					
2034		d. Eradicating the information from the contaminated information system or component;					
2035 2036		e. Identifying other information systems or system components that may have been subsequently contaminated; and					
2037		f. I	Performing other [Assignment: of	organization-defined actions].			
2038 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049		<u>Supplemental Guidance</u> : Information spillage refers to instances where either classified or sensitive information is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. At that point, corrective action is required. The nature of the organizational response is generally based upon the degree of sensitivity of the spilled information (e.g., security category or classification level), the security capabilities of the information system, the specific nature of contaminated storage media, and the access authorizations (e.g., security clearances) of individuals with authorized access to the contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such					
2050							
2051		Refere	ences: None.				
2052		<u>Priorit</u>	y and Baseline Allocation:				
		P0	LOW Not Selected	MOD Not Selected	HIGH Not Selected		

2054 **FAMILY: MAINTENANCE**

2055	MA-1	SYSTEM MAINTENANCE POLICY AND	PROCEDURES	[Back to SCRM Control]			
2056							
2057		Control: The organization:					
2058 2059		a. Develops, documents, and dissen <i>roles</i>]:	ninates to [Assignment: organ	ization-defined personnel or			
2060 2061 2062		1. A system maintenance polic management commitment, c and	y that addresses purpose, scop oordination among organization	e, roles, responsibilities, onal entities, and compliance;			
2063 2064		2. Procedures to facilitate the in associated system maintenant	nplementation of the system race controls; and	naintenance policy and			
2065		b. Reviews and updates the current:					
2066		1. System maintenance policy	Assignment: organization-dep	fined frequency]; and			
2067		2. System maintenance procedu	ares [Assignment: organizatio	n-defined frequency].			
2068 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080		Supplemental Guidance: This contro effective implementation of selected s family. Policy and procedures reflect regulations, policies, standards, and g organization level may make the need The policy can be included as part of conversely, can be represented by mu organizations. The procedures can be particular information systems, if nee factor in establishing policy and proce <u>Control Enhancements:</u> None. <u>References:</u> NIST Special Publications 80 <u>Priority and Baseline Allocation:</u>	addresses the establishment of security controls and control e applicable federal laws, Exect uidance. Security program po l for system-specific policies a the general information securi ltiple policies reflecting the co established for the security pr ded. The organizational risk n edures. Related control: PM-9 0-12, 800-100.	of policy and procedures for the nhancements in the MA utive Orders, directives, licies and procedures at the and procedures unnecessary. ity policy for organizations or omplex nature of certain rogram in general and for nanagement strategy is a key			
2001		P1 LOW MA-1	MOD MA-1	HIGH MA-1			
2081							
2082	MA-2	CONTROLLED MAINTENANCE					
2083		Control: The organization:					
2084 2085 2086		 Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements: 					
2087 2088		b. Approves and monitors all maint whether the equipment is service	enance activities, whether per d on site or removed to anothe	formed on site or remotely and er location;			
2089 2090 2091		c. Requires that [<i>Assignment: organ</i> removal of the information system off-site maintenance or repairs;	<i>nization-defined personnel or</i> m or system components from	<i>roles</i>] explicitly approve the organizational facilities for			
2002		d Somitizes againment to remove al	1 information from accounted	madia prior to removal from			

2092d.Sanitizes equipment to remove all information from associated media prior to removal from
organizational facilities for off-site maintenance or repairs;

2095		e. C fi	checks all potentially im unctioning properly foll	pacted security controls to verify that owing maintenance or repair actions	it the controls are still ; and
2096 2097		f. In	ncludes [Assignment: or rganizational maintenar	rganization-defined maintenance-relance records.	ated information] in
2098 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2110		Supple system (inclu house direct copier for ex mainta and (v numbe the sec issues CM-4	emental Guidance: This c n maintenance program ding applications) cond s, software maintenance ly associated with infor- rs, and printers. Informa ample: (i) date and time enance; (iii) name of es y) information system co ers, if applicable). The l curity categories of orga a associated with replace y, MA-4, MP-6, PE-16, T	control addresses the information sector and applies to all types of maintenan lucted by any local or nonlocal entity agreement). System maintenance als mation processing and/or data/inform ation necessary for creating effective e of maintenance; (ii) name of individ cort, if necessary; (iv) a description of omponents/equipment removed or re level of detail included in maintenance anizational information systems. Org ement components for information sys SA-12, SI-2.	urity aspects of the information nee to any system component (e.g., in-contract, warranty, in- so includes those components not nation retention such as scanners, maintenance records includes, duals or group performing the of the maintenance performed; placed (including identification ce records can be informed by ganizations consider supply chain ystems. Related controls: CM-3,
2111		<u>Contro</u>	I Enhancements:		
2112 2113	MA-2 (2)	C A	CONTROLLED MAINTENAN CTIVITIES	CE AUTOMATED MAINTENANCE	[BACK TO SCRM CONTROL]
2114		Т	The organization:		
2115 2116		(8	a) Employs automated and repairs; and	d mechanisms to schedule, conduct	t, and document maintenance
2117		(1	b) Produces up-to dat	e, accurate, and complete records	of all maintenance and repair
1110					1
2118 2119		S	actions requested, s	scheduled, in process, and complete Related controls: CA-7 MA-3	ed.
2118 2119 2120		<u>S</u> <u>Refere</u>	actions requested, s upplemental Guidance: ences: None.	scheduled, in process, and complete Related controls: CA-7, MA-3.	ed.
2118 2119 2120 2121		<u>S</u> <u>Refere</u> <u>Priority</u>	actions requested, s upplemental Guidance: ences: None. and Baseline Allocation:	scheduled, in process, and complete records scheduled, in process, and complete Related controls: CA-7, MA-3.	ed.
2118 2119 2120 2121		<u>S</u> <u>Refere</u> <u>Priority</u> P2	actions requested, s supplemental Guidance: ences: None. and Baseline Allocation: LOW MA-2	Related controls: CA-7, MA-3.	HIGH MA-2 (2)
21182119212021212122		<u>S</u> <u>Refere</u> <u>Priority</u> P2	actions requested, s supplemental Guidance: ences: None. and Baseline Allocation: LOW MA-2	Scheduled, in process, and complete Related controls: CA-7, MA-3. MOD MA-2	HIGH MA-2 (2)
 2118 2119 2120 2121 2122 2122 2123 	MA-3	<u>S</u> Refere Priority P2 MAIN	actions requested, s supplemental Guidance: ences: None. and Baseline Allocation: LOW MA-2	MOD MA-2	HIGH MA-2 (2) [Back to SCRM Control]
 2118 2119 2120 2121 2122 2122 2123 2124 	MA-3	<u>S</u> <u>Refere</u> <u>Priority</u> <u>P2</u> <u>MAIN</u>	actions requested, s supplemental Guidance: ences: None. and Baseline Allocation: LOW MA-2 TENANCE TOOLS	MOD MA-2	HIGH MA-2 (2) [Back to SCRM Control] ration system maintenance tools.
 2118 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2130 2131 2132 2133 2134 2135 	MA-3	S Refere Priority P2 MAIN Contro Supple tools to Maint facilit for ex This c mainte "ipcon Relate Contro	actions requested, s supplemental Guidance: ances: None. and Baseline Allocation: LOW MA-2 TENANCE TOOLS a: The organization app emental Guidance: This c used specifically for dia tenance tools can includ tial vehicles for transpo y and subsequently into ample, hardware/softwa control does not cover h enance, yet are a part of nfig," or the hardware a ed controls: MA-2, MA- of Enhancements:	MOD MA-2 MOD MA-2 MOD MA-2 more solution of the solution of th	HIGH MA-2 (2) [Back to SCRM Control] ation system maintenance tools. tes associated with maintenance trational information systems. atiems. Maintenance tools are ally or unintentionally, into a Maintenance tools can include, rdware/software packet sniffers. may support information system re implementing "ping," "ls," oring port of an Ethernet switch.
 2118 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2130 2131 2132 2133 2134 2135 2136 	MA-3	S Refere Priority P2 MAIN Contro Supple tools to Maint potent facilit for ex This c maint "ipcon Relate Contro	actions requested, s supplemental Guidance: ances: None. and Baseline Allocation: LOW MA-2 TENANCE TOOLS a: The organization app emental Guidance: This c used specifically for dia tenance tools can includ tial vehicles for transpo- y and subsequently into ample, hardware/softwa control does not cover h enance, yet are a part of nfig," or the hardware a ed controls: MA-2, MA- ble Enhancements:	MOD MA-2 MOD MA-2 MOD MA-2 MOD MA-2	HIGH MA-2 (2) [Back to SCRM Control] ation system maintenance tools. tes associated with maintenance tational information systems. titems. Maintenance tools are ally or unintentionally, into a Maintenance tools can include, dware/software packet sniffers. may support information system re implementing "ping," "ls," oring port of an Ethernet switch.

2138 2139		The organization inspects the ma personnel for improper or unaut	intenance tools carried into horized modifications.	o a facility by maintenance
2140 2141 2142 2143		Supplemental Guidance: If, upon i that the tools have been modified in code, the incident is handled consist incident handling. Related control:	nspection of maintenance to n an improper/unauthorized n stent with organizational poli SI-7.	ols, organizations determine manner or contain malicious icies and procedures for
2144	MA-3 (2)	MAINTENANCE TOOLS INSPECT MEDI	A	[BACK TO SCRM CONTROL]
2145 2146 2147 2148		The organization checks media concerning the organization checks media concerning the media are used in Supplemental Guidance: If, upon i	ontaining diagnostic and te a the information system.	est programs for malicious
2149 2150 2151		test programs, organizations determ handled consistent with organization control: SI-3.	nine that the media contain n onal incident handling policie	nalicious code, the incident is es and procedures. Related
2152	MA-3 (3)	MAINTENANCE TOOLS / PREVENT UNA	UTHORIZED REMOVAL	[BACK TO SCRM CONTROL]
2153 2154		The organization prevents the un containing organizational inform	authorized removal of mai ation by:	ntenance equipment
2155		(a) Verifying that there is no org	ganizational information co	ontained on the equipment;
2156		(b) Sanitizing or destroying the e	equipment;	
2157		(c) Retaining the equipment with	hin the facility; or	
2158 2159		(d) Obtaining an exemption from explicitly authorizing remova	n [<i>Assignment: organization</i> al of the equipment from th	<i>n-defined personnel or roles</i>] ne facility.
2160 2161 2162		Supplemental Guidance: Organiza owned by organizations and inform serve as information stewards.	tional information includes a nation provided to organization	Il information specifically ons in which organizations
2163				
2164		References: NIST Special Publication 800-8	8.	
2165		Priority and Baseline Allocation:		
		P3 LOW Not Selected M	IOD MA-3 (1) (2)	HIGH MA-3 (1) (2) (3)
2166				
2167	MA-4	NONLOCAL MAINTENANCE		[Back to SCRM Control]
2168		Control: The organization:		
2169		a. Approves and monitors nonlocal m	aintenance and diagnostic ad	ctivities;
2170 2171		b. Allows the use of nonlocal mainten organizational policy and documen	ance and diagnostic tools or ted in the security plan for th	ly as consistent with ne information system;
2172 2173		c. Employs strong authenticators in th sessions;	e establishment of nonlocal	maintenance and diagnostic
2174		d. Maintains records for nonlocal mai	ntenance and diagnostic acti	vities; and
2175		e. Terminates session and network co	nnections when nonlocal ma	intenance is completed.
2176 2177		<u>Supplemental Guidance</u> : Nonlocal main conducted by individuals communicating	ntenance and diagnostic acting through a network, either	vities are those activities an external network (e.g., the

2178 2179 2180 2181 2182 2183 2184 2185 2186 2187		Inte carri in t req PK Enf AC 10,	ern rie npo he uir lay I w for 2-3, SC	et) or an in d out by in onent and r establishme ements in 1 v attacks an vhere certificing requir , AC-6, AC C-17.	ternal netw dividuals p not commu- nent of non IA-2. Typi- ad employ p ficates are s ements in 1 C-17, AU-2	vork. Loc hysically nicating a local mai cally, stro multifacto stored on MA-4 is a , AU-3, I	al maintenance present at the across a networ ntenance and d ong authenticatio a token protect accomplished in A-2, IA-4, IA-5	e and diagnostic information system k connection. A liagnostic session ion requires auton. Strong auther ted by a passwor n part by other 5, IA-8, MA-2,	controls MA-5, 1	es are those act nformation sys cation techniqu ct the network ors that are res s include, for e phrase, or bion . Relate control MP-6, PL-2, So	ivities tem les used access istant to xample, hetric. l: AC-2, C-7, SC-
2188		Cor	ntro	l Enhancem	ents:						
2189	MA-4 (2)		N	ONLOCAL M	IAINTENANG	CE DOCU	MENT NONLOCA	L MAINTENANCE	3 	BACK TO SCRM	<u>CONTROL]</u>
2190 2191 2192 2192			T ai co	he organiz nd proced onnections	zation doc ures for th s.	uments i 1e establi	n the security shment and us	plan for the in se of nonlocal i	lformati mainten	on system, the ance and diag	policies nostic
2193 2194		Ref	ere	nces: FIPS	Publications	s 140-2, 19	97, 201; NIST Sp	ecial Publications	s 800-63, i	800-88; CNSS P	olicy 15.
2195		Pric	ority	v and Baselin	ne Allocatior	<u>ı</u> :					
		P2	2	LOW MA	-4		MOD MA-4 (2	.)	HIGH	MA-4 (2) (3)	
2196											
2197	MA-5	MA	IN'	TENANCE I	PERSONNE	L				[Back to SCR	<u>M Control]</u>
2198											
2199		<u>Co</u> 1	ntro	ol: The org	ganization:						
2200 2201		a.	E ai	stablishes uthorized r	a process f naintenanc	or mainte e organiz	enance personne ations or perso	el authorization nnel;	1 and ma	intains a list of	
2202 2203		b.	E re	nsures that equired acc	t non-escor	ted perso	nnel performin and	g maintenance	on the ir	nformation syst	tem have
2204 2205 2206		c.	D co re	Designates of ompetence equired acc	organizatio to supervi cess author	nal perso se the ma izations.	onnel with requi	ired access auth vities of personn	norization nel who	ns and technica do not possess	ıl the
2207 2208 2209 2210 2211 2212 2213 2214 2215 2216 2217 2218 2219		Sur mai ind sys sup hav not mai org wit tem ver	ppl inte ivie tem erv ving pr nuf ani h li npo y li	emental Gr enance on o duals whose ns (e.g., cu vising indiv g required eviously ic facturers, v izational in ittle or no n orary crede imited time	uidance: T organizatio se maintena stodial stat viduals rela access auth lentified as rendors, syn formation notice. Bas ntials to the e periods. I	his contro onal infor- ance dutic ff, physica tes to the norization authoriz stems into systems, ed on org ese indivi Related co	ol applies to ind mation systems es place them v al plant mainten e maintenance p as refers to main ed maintenance egrators, and co for example, w ganizational ass iduals. Tempor pontrols: AC-2, 1	dividuals perfor s, while PE-2 ac vithin the physi nance personne performed on the ntenance on and e personnel, suc onsultants, may when required to essments of ris ary credentials IA-8, MP-2, PE	rming ha ddresses cal prote el). Techn ie inform d near th ch as infor require o conduc k, organ may be E-2, PE-2	ardware or soft physical acces ection perimete nical competen nation systems e systems. Indi ormation techn privileged acce t maintenance izations may is for one-time us 3, PE-4, RA-3.	ware s for r of the ce of while viduals ology ess to activities sue e or for
2220		Ref	ere	nces None	.						
2221		Pric	ority	and Baselir	ne Allocation) .					

		P2	LOW MA-5	MOD MA-5	HIGH MA-5 (1)			
2222								
2223	MA-6	TIME	LY MAINTENANCE		[Back to SCRM Control]			
2224 2225 2226		<u>Contro</u> organ time p	<u>اا:</u> The organization obtains ma <i>aization-defined information sy.</i> <i>period</i>] of failure.	intenance support and/or spare stem components] within [Assig	parts for [Assignment: nment: organization-defined			
2227 2228 2229 2230 2231		<u>Supplemental Guidance</u> : Organizations specify the information system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support typically include having appropriate contracts in place.						
2232 2233		<u>Refere</u> Priorit	ences: None. y and Baseline Allocation:					
2234		P2	LOW Not Selected	MOD MA-6	HIGH MA-6			

2235 FAMILY: MEDIA PROTECTION

2236	MP-1	MEDIA PROTECTION POLICY AND PROCED	URES	[Back to SCRM Control]				
2237 2238		<u>Control</u> : The organization:						
2239 2240		a. Develops, documents, and disseminate <i>roles</i>]:	es to [Assignment: organi	zation-defined personnel or				
2241 2242 2243		 A media protection policy that add management commitment, coordiand 	dresses purpose, scope, re nation among organizatio	bles, responsibilities, onal entities, and compliance;				
2244 2245		2. Procedures to facilitate the impler media protection controls; and	nentation of the media pr	otection policy and associated				
2246		b. Reviews and updates the current:						
2247		1. Media protection policy [Assignm	ent: organization-defined	lfrequency]; and				
2248		2. Media protection procedures [Ass	ignment: organization-de	fined frequency].				
2249 2250 2251 2252 2253 2254 2255 2256 2257 2258		<u>Supplemental Guidance</u> : This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing						
2259		Control Enhancements: None.						
2260		References: NIST Special Publications 800-12,	800-100.					
2261		Priority and Baseline Allocation:						
		P1 LOW MP-1 MOD	MP-1	HIGH MP-1				
2262 2263	MP-5	MEDIA TRANSPORT		[Back to SCRM Control]				
2264 2265		<u>Control</u> : The organization:						
2266 2267 2268		a. Protects and controls [<i>Assignment: org</i> during transport outside of controlled a <i>safeguards</i>];	ganization-defined types of areas using [Assignment:	of information system media] organization-defined security				
2269 2270		b. Maintains accountability for informatiareas;	on system media during t	ransport outside of controlled				
2271		c. Documents activities associated with t	he transport of information	on system media; and				
2272 2273		d. Restricts the activities associated with personnel.	the transport of informat	ion system media to authorized				
2274 2275		<u>Supplemental Guidance</u> : Information syste Digital media includes, for example, disket	em media includes both d tes, magnetic tapes, exter	igital and non-digital media. mal/removable hard disk				

2276 2277 2278 2279 2280 2281		drives, flash drives, compact disks, ar example, paper and microfilm. This c storage capability (e.g., smart phones areas. Controlled areas are areas or sp and/or procedural safeguards to meet and/or information systems.	nd digital video disks. Non-dig control also applies to mobile d , tablets, E-readers) that are tra paces for which organizations p the requirements established for	ital media includes, for evices with information nsported outside of controlled provide sufficient physical or protecting information			
2282 2283 2284 2285 2286 2287 2288 2289 2290 2291 2292 2293 2294 2295 2296 2297 2298		Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records. Related controls: AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28.					
2220		Potoronoog, EIDS Dublication 100, NIST	Special Publication 800 60				
22))		References. FIFS Fublication 199, NIST	Special Fublication 800-60.				
2300		P1 LOW Not Selected	MOD MP-5 (4)	HIGH MP-5 (4)			
2301							
2302	MP-6	MEDIA SANITIZATION		[Back to SCRM Control]			
2303		Control: The organization:					
2304 2305 2306 2307		a. Sanitizes [Assignment: organizat release out of organizational com defined sanitization techniques a organizational standards and pol	tion-defined information system trol, or release for reuse using [and procedures] in accordance icies; and	n media] prior to disposal, [Assignment: organization- with applicable federal and			
2308 2309		b. Employs sanitization mechanism security category or classification	ns with the strength and integrit n of the information.	y commensurate with the			
2310 2311 2312 2313 2314 2315 2316 2317 2318 2319 2320 2321		Supplemental Guidance: This contro non-digital, subject to disposal or reu Examples include media found in sca network components, and mobile dev media such that the information canno including clearing, purging, cryptogra information to unauthorized individu Organizations determine the appropri sometimes necessary when other met Organizations use discretion on the e	ol applies to all information systems, whether or not the media is se, whether or not the media is unners, copiers, printers, noteborices. The sanitization process is ot be retrieved or reconstructed aphic erase, and destruction, pr als when such media is reused internation methods recogn hods cannot be applied to media mployment of approved sanitiz	stem media, both digital and considered removable. bok computers, workstations, removes information from the l. Sanitization techniques, event the disclosure of or released for disposal. nizing that destruction is ia requiring sanitization. ration techniques and blic domain or publicly			

2324 2325 2326	docun remov for me	ient by obscuring the redacted s ing them from the document. Needia containing classified inform	sections/words in a manner equ JSA standards and policies con nation. Related controls: MA-2	ivalent in effectiveness to trol the sanitization process , MA-4, RA-3, SC-4.	
2327 2328 2329	<u>References</u> : FIPS Publication 199; NIST Special Publications 800-60, 800-88; Web: www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.				
	P1	LOW MP-6	MOD MP-6	HIGH MP-6 (1) (2) (3)	

2332 FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

2333 2334	PE-1	PHYSICAL AND ENVIRONMENTAL PROT PROCEDURES	ECTION POLICY AND	[Back to SCRM Control]
2335		Control: The organization:		
2336 2337		a. Develops, documents, and dissemin <i>roles</i>]:	ates to [Assignment: organiza	tion-defined personnel or
2338 2339 2340		 A physical and environmental presponsibilities, management co and compliance; and 	protection policy that addresse commitment, coordination amo	s purpose, scope, roles, ng organizational entities,
2341 2342		2. Procedures to facilitate the imp policy and associated physical a	lementation of the physical an and environmental protection	d environmental protection controls; and
2343		b. Reviews and updates the current:		
2344 2345		 Physical and environmental pro <i>frequency</i>]; and 	stection policy [Assignment: c	organization-defined
2346 2347		2. Physical and environmental pro <i>frequency</i>].	otection procedures [Assignme	nt: organization-defined
2348 2349 2350 2351 2352 2353 2354 2355 2356 2357		Supplemental Guidance: This control ac effective implementation of selected sec Policy and procedures reflect applicable policies, standards, and guidance. Securi level may make the need for system-spe be included as part of the general inform be represented by multiple policies refle procedures can be established for the sec systems, if needed. The organizational ri- policy and procedures. Related control:	Idresses the establishment of p urity controls and control enha federal laws, Executive Order ity program policies and procedures un ation security policy for organ cting the complex nature of ce curity program in general and isk management strategy is a k PM-9.	policy and procedures for the ancements in the PE family. rs, directives, regulations, edures at the organization innecessary. The policy can nizations or conversely, can ertain organizations. The for particular information rey factor in establishing
2358		Control Enhancements: None.		
2359		References: NIST Special Publications 800-1	2, 800-100.	
2360		Priority and Baseline Allocation:		
		P1 LOW PE-1 MG	DD PE-1 H	IIGH PE-1
2361				
2362	PE-3	PHYSICAL ACCESS CONTROL		[Back to SCRM Control]
2363 2364		Control: The organization:		
2365 2366		a. Enforces physical access authorizat to the facility where the information	ons at [Assignment: organizate system resides] by;	tion-defined entry/exit points
2367		1. Verifying individual access aut	horizations before granting ac	cess to the facility; and
2368 2369		2. Controlling ingress/egress to th organization-defined physical c	e facility using [Selection (one access control systems/devices	e or more): [Assignment:]; guards];
2370		b. Maintains physical access audit log	s for [Assignment: organizatio	m-defined entry/exit points];
2371 2372		c. Provides [Assignment: organization within the facility officially designated and the second statement of the second stateme	-defined security safeguards] ted as publicly accessible;	to control access to areas

2373 2374		d.	Escorts visitors and monitors vi circumstances requiring visitor	sitor activity [Assignment: orga escorts and monitoring];	inization-defined
2375		e.	Secures keys, combinations, and other physical access devices;		
2376 2377		f.	Inventories [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and		
2378 2379		g.	Changes combinations and keys [Assignment: organization-defined frequency] and/ keys are lost, combinations are compromised, or individuals are transferred or terminations		<i>fined frequency</i>] and/or when e transferred or terminated.
2380 2381 2382 2383 2384 2385 2386 2387 2388 2389 2390 2391 2392 2393 2394 2395 2396 2397 2398		<u>Supplemental Guidance</u> : This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices. Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.			
2399 2400		Cor	trol Enhancements:		
2401	PE-3 (5)		PHYSICAL ACCESS CONTROL / TAM	IPER PROTECTION	[BACK TO SCRM CONTROL]
2402 2403 2404 2405 2406 2407 2408 2409 2410 2411 2412 2413 2414 2415 2416		The organization employs [Assignment: organization-defined security safeguards] to [Selection (one or more): detect; prevent] physical tampering or alteration of [Assignment: organization-defined hardware components] within the information system. Supplemental Guidance: Organizations may implement tamper detection/prevention at selected hardware components or tamper detection at some components and tamper prevention at other components. Tamper detection/prevention activities can employ many types of anti-tamper technologies including, for example, tamper-detection seals and anti- tamper coatings. Anti-tamper programs help to detect hardware alterations through counterfeiting and other supply chain-related risks. Related control: SA-12.References:FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78, 800-116; ICD 704, 705; DoDI 5200.39; Personal Identity Verification (PIV) in Enterprise Physical Access Control System (E-PACS); Web: idmanagement.gov, fips201ep.cio.gov.Priority and Baseline Allocation:MOD PE-3HIGH PE-3 (1)			
2410					
2418	PE-6	мо	NITORING PHYSICAL ACCESS		[Back to SCRM Control]

2419						
2420		Cor	ntrol: The organization:			
2421 2422		a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;				
2423 2424 2425		b. Reviews physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and				
2426 2427		c. Coordinates results of reviews and investigations with the organizational incident response capability.				
2428 2429 2430 2431 2432 2433 2434		<u>Supplemental Guidance</u> : Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses. Related controls: CA-7, IR-4, IR-8.				
2435		References: None.				
2436		<u>Prio</u>	prity and Baseline Allocation:			
		P1	LOW PE-6	MOD_PE-6 (1)	HIGH $PE-6(1)(4)$	
2437						
2438	PE-16	DEI	LIVERY AND REMOVAL		[Back to SCRM Control]	
2439						
2440 2441 2442		<u>Control</u> : The organization authorizes, monitors, and controls [<i>Assignment: organization-defined types of information system components</i>] entering and exiting the facility and maintains records of those items.				
2443 2444 2445 2446		<u>Supplemental Guidance</u> : Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries. Related controls: CM-3, MA-2, MA-3, MP-5, SA-12.				
2447		Control Enhancements: None.				
2448		References: None.				
2449		Priority and Baseline Allocation:				
		P2	LOW PE-16	MOD PE-16	HIGH PE-16	
2450						
2451						
	PE-17	ALT	FERNATE WORK SITE		[Back to SCRM Control]	
2452	PE-17	ALT	FERNATE WORK SITE		[Back to SCRM Control]	
2452 2453	PE-17	ALT <u>Cor</u>	TERNATE WORK SITE <u>ntrol</u> : The organization:		[Back to SCRM Control]	
2452 2453 2454	PE-17	ALT <u>Cor</u> a.	TERNATE WORK SITE <u>ntrol</u> : The organization: Employs [<i>Assignment: organ</i>	ization-defined security controls]	[Back to SCRM Control] at alternate work sites;	
2452245324542455	PE-17	ALT <u>Cor</u> a. b.	TERNATE WORK SITE <u>ntrol</u> : The organization: Employs [<i>Assignment: organ</i> Assesses as feasible, the effect	<i>ization-defined security controls</i>] ctiveness of security controls at alt	[Back to SCRM Control] at alternate work sites; ternate work sites; and	
2452 2453 2454 2455 2456 2456 2457	PE-17	ALT <u>Cor</u> a. b. c.	TERNATE WORK SITE <u>introl</u> : The organization: Employs [<i>Assignment: organ</i> Assesses as feasible, the effect Provides a means for employ of security incidents or proble	<i>ization-defined security controls</i>] ctiveness of security controls at alr ees to communicate with informatems.	[Back to SCRM Control] at alternate work sites; ternate work sites; and tion security personnel in case	

2458 2459 2460 2461 2462 2463 2463		<u>Supplemental Guidance</u> : Alternate w private residences of employees. Wh alternate work sites may provide read operations. Organizations may defin sites or types of sites depending on t control supports the contingency pla initiative. Related controls: AC-17, 0	work sites may include, for examined of the second structure of the second structure of the second structure of the second secon	mple, government facilities or ernative processing sites, s as part of contingency rols for specific alternate work acted at those sites. This s and the federal telework		
2465		Control Enhancements: None.				
2466		References: NIST Special Publication 80	0-46.			
2467		Priority and Baseline Allocation:				
		P2 LOW Not Selected	MOD PE-17	HIGH PE-17		
2468						
2469	PE-18	LOCATION OF INFORMATION SYSTE	M COMPONENTS	[Back to SCRM Control]		
2470						
2471 2472 2473		<u>Control</u> : The organization positions information system components within the facility to minimize potential damage from [<i>Assignment: organization-defined physical and environmental hazards</i>] and to minimize the opportunity for unauthorized access.				
2474 2475 2476 2477 2478 2479 2480		<u>Supplemental Guidance</u> : Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. In addition, organizations consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). Related controls: CP-2, PE-19, RA-3.				
2481		Control Enhancements:				
2482		References: None.				
2483		Priority and Baseline Allocation:				
		P3 LOW Not Selected	MOD Not Selected	HIGH PE-18		
2484						
2485	PE-20	ASSET MONITORING AND TRACKING	:	[Back to SCRM Control]		
2486						
2487		Control: The organization:				
2488 2489 2490		a. Employs [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas]; and				
2491 2492		b. Ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.				
2493 2494 2495 2496 2497		<u>Supplemental Guidance</u> : Asset location technologies can help organizations ensure that critical assets such as vehicles or essential information system components remain in authorized locations. Organizations consult with the Office of the General Counsel and the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) regarding the deployment and use of asset location technologies to address potential privacy concerns. Related control: CM-8.				
2498		Control Enhancements: None.				

2499 <u>References</u>: None.

2500 Priority and Baseline Allocation:

P0	LOW Not Selected	MOD Not Selected	HIGH Not Selected
2501 FAMILY: PERSONNEL SECURITY

2502	PS-1	PERS	ONNEL SECURITY POLICY AND	PROCEDURES	[Back to SCRM Control]			
2503		Cont	rol: The organization:					
2504 2505		a. 1	Develops, documents, and dissenvolues]:	minates to [Assignment: organi	zation-defined personnel or			
2506 2507 2508		-	 A personnel security policy management commitment, c and 	that addresses purpose, scope, coordination among organizatio	roles, responsibilities, onal entities, and compliance;			
2509 2510		2	2. Procedures to facilitate the i associated personnel securit	mplementation of the personne y controls; and	l security policy and			
2511		b. I	. Reviews and updates the current:					
2512			1. Personnel security policy [Assignment: organization-defined frequency]; and					
2513		-	2. Personnel security procedur	es [Assignment: organization-c	lefined frequency].			
2514 2515 2516 2517 2518 2519 2520 2521 2522 2523 2524		Supp effec Polic polic level be in be re proce syste polic <u>Cont</u>	Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None.					
2525		<u>Refer</u>	ences: NIST Special Publications 80	00-12, 800-100.				
2526		<u>Priorit</u>	y and Baseline Allocation:					
		P1	LOW PS-1	MOD PS-1	HIGH PS-1			
2527								
2528	PS-6	ACCI	ESS AGREEMENTS		[Back to SCRM Control]			
2529								
2530		Cont	rol: The organization:					
2531		a. I	Develops and documents access	agreements for organizational	information systems;			
2532 2533		b. Reviews and updates the access agreements [<i>Assignment: organization-defined frequency</i>]; and						
2534 2535		c. l	Ensures that individuals requirin systems:	g access to organizational info	mation and information			
2536			1. Sign appropriate access agre	eements prior to being granted	access; and			
2537 2538 2539		2	 Re-sign access agreements t when access agreements hav frequency]. 	to maintain access to organizati we been updated or [Assignmen	onal information systems t: organization-defined			
2540 2541	Suppleme behavior,	ntal Gu and cor	idance: Access agreements include, for iflict-of-interest agreements. Signed acco	example, nondisclosure agreements, a ess agreements include an acknowledg	cceptable use agreements, rules of ement that individuals have read,			

2542 2543 2544	understan Organizat Related c	d, and ag tions can ontrol: P	gree to abide by the constraints associat use electronic signatures to acknowled L-4, PS-2, PS-3, PS-4, PS-8.	ted with organizational information system access agreements unless specifical	tems to which access is authorized. ly prohibited by organizational policy.		
2545							
2546		Refere	ences: None.				
2547		Priorit	y and Baseline Allocation:				
		P3	LOW PS-6	MOD PS-6	HIGH PS-6		
2548							
2549	PS-7	THIR	D-PARTY PERSONNEL SECURITY	Y	[Back to SCRM Control]		
2550							
2551		Contr	<u>col</u> : The organization:				
2552 2553		a. E t ⁱ	Establishes personnel security re hird-party providers;	equirements including security i	roles and responsibilities for		
2554 2555		b.F e	Requires third-party providers to established by the organization;	o comply with personnel securit	ty policies and procedures		
2556		с. I	Documents personnel security requirements;				
2557 2558 2559 2560		d. F r c	Requires third-party providers to notify [<i>Assignment: organization-defined personnel or roles</i>] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [<i>Assignment: organization-defined time period</i>]; and				
2561		e. N	Monitors provider compliance.				
2562 2563 2564 2565 2566 2567 2568 2569 2570 2571		Suppl and o servic incluc may l system appro- termi funct	lemental Guidance: Third-party ther organizations providing inf ces, outsourced applications, and de personnel security requirement have personnel working at organizator privileges issued by organizator priate termination of privileges nations deemed reportable by sec- ions, roles, and nature of creder nated. Related controls: PS-2, F	y providers include, for example formation system development, d network and security manage ents in acquisition-related docur nizational facilities with creden tions. Notifications of third-par and credentials. Organizations ecurity-related characteristics the tials/privileges associated with PS-3, PS-4, PS-5, PS-6, SA-9, S	e, service bureaus, contractors, information technology ment. Organizations explicitly nents. Third-party providers tials, badges, or information ty personnel changes ensure define the transfers and nat include, for example, individuals transferred or 6A-21.		
2572		Contr	col Enhancements: None.				
2573		Refere	ences: NIST Special Publication 80	0-35.			
2574		Priorit	y and Baseline Allocation:				
		P1	LOW PS-7	MOD PS-7	HIGH PS-7		

2576 FAMILY: RISK ASSESSMENT

2577	RA-1	RISK ASSESSMENT	POLICY AND PROCEDU	URES	[Back to SCRM Control]
2578 2579		Control: The orga	nization:		
2580 2581		a. Develops, doo <i>roles</i>]:	cuments, and disseminat	tes to [Assignment: organi	zation-defined personnel or
2582 2583 2584		1. A risk as managem and	sessment policy that add tent commitment, coord	lresses purpose, scope, role ination among organizatio	es, responsibilities, nal entities, and compliance;
2585 2586		2. Procedur risk asses	es to facilitate the imple sment controls; and	ementation of the risk asses	ssment policy and associated
2587		b. Reviews and	updates the current:		
2588		1. Risk asse	ssment policy [Assignm	ent: organization-defined	frequency]; and
2589		2. Risk asse	ssment procedures [Ass	ignment: organization-def	ined frequency].
2590 2591 2592 2593 2594 2595 2596 2597 2598 2599		Supplemental Gui effective impleme Policy and proced policies, standards level may make th be included as par be represented by procedures can be systems, if needed policy and proced	<u>lance</u> : This control addition of selected securities reflect applicable for , and guidance. Security e need for system-specitor of the general informa multiple policies reflect established for the securities. Related control: Planet	Iresses the establishment or rity controls and control er ederal laws, Executive Orce y program policies and pro- fic policies and procedures tion security policy for org ing the complex nature of arity program in general an k management strategy is a M-9.	f policy and procedures for the nhancements in the RA family. ders, directives, regulations, ocedures at the organization s unnecessary. The policy can ganizations or conversely, can certain organizations. The d for particular information a key factor in establishing
2600		Control Enhancen	ents: None.		
2601		References: NIST S	pecial Publications 800-12	, 800-30, 800-100.	
2602		Priority and Baseline	Allocation:		
		P1 LOW RA-1	MOI	D RA-1	HIGH RA-1
2603					
2604	RA-2	SECURITY CATEG	ORIZATION		[Back to SCRM Control]
2605 2606		Control: The orga	nization:		
2607 2608		a. Categorizes in laws, Executi	formation and the infor ve Orders, directives, po	mation system in accordant plicies, regulations, standar	nce with applicable federal rds, and guidance;
2609 2610		b. Documents the plan for the in	e security categorization formation system; and	n results (including suppor	ting rationale) in the security
2611 2612		c. Ensures that t official or aut	he security categorization horizing official designation	on decision is reviewed and ated representative.	d approved by the authorizing
2613 2614 2615 2616 2617		Supplemental Gui security categoriza organizational ope information system Organizations com	<u>dance</u> : Clearly defined tion decisions. Security rations, organizational a ns are comprised throug duct the security catego	authorization boundaries a categories describe the po- assets, and individuals if o the a loss of confidentiality, prization process as an organication	are a prerequisite for effective otential adverse impacts to rganizational information and integrity, or availability. unization-wide activity with

2618 2619 2620 2621 2622 2623 2624 2625		the sys con PA adv dev info con	involvement of chief informatio tem owners, mission/business ov isider the potential adverse impar TRIOT Act of 2001 and Homela verse impacts. Security categoriz velopment of inventories of infor prmation system components wh ntrols: CM-8, MP-4, RA-3, SC-7	n officers, senior information services, and information owners/sects to other organizations and, in and Security Presidential Directivation processes carried out by or mation assets, and along with Cluere information is processed, stor.	curity officers, information tewards. Organizations also accordance with the USA ves, potential national-level ganizations facilitate the M-8, mappings to specific red, or transmitted. Related
2626		Co	ntrol Enhancements: None.		
2627		Ref	erences: FIPS Publication 199	; NIST Special Publications 8	00-30, 800-39, 800-60.
2628		<u>Pric</u>	prity and Baseline Allocation:		
		DI		MOD DA 1	
2629		PI	LOW RA-2	MOD KA-2	пібн ка-2
2630	RA-3	RIS	K ASSESSMENT		[Back to SCRM Control]
2631 2632		Con	ntrol: The organization:		
2633 2634 2635		a.	Conducts an assessment of risk unauthorized access, use, discle information system and the info	, including the likelihood and ma osure, disruption, modification, c ormation it processes, stores, or t	agnitude of harm, from the or destruction of the ransmits;
2636 2637		b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];			
2638		c.	Reviews risk assessment result	s [Assignment: organization-def	ined frequency];
2639 2640		d.	Disseminates risk assessment re roles]; and	esults to [Assignment: organizat	ion-defined personnel or
2641 2642 2643 2644		e.	Updates the risk assessment [A are significant changes to the in identification of new threats an security state of the system.	ssignment: organization-defined nformation system or environmen d vulnerabilities), or other condi	<i>frequency</i>] or whenever there nt of operation (including the tions that may impact the
2645 2646 2647 2648 2649 2650 2651 2652 2653 2654 2655			Supplemental Guidance: Clear effective risk assessments. Risk likelihood, and impact to organ organizations, and the Nation b assessments also take into acco contractors operating informati organizational information syst and related E-authentication in information systems may also I As such, organizational assess systems.	ely defined authorization boundat c assessments take into account t dizational operations and assets, i based on the operation and use of point risk from external parties (e. on systems on behalf of the orga tems, outsourcing entities). In ac- itiatives, authentication of public be required to protect nonpublic ments of risk also address public	ries are a prerequisite for hreats, vulnerabilities, ndividuals, other information systems. Risk g., service providers, nization, individuals accessing cordance with OMB policy users accessing federal or privacy-related information. access to federal information
2656 2657 2658 2659 2660 2661 2662 2663			Risk assessments (either forma management hierarchy (i.e., org system level) and at any phase also be conducted at various sta categorization, security control assessment, information system noteworthy in that the control r other controls in order to comp	l or informal) can be conducted a ganization level, mission/busines in the system development life c eps in the Risk Management Fran- selection, security control imple n authorization, and security com- nust be partially implemented pr lete the first two steps in the Rist	at all three tiers in the risk sprocess level, or information ycle. Risk assessments can mework, including mentation, security control trol monitoring. RA-3 is ior to the implementation of k Management Framework.

2664 2665 2666	Risk assessments can play an in particularly during the applicat supplementation. Related contr	mportant role in security control ion of tailoring guidance, which ols: RA-2, PM-9.	selection processes, includes security control				
2667 2668 2669	Control Enhancements: None.						
2670	References: OMB Memorandum 04-04;	References: OMB Memorandum 04-04; NIST Special Publication 800-30, 800-39; Web: idmanagement.gov.					
2671	Priority and Baseline Allocation:						
	P1 LOW RA-3	MOD RA-3	HIGH RA-3				

2673 2674 FAMILY: SYSTEM AND SERVICES ACQUISITION

2675	SA-1	SYSTEM AND SERVICES ACQUISITION	POLICY AND PROCEDURES	[Back to SCRM Control]			
2676		Control: The organization:					
2677 2678		a. Develops, documents, and dissem <i>roles</i>]:	inates to [Assignment: organiz	cation-defined personnel or			
2679 2680 2681		 A system and services acquis responsibilities, management and compliance; and 	ition policy that addresses purj commitment, coordination am	pose, scope, roles, long organizational entities,			
2682 2683		2. Procedures to facilitate the im and associated system and ser	plementation of the system and rvices acquisition controls; and	nd services acquisition policy			
2684		b. Reviews and updates the current:					
2685 2686		 System and services acquisitiand 	on policy [Assignment: organi	ization-defined frequency];			
2687 2688		2. System and services acquisit <i>frequency</i>].	ion procedures [Assignment: o	rganization-defined			
2689 2690 2691 2692 2693 2694 2695 2696 2697 2698		Supplemental Guidance: This control effective implementation of selected se Policy and procedures reflect applicab policies, standards, and guidance. Secu level may make the need for system-sp be included as part of the general infor be represented by multiple policies ref procedures can be established for the s systems, if needed. The organizational policy and procedures. Related control	addresses the establishment of ecurity controls and control en le federal laws, Executive Ord arity program policies and proce pecific policies and procedures mation security policy for org lecting the complex nature of ecurity program in general and risk management strategy is a b: PM-9.	f policy and procedures for the hancements in the SA family. ers, directives, regulations, cedures at the organization anizations or conversely, can certain organizations. The d for particular information key factor in establishing			
2699		Control Enhancements: None.					
2700		References: NIST Special Publications 800-12, 800-100.					
2701		Priority and Baseline Allocation:					
		P1 LOW SA-1	MOD SA-1	HIGH SA-1			
2702							
2703	SA-2	ALLOCATION OF RESOURCES		[Back to SCRM Control]			
2704 2705		Control: The organization:					
2706 2707		a. Determines information security r system service in mission/busines	equirements for the informatic s process planning;	on system or information			
2708		b. Determines, documents, and allocates the resources required to protect the information system					

- 2709 2710 or information system service as part of its capital planning and investment control process; and 2711 Establishes a discrete line item for information security in organizational programming and c.
- 2712 budgeting documentation.

2713Supplemental Guidance: Resource allocation for information security includes funding for the
initial information system or information system service acquisition and funding for the
sustainment of the system/service. Related controls: PM-3, PM-11.

- 2716 <u>Control Enhancements:</u> None.
- 2717 <u>References</u>: NIST Special Publication 800-65.

LOW SA-2

Control: The organization:

SYSTEM DEVELOPMENT LIFE CYCLE

2718 Priority and Baseline Allocation:

P1

а

b.

2719

2720

SA-3

726		development life cycle;
727	c.	Identifies individuals having information security roles and responsibilities; and

MOD SA-2

Manages the information system using [Assignment: organization-defined system

Defines and documents information security roles and responsibilities throughout the system

development life cycle] that incorporates information security considerations;

HIGH SA-2

[Back to SCRM Control]

2728	d.	Integrates the organizational information security risk management process into system
2729		development life cycle activities.

2730 Supplemental Guidance: A well-defined system development life cycle provides the foundation 2731 for the successful development, implementation, and operation of organizational information 2732 systems. To apply the required security controls within the system development life cycle requires 2733 a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to 2734 critical missions/business functions. The security engineering principles in SA-8 cannot be 2735 properly applied if individuals that design, code, and test information systems and system 2736 components (including information technology products) do not understand security. Therefore, 2737 organizations include qualified personnel, for example, chief information security officers, 2738 security architects, security engineers, and information system security officers in system 2739 development life cycle activities to ensure that security requirements are incorporated into 2740 organizational information systems. It is equally important that developers include individuals on 2741 the development team that possess the requisite security expertise and skills to ensure that needed 2742 security capabilities are effectively integrated into the information system. Security awareness and 2743 training programs can help ensure that individuals having key security roles and responsibilities 2744 have the appropriate experience, skills, and expertise to conduct assigned system development life 2745 cycle activities. The effective integration of security requirements into enterprise architecture also 2746 helps to ensure that important security considerations are addressed early in the system 2747 development life cycle and that those considerations are directly related to the organizational 2748 mission/business processes. This process also facilitates the integration of the information security 2749 architecture into the enterprise architecture, consistent with organizational risk management and 2750 information security strategies. Related controls: AT-3, PM-7, SA-8.

2751 <u>Control Enhancements:</u> None.

27	52	2	References:	NIST	Special	Publications	800-37,	800-64
----	----	---	-------------	------	---------	--------------	---------	--------

2753 Priority and Baseline Allocation:

P1	LOW SA-3	MOD SA-3	HIGH SA-3
----	----------	----------	-----------

2755 SA-4 ACQUISITION PROCESS

2756 2757

2758

2759

2760

2761

2766

2767

2768

2770

2771

2772

2773

2774

2775

2776

2777

2778

2779

2780

<u>Control</u>: The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

- a. Security functional requirements;
- b. Security strength requirements;
- c. Security assurance requirements;
- d. Security-related documentation requirements;
 - e. Requirements for protecting security-related documentation;
 - f. Description of the information system development environment and environment in which the system is intended to operate; and
- 2769 g. Acceptance criteria.

<u>Supplemental Guidance</u>: Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial information technology products. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include: (i) development processes, procedures, practices, and methodologies; and (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security documentation requirements address all phases of the system development life cycle.

2781 Security functionality, assurance, and documentation requirements are expressed in terms of 2782 security controls and control enhancements that have been selected through the tailoring process. 2783 The security control tailoring process includes, for example, the specification of parameter values 2784 through the use of assignment and selection statements and the specification of platform 2785 dependencies and implementation information. Security documentation provides user and 2786 administrator guidance regarding the implementation and operation of security controls. The level 2787 of detail required in security documentation is based on the security category or classification level 2788 of the information system and the degree to which organizations depend on the stated security 2789 capability, functions, or mechanisms to meet overall risk response expectations (as defined in the 2790 organizational risk management strategy). Security requirements can also include organizationally 2791 mandated configuration settings specifying allowed functions, ports, protocols, and services. 2792 Acceptance criteria for information systems, information system components, and information 2793 system services are defined in the same manner as such criteria for any organizational acquisition 2794 or procurement. The Federal Acquisition Regulation (FAR) Section 7.103 contains information 2795 security requirements from FISMA. Related controls: CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-2796 11, SA-12.

- 2797 Control Enhancements:
- 2798 SA-4 (5) ACQUISITION PROCESS / SYSTEM / COMPONENT / SERVICE CONFIGURATIONS

2800The organization requires the developer of the information system, system component,
or information system service to:

[BACK TO SCRM CONTROL]

2802 2803		(a) Deliver the system, component, or service with [Assignment: organization-defined security configurations] implemented; and				
2804 2805		(b) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.				
2806 2807 2808 2809		<u>Supplemental Guidance</u> : Security configurations include, for example, the U.S. Government Configuration Baseline (USGCB) and any limitations on functions, ports, protocols, and services. Security characteristics include, for example, requiring that all default passwords have been changed. Related control: CM-8.				
2810	SA-4 (7)	ACQUISITION PROCESS NIAP-APPROVED PROTECTION PROFILES [BACK TO SCRM CONTROL]				
2811		The organization:				
2812 2813 2814 2815		(a) Limits the use of commercially provided information assurance (IA) and IA-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; and				
2816 2817 2818 2819		(b) Requires, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated.				
2820		Supplemental Guidance: Related controls: SC-12, SC-13.				
2821 2822 2823		<u>References:</u> HSPD-12; ISO/IEC 15408; FIPS Publications 140-2, 201; NIST Special Publications 800-23, 800- 35, 800-36, 800-37, 800-64, 800-70, 800-137; Federal Acquisition Regulation; Web: www.niap-ccevs.org, fips201ep.cio.gov, www.acquisition.gov/far.				
2824		Priority and Baseline Allocation:				
		P1 LOW SA-4 (10) MOD SA-4 (1) (2) (9) (10) HIGH SA-4 (1) (2) (9) (10)				
2825						
2826	SA-5	INFORMATION SYSTEM DOCUMENTATION [Back to SCRM Control]				
2827						
2828		<u>Control</u> : The organization:				
2829 2830		a. Obtains administrator documentation for the information system, system component, or information system service that describes:				
2831		1. Secure configuration, installation, and operation of the system, component, or service;				
2832		2. Effective use and maintenance of security functions/mechanisms; and				
2833 2834		3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;				
2835 2836		b. Obtains user documentation for the information system, system component, or information system service that describes:				
2837 2838		1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;				
2839 2840		2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and				
2841		3. User responsibilities in maintaining the security of the system, component, or service;				

2842 2843 2844	c. Documents service doc [Assignment]	s attempts to obtain in cumentation when suc nt: organization-defin	formation system, system comp th documentation is either unav <i>ed actions</i>] in response;	ponent, or information system ailable or nonexistent and		
2845	d. Protects do	ocumentation as requir	red, in accordance with the risk	management strategy; and		
2846	e. Distributes	documentation to [A.	ssignment: organization-defined	d personnel or roles].		
2847 2848 2849 2850 2851 2852 2853 2854 2855 2856 2857 2858 2859 2860 2861 2862 2863 2864	Supplemental C implementation components, an measures to den needed docume system/compor organizations in the effective im selected inform security catego key DoD weap of protection th system vulneral information system System operation PS-2, SA-3, SA References: Nor Priority and Base	<u>Guidance</u> : This control and operation of sect and information system termine the quality/co entation may occur, for nent or lack of support may need to recreate so plementation or oper- nation system, compor- ry or classification of ons system or comma and a routine administration bilities may also requi- stem, includes, for exa- on after any lapse in sy A-4. ne. <u>line Allocation</u> :	ol helps organizational personne urity controls associated with in services. Organizations consid mpleteness of the content provi- or example, due to the age of the t from developers and contractor elected documentation if such d ation of security controls. The I nent, or service documentation if the system. For example, document and and control system would ty rative system. Documentation to ire an increased level of protect mple, initially starting the system system operation. Related control	el understand the nformation systems, system er establishing specific ided. The inability to obtain e information ors. In those situations, locumentation is essential to evel of protection provided for is commensurate with the mentation associated with a rpically require a higher level hat addresses information ion. Secure operation of the em and resuming secure ols: CM-6, CM-8, PL-2, PL-4,		
	P2 LOW SA	<u>x-5</u>	MOD SA-5	HIGH SA-5		
2865 SA-8 2867 2868 2869 2870 2871 2872	SECURITY ENG <u>Control</u> : The o specification, d <u>Supplemental (</u> development in organizations a	INEERING PRINCIPLE organization applies in esign, development, i <u>Guidance</u> : Organization formation systems or	s formation system security engi mplementation, and modification ons apply security engineering j systems undergoing major upg ring principles to system ungravity	[Back to SCRM Control] neering principles in the on of the information system. principles primarily to new rades. For legacy systems, des and modifications to the		
2872 2873 2874 2875 2876 2877 2878 2879 2880 2881 2882	extent feasible, Security engine establishing so incorporating s physical and lo build secure so (vii) performin patterns as well reducing risk to controls: PM-7	given the current stat eering principles inclu und security policy, ar ecurity requirements i gical security boundar ftware; (vi) tailoring s g threat modeling to id as compensating com o acceptable levels, the , SA-3, SA-4, SA-17,	e of hardware, software, and fin de, for example: (i) developing rchitecture, and controls as the into the system development lif ries; (v) ensuring that system de eccurity controls to meet organize dentify use cases, threat agents, throls and design patterns neede us enabling informed risk mana SC-2, SC-3.	the and modifications to the rmware within those systems. layered protections; (ii) foundation for design; (iii) e cycle; (iv) delineating evelopers are trained on how to zational and operational needs; attack vectors, and attack d to mitigate risk; and (viii) gement decisions. Related		
2883	Control Enhancements: None.					
2884	Control Enhance	cements: None.				
_001	Control Enhance <u>References</u> : NIS	cements: None. T Special Publication 80	0-27.			
2885	Control Enhance References: NIS Priority and Base	cements: None. T Special Publication 80 line Allocation:	0-27.			

2887	SA-9	EXTERNAL INFORMATION SYSTEM SERVICES	[Back to SCRM Control]
2888			
2889		<u>Control</u> : The organization:	
2890 2891 2892 2893		a. Requires that providers of external information system service information security requirements and employ [<i>Assignment: controls</i>] in accordance with applicable federal laws, Executive regulations, standards, and guidance;	es comply with organizational organization-defined security ve Orders, directives, policies,
2894 2895		b. Defines and documents government oversight and user roles a to external information system services; and	and responsibilities with regard
2896 2897		c. Employs [<i>Assignment: organization-defined processes, methors</i> security control compliance by external service providers on a	ods, and techniques] to monitor an ongoing basis.
2898 2899 2900 2901 2902 2903 2904 2905 2906 2907 2908 2909 2910 2911 2912 2913 2914 2915 2916 2917 2918		Supplemental Guidance: External information system services are outside of the authorization boundaries of organizational informat services that are used by, but not a part of, organizational informat policy require that organizations using external service providers transmitting federal information or operating information systems government ensure that such providers meet the same security req are required to meet. Organizations establish relationships with exvariety of ways including, for example, through joint ventures, but interagency agreements, lines of business arrangements, licensing exchanges. The responsibility for managing risks from the use of eservices remains with authorizing officials. For services external trequires that organizations establish and retain a level of confidence provider in the potentially complex consumer-provider relationships for the services rendered. The extent and nature of this chain of the system services documentation includes government, service providers system services documentation includes government, service providers of the service provider controls, describe measurable outcomes, response requirements for identified instances of noncompliance. PS-7.	e services that are implemented ion systems. This includes tion systems. FISMA and OMB that are processing, storing, or on behalf of the federal uirements that federal agencies ternal service providers in a siness partnerships, contracts, agreements, and supply chain external information system o organizations, a chain of trust ce that each participating p provides adequate protection ust varies based on the rganizations document the basis ime. External information riders, end user security roles and ments define expectations of and identify remedies and Related controls: CA-3, IR-7,
2919		Control Enhancements:	
2920 2921	SA-9(1)	EXTERNAL INFORMATION SYSTEMS RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS	[BACK TO SCRM CONTROL]
2922 2923			
2924		The organization:	
2925 2926		(a) Conducts an organizational assessment of risk prior t outsourcing of dedicated information security services	o the acquisition or s; and
2927 2928 2929 2930 2931		(b) Ensures that the acquisition or outsourcing of dedicat services is approved by [Assignment: organization-defi Supplemental Guidance: Dedicated information security serv incident monitoring, analysis and response, operation of infor such as firewalls, or key management services. Related control	ted information security <i>ined personnel or roles</i>]. vices include, for example, mation security-related devices bls: CA-6, RA-3.
2932 2933	SA-9 (3)	EXTERNAL INFORMATION SYSTEMS ESTABLISH / MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS	[BACK TO SCRM CONTROL]

The organization establishes, documents, and maintains trust relationships with external service providers based on [Assignment: organization-defined security requirements, properties, factors, or conditions defining acceptable trust relationships].

- 2938 Supplemental Guidance: The degree of confidence that the risk from using external services 2939 is at an acceptable level depends on the trust that organizations place in the external providers, 2940 individually or in combination. Trust relationships can help organization to gain increased 2941 levels of confidence that participating service providers are providing adequate protection for 2942 the services rendered. Such relationships can be complicated due to the number of potential 2943 entities participating in the consumer-provider interactions, subordinate relationships and 2944 levels of trust, and the types of interactions between the parties. In some cases, the degree of 2945 trust is based on the amount of direct control organizations are able to exert on external 2946 service providers with regard to employment of security controls necessary for the protection 2947 of the service/information and the evidence brought forth as to the effectiveness of those 2948 controls. The level of control is typically established by the terms and conditions of the 2949 contracts or service-level agreements and can range from extensive control (e.g., negotiating 2950 contracts or agreements that specify security requirements for the providers) to very limited 2951 control (e.g., using contracts or service-level agreements to obtain commodity services such as 2952 commercial telecommunications services). In other cases, levels of trust are based on factors 2953 that convince organizations that required security controls have been employed and that 2954 determinations of control effectiveness exist. For example, separately authorized external 2955 information system services provided to organizations through well-established business 2956 relationships may provide degrees of trust in such services within the tolerable risk range of 2957 the organizations using the services. External service providers may also outsource selected 2958 services to other external entities, making the trust relationship more difficult and complicated 2959 to manage. Depending on the nature of the services, organizations may find it very difficult to 2960 place significant trust in external providers. This is not due to any inherent untrustworthiness 2961 on the part of providers, but to the intrinsic level of risk in the services.
- 2962 SA-9 (4) EXTERNAL INFORMATION SYSTEMS / CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS

[BACK TO SCRM CONTROL]

The organization employs [Assignment: organization-defined security safeguards] to ensure that the interests of [Assignment: organization-defined external service providers] are consistent with and reflect organizational interests.

<u>Supplemental Guidance</u>: As organizations increasingly use external service providers, the possibility exists that the interests of the service providers may diverge from organizational interests. In such situations, simply having the correct technical, procedural, or operational safeguards in place may not be sufficient if the service providers that implement and control those safeguards are not operating in a manner consistent with the interests of the consuming organizations. Possible actions that organizations might take to address such concerns include, for example, requiring background checks for selected service provider personnel, examining ownership records, employing only trustworthy service providers (i.e., providers with which organizations have had positive experiences), and conducting periodic/unscheduled visits to service provider facilities.

2978
2979SA-9 (5)EXTERNAL INFORMATION SYSTEMS / PROCESSING, STORAGE, AND
SERVICE LOCATION

[BACK TO SCRM CONTROL]

29802981The organization restricts the location of [Selection (one or more): information2982processing; information/data; information system services] to [Assignment: organization-2983defined locations] based on [Assignment: organization-defined requirements or2984conditions].

2934 2935

2936

2937

2964 2965

2966

2967

2968

2969

2970

2971

2972

2973

2974

2975

2976

2985 2986 2987 2988 2989 2990 2991 2992 2993 2994 2995 2996 2997		 <u>Supplemental Guidance</u>: The location of information processing, information/data storage, or information system services that are critical to organizations can have a direct impact on the ability of those organizations to successfully execute their missions/business functions. This situation exists when external providers control the location of processing, storage or services. The criteria external providers use for the selection of processing, storage, or service locations may be different from organizational criteria. For example, organizations may want to ensure that data/information storage locations are restricted to certain locations to facilitate incident response activities (e.g., forensic analyses, after-the-fact investigations) in case of information security breaches/compromises. Such incident response activities may be adversely affected by the governing laws or protocols in the locations where processing and storage occur and/or the locations from which information system services emanate. <u>References</u>: NIST Special Publication 800-35. <u>Priority and Baseline Allocation</u>: 					
		P1 LOW SA-9	MOD SA-9 (2)	HIGH SA-9 (2)			
2998							
2999	SA-10	DEVELOPER CONFIGURATION	MANAGEMENT	[Back to SCRM Control]			
3000 3001		<u>Control</u> : The organization requored or information system service t	uires the developer of the informatio to:	n system, system component,			
3002 3003		a. Perform configuration man more): design; development	nagement during system, component nt; implementation; operation];	t, or service [Selection (one or			
3004 3005		b. Document, manage, and configuration items under	ontrol the integrity of changes to [As configuration management];	signment: organization-defined			
3006		c. Implement only organizati	ion-approved changes to the system,	component, or service;			
3007 3008		d. Document approved change impacts of such changes; a	ges to the system, component, or ser and	vice and the potential security			
3009 3010		e. Track security flaws and f findings to [Assignment: o	law resolution within the system, co organization-defined personnel].	mponent, or service and report			
3011 3012 3013 3014 3015 3016 3017 3018 3019 3020 3021 3022 3023 3024 3025 3026 3027 3028		Supplemental Guidance: This information systems developm completeness of the configurat applying effective security safe unauthorized modification or d security-relevant portions of th integrity of changes to the info system service requires configu- track authorized changes and p under configuration management the formal model; the functions data; implementation document of the object code; tools for con- and software/firmware source of Depending on the mission/busi- relationships in place, developed operations and maintenance ph 12, SI-2.	control also applies to organizations ent and integration. Organizations co- ion management activities conducted eguards. Safeguards include, for exai- lestruction, the master copies of all m resystem hardware, software, and fin rmation system, information system uration control throughout the system prevent unauthorized changes. Config- ent (if existence/use is required by ot al, high-level, and low-level design s- tation; source code and hardware sc mparing new versions of security-re- code with previous versions; and tes iness needs of organizations and the ers may provide configuration mana- nases of the life cycle. Related control	conducting internal onsider the quality and d by developers as evidence of mple, protecting from naterial used to generate mware. Maintaining the component, or information n development life cycle to guration items that are placed her security controls) include: specifications; other design hematics; the running version levant hardware descriptions t fixtures and documentation. nature of the contractual gement support during the ols: CM-3, CM-4, CM-9, SA-			
3029		<u>References</u> : NIST Special Publica <u>Priority and Baseline Allocation</u> :	11011 6UU-128.				

		P1	LOW	Not Selected	MOD SA-10	HIGH SA-10		
3031								
3032	SA-11	DEVELOPER SECURITY TESTING AND EVALUATION [Back to SCRM Control]						
3033 3034		<u>Con</u> or ir	<u>trol</u> : Th nformati	ne organization requires on system service to:	the developer of the information	n system, system component,		
3035		a.	Create	and implement a securit	y assessment plan;			
3036 3037		b.	Perform [Assign	n [Selection (one or mon ment: organization-defi	e): unit; integration; system; re ned depth and coverage];	gression] testing/evaluation at		
3038 3039		c.	Produc security	e evidence of the execut y testing/evaluation;	ion of the security assessment p	lan and the results of the		
3040		d.	Implen	nent a verifiable flaw rer	nediation process; and			
3041		e.	Correct	flaws identified during	security testing/evaluation.			
3042 3043 3044 3045 3046 3047 3048 3049 3050 3051 3052 3053 3054 3055 3056 3057 3058 3059 3060 3061 3062 3063 3064		Supplemental Guidance: Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches. Developers can employ these analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The <i>depth</i> of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or eleminate of security and protecting assessment plans, evidence, and documentation are commensurate with the security category or eleminate of security assessment plans, evidence, and documentation are commensurate with the security category or eleminate of the plans/processes have been diligently applied						
3065 3066		References: ISO/IEC 15408; NIST Special Publication 800-53A; Web: nvd.nist.gov, cwe.mitre.org, cve.mitre.org.						
3067		Priority and Baseline Allocation:						
		P1	LOW	Not Selected	MOD SA-11	HIGH SA-11		
3068								
3069	SA-12	SUP	PLY CH	AIN PROTECTION		[Back to SCRM Control]		
3070								
3071 3072 3073		Con com secu	<u>trol</u> : Th ponent, <i>urity safe</i>	ne organization protects or information system s eguards] as part of a con	against supply chain threats to t service by employing [Assignme nprehensive, defense-in-breadth	he information system, system <i>nt: organization-defined</i> information security strategy.		

3074 3075 3076 3077 3078 3079 3080 3081 3082 3083 3084 3085 3086 3087 3088 3089 3090 3091 3092 3093 3094		<u>Supplemental Guidance:</u> Information systems (including system components that compose those systems) need to be protected throughout the system development life cycle (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). Protection of organizational information systems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk. Organizations consider implementing a standardized process to address supply chain risk with respect to information systems and system components, and to educate the acquisition workforce on threats, risk, and required security controls. Organizations use the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain; and (ii) protect information systems and information system components, prior to taking delivery of such systems/components. This control enhancement also applies to information systems, development facilities, and external connections to development systems; (ii) vetting development personnel; and (iii) use of tamper-evident packaging during shipping/warehousing. Methods for reviewing and protecting development plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements. Related controls: AT-3, CM-8, IR-4, PE-16, PL-8, SA-3, SA-4, SA-8, SA-10, SA-14, SA-15, SA-18, SA-19, SC-29, SC-30, SC-38, SI-7.
3095		Control Enhancements:
3096 3097	SA-12 (1)	SUPPLY CHAIN PROTECTION ACQUISITION STRATEGIES / TOOLS / METHODS
3098 3099 3100		The organization employs [Assignment: organization-defined tailored acquisition strategies, contract tools, and procurement methods] for the purchase of the information system, system component, or information system service from suppliers.
3101 3102 3103 3104 3105 3106 3107 3108 3109 3110 3111 3112 3113 3114 3115 3116		<u>Supplemental Guidance</u> : The use of acquisition and procurement processes by organizations early in the system development life cycle provides an important vehicle to protect the supply chain. Organizations use available all-source intelligence analysis to inform the tailoring of acquisition strategies, tools, and methods. There are a number of different tools and techniques available (e.g., obscuring the end use of an information system or system component, using blind or filtered buys). Organizations also consider creating incentives for suppliers who: (i) implement required security safeguards; (ii) promote transparency into their organizational processes and security practices; (iii) provide additional vetting of the processes and security practices of subordinate suppliers, critical information system components, and services; (iv) restrict purchases from specific suppliers or countries; and (v) provide contract language regarding the prohibition of tainted or counterfeit components. In addition, organizations consider minimizing the time between purchase decisions and required delivery to limit opportunities for adversaries to corrupt information system components or products. Finally, organizations can use trusted/controlled distribution, delivery, and warehousing options to reduce supply chain risk (e.g., requiring tamper-evident packaging of information system components during shipping and warehousing). Related control: SA-19.
3117	SA-12 (2)	SUPPLY CHAIN PROTECTION SUPPLIER REVIEWS [BACK TO SCRM CONTROL]
3118 3119 3120 3121 3122 3123 3123 3124		 The organization conducts a supplier review prior to entering into a contractual agreement to acquire the information system, system component, or information system service. <u>Supplemental Guidance</u>: Supplier reviews include, for example: (i) analysis of supplier processes used to design, develop, test, implement, verify, deliver, and support information systems, system components, and information system services; and (ii) assessment of supplier training and experience in developing systems, components, or services with the required

3125 3126 3127 3128 3129		security capability. These reviews provide organizations with increased levels of visibility into supplier activities during the system development life cycle to promote more effective supply chain risk management. Supplier reviews can also help to determine whether primary suppliers have security safeguards in place and a practice for vetting subordinate suppliers, for example, second- and third-tier suppliers, and any subcontractors.
3130	SA-12 (5)	SUPPLY CHAIN PROTECTION / LIMITATION OF HARM [BACK TO SCRM CONTROL]
3131 3132 3133		The organization employs [Assignment: organization-defined security safeguards] to limit harm from potential adversaries identifying and targeting the organizational supply chain.
3134 3135 3136 3137 3138 3139 3140 3141		<u>Supplemental Guidance</u> : Supply chain risk is part of the advanced persistent threat (APT). Security safeguards and countermeasures to reduce the probability of adversaries successfully identifying and targeting the supply chain include, for example: (i) avoiding the purchase of custom configurations to reduce the risk of acquiring information systems, components, or products that have been corrupted via supply chain actions targeted at specific organizations; (ii) employing a diverse set of suppliers to limit the potential harm from any given supplier in the supply chain; (iii) employing approved vendor lists with standing reputations in industry, and (iv) using procurement carve outs (i.e., exclusions to commitments or obligations).
3142 3143	SA-12 (7)	SUPPLY CHAIN PROTECTION / ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE [BACK TO SCRM CONTROL]
3144 3145 3146		The organization conducts an assessment of the information system, system component, or information system service prior to selection, acceptance, or update. Supplemental Guidance: Assessments include, for example, testing, evaluations, reviews, and
3147 3148 3149 3150 3151 3152 3153 3154 3155		analyses. Independent, third-party entities or organizational personnel conduct assessments of systems, components, products, tools, and services. Organizations conduct assessments to uncover unintentional vulnerabilities and intentional vulnerabilities including, for example, malicious code, malicious processes, defective software, and counterfeits. Assessments can include, for example, static analyses, dynamic analyses, simulations, white, gray, and black box testing, fuzz testing, penetration testing, and ensuring that components or services are genuine (e.g., using tags, cryptographic hash verifications, or digital signatures). Evidence generated during security assessments is documented for follow-on actions carried out by organizations. Related controls: CA-2, SA-11.
3156	SA-12 (8)	SUPPLY CHAIN PROTECTION / USE OF ALL-SOURCE INTELLIGENCE [BACK TO SCRM CONTROL]
3157 3158		The organization uses all-source intelligence analysis of suppliers and potential suppliers of the information system, system component, or information system service.
3159 3160 3161 3162 3163 3164 3165 3166 3167		<u>Supplemental Guidance</u> : All-source intelligence analysis is employed by organizations to inform engineering, acquisition, and risk management decisions. All-source intelligence consists of intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data in the production of finished intelligence. Where available, such information is used to analyze the risk of both intentional and unintentional vulnerabilities from development, manufacturing, and delivery processes, people, and the environment. This review is performed on suppliers at multiple tiers in the supply chain sufficient to manage risks. Related control: SA-15.
3168	SA-12 (9)	SUPPLY CHAIN PROTECTION / OPERATIONS SECURITY [BACK TO SCRM CONTROL]
3169 3170 3171		The organization employs [Assignment: organization-defined Operations Security (OPSEC) safeguards] in accordance with classification guides to protect supply chain-

3172 3173		related information for the information system, system componen system service.	nt, or information
3174 3175 3176 3177 3178 3179 3180 3181 3182 3183 3184 3185 3186 3187 3188		<u>Supplemental Guidance</u> : Supply chain information includes, for exar uses for information systems, information system components, and in services; supplier identities; supplier processes; security requirements testing and evaluation results; and system/component configurations. enhancement expands the scope of OPSEC to include suppliers and p OPSEC is a process of identifying critical information and subsequen actions attendant to operations and other activities to: (i) identify those observed by potential adversaries; (ii) determine indicators that adver could be interpreted or pieced together to derive critical information is cause harm to organizations; (iii) implement safeguards or countermer reduce to an acceptable level, exploitable vulnerabilities; and (iv) cont information may compromise the confidentiality of users or uses of the may require organizations to withhold critical mission/business inform and may include the use of intermediaries to hide the end use, or user systems, system components, or information system services. Related	mple: user identities; formation system s; design specifications; This control otential suppliers. ttly analyzing friendly se actions that can be rearies might obtain that n sufficient time to easures to eliminate or usider how aggregated ne supply chain. OPSEC mation from suppliers s, of information a control: PE-21.
3189 3190	SA-12 (10)	SUPPLY CHAIN PROTECTION / VALIDATE AS GENUINE AND NOT ALTERED	[BACK TO SCRM CONTROL]
3191 3192 3193 3194 3195 3196 3197 3198 3199 3200		The organization employs [Assignment: organization-defined security validate that the information system or system component received not been altered. Supplemental Guidance: For some information system components, there are technical means to help determine if the components are ger altered. Security safeguards used to validate the authenticity of information system components include, for example, optical/nanotec side-channel analysis. For hardware, detailed bill of material information elements with embedded logic complete with component and product	rity safeguards] to ed is genuine and has especially hardware, nuine or have been nation systems and chnology tagging and tion can highlight the tion location
3201 3202	SA-12 (11)	SUPPLY CHAIN PROTECTION PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS	[BACK TO SCRM CONTROL]
3203 3204 3205 3206 3207 3208 3209 3210 3211 3212 3213 3214 3215 3216 3217 3218 3219		The organization employs [Selection (one or more): organizational third-party analysis, organizational penetration testing, independent testing] of [Assignment: organization-defined supply chain elements associated with the information system, system component, or infor Supplemental Guidance: This control enhancement addresses analyst supply chain, not just delivered items. Supply chain elements are infor products or product components that contain programmable logic and important to information system functions. Supply chain processes in hardware, software, and firmware development processes; (ii) shippir (iii) personnel and physical security programs; (iv) configuration mart to maintain provenance; or (v) any other programs, processes, or product specific roles and responsibilities in the supply chain. The evidence g and testing of supply chain elements, processes, and actors is docume organizational risk management activities and decisions. Related context of the production of supply chain elements. Related context of the production of supply chain elements. Related context of supply chain are specific roles and responsibilities in the supply chain. Related context of supply chain elements. Related context of supply chain are specific roles and responsibilities and decisions. Related context of supply chain are specific roles and responsibilities and decisions. Related context of supply chain are specific roles and responsibilities and decisions. Related context of supply chain are specific roles and responsibilities and decisions. Related context of supply chain are specific roles and responsibilities and decisions. Related context of supply chain are specific roles and responsibilities and decisions. Related context of supply chain are specific roles and responsibilities and decisions.	analysis, independent t third-party penetration s, processes, and actors] rmation system service. is and/or testing of the ormation technology t that are critically clude, for example: (i) ng/handling procedures; hagement tools/measures bedures associated with tors are individuals with enerated during analyses ented and used to inform trol: RA-5.
3220 3221	SA-12 (12)	SUPPLY CHAIN PROTECTION INTER-ORGANIZATIONAL AGREEMENTS	[BACK TO SCRM CONTROL]

3222		The organization establishes inter-organizational agreements and procedures with
3223		entities involved in the supply chain for the information system, system component, or
3224		information system service.
3225		Supplemental Guidance: The establishment of inter-organizational agreements and
3226		procedures provides for notification of supply chain compromises. Early notification of
3227		supply chain compromises that can potentially adversely affect or have adversely affected
3228		organizational information systems, including critical system components, is essential for
3229		organizations to provide appropriate responses to such incidents.
3230 3231	SA-12 (13)	SUPPLY CHAIN PROTECTION / CRITICAL INFORMATION SYSTEM COMPONENTS
3232		The organization employs [Assignment: organization-defined security safeguards] to
3233		ensure an adequate supply of [Assignment: organization-defined critical information
3234		system components].
3235		Supplemental Guidance: Adversaries can attempt to impede organizational operations by
3236		disrupting the supply of critical information system components or corrupting supplier
3237		operations. Safeguards to ensure adequate supplies of critical information system components
3238		include, for example: (i) the use of multiple suppliers throughout the supply chain for the
3239		identified critical components; and (ii) stockpiling of spare components to ensure operation
3240		during mission-critical times.
3241	SA-12 (14)	SUPPLY CHAIN PROTECTION / IDENTITY AND TRACEABILITY [BACK TO SCRM CONTROL]
3242		The organization establishes and retains unique identification of [Assignment:
3243		organization-defined supply chain elements, processes, and actors] for the information
3244		system, system component, or information system service.
3245		Supplemental Guidance: Knowing who and what is in the supply chains of organizations is
3246		critical to gaining visibility into what is happening within such supply chains, as well as
3247		monitoring and identifying high-risk events and activities. Without reasonable visibility and
3248		traceability into supply chains (i.e., elements, processes, and actors), it is very difficult for
3249		organizations to understand and therefore manage risk, and to reduce the likelihood of adverse
3250		events. Uniquely identifying acquirer and integrator roles, organizations, personnel, mission
3251		and element processes, testing and evaluation procedures, delivery mechanisms, support
3232		mechanisms, communications/delivery paths, and disposal/final disposition activities as well
3233		as the components and tools used, establishes a foundational identity structure for assessment
3234 2255		of supply chain activities. For example, labeling (using serial numbers) and tagging (using
3233 2756		radio-irrequency identification [RFID] tags) individual supply chain elements including
2250		software packages, modules, and nardware devices, and processes associated with those alements can be used for this number. Identification methods are sufficient to support the
3258		provenance in the event of a supply chain issue or adverse supply chain event
3259 3260	SA-12 (15)	SUPPLY CHAIN PROTECTION / PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES [BACK TO SCRM CONTROL]
3261		The organization establishes a process to address weaknesses or deficiencies in supply
3262		choin alamants identified during independent or organizational assessments of such
3263		elements.
3264		Supplemental Guidance: Evidence generated during independent or organizational
3265		assessments of supply chain elements (e.g., penetration testing, audits, verification/validation
3266		activities) is documented and used in follow-on processes implemented by organizations to
3267		respond to the risks related to the identified weaknesses and deficiencies. Supply chain
3268		elements include, for example, supplier development processes and supplier distribution
3269		systems.

3270 3271		References: NIST Special Publication 800-161; NIST Interagency Report 7622. Priority and Baseline Allocation:							
		P1	LOW Not Selected		MOD Not Selected		HIGH SA-12		
3272					nob not bleeted				
3273	SA-14	CRITI	ICALITY ANALYSIS				[Back to SCRM Cor	<u>itrol]</u>	
3274 3275 3276 3277		Contr perfo inforr define	<u>Control</u> : The organization identifies critical information system components and functions by performing a criticality analysis for [<i>Assignment: organization-defined information systems, information system components, or information system services</i>] at [<i>Assignment: organization-defined decision points in the system development life cycle</i>]						
3278 3279 3280 3281 3282 3283 3284 3285 3286 3287 3288 3289 3290 3291 3292 3293 3294		<u>Supplemental Guidance</u> : Criticality analysis is a key tenet of supply chain risk management and informs the prioritization of supply chain protection activities such as attack surface reduction, use of all-source intelligence, and tailored acquisition strategies. Information system engineers can conduct an end-to-end functional decomposition of an information system to identify mission-critical functions and components. The functional decomposition includes the identification of core organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and beyond the information system boundary. Information system components that allow for unmediated access to critical components or functions are considered critical due to the inherent vulnerabilities such components create. Criticality is assessed in terms of the impact of the function or component failure on the ability of the component to complete the organizational missions supported by the information system. A criticality analysis is performed whenever an architecture or design is being developed or modified, including upgrades. Related controls: CP-2, PL-2, PL-8, PM-1, SA-8, SA-12, SA-13, SA-15, SA-20.							
		P0	LOW Not Selected		MOD Not Selected		HIGH Not Selected		
3295									
3296	SA-15	DEVE	CLOPMENT PROCESS, ST	ANDARI	DS, AND TOOLS		[Back to SCRM Cor	itrol]	
3297		Contr	rol: The organization:						
3298 3299		a. Requires the developer of the information system, system component, or information system service to follow a documented development process that:							
3300		1	1. Explicitly addresses security requirements;						
3301		2. Identifies the standards and tools used in the development process;							
3302 3303		3. Documents the specific tool options and tool configurations used in the development process; and							
3304 3305		4	 Documents, manage used in development 	es, and e nt; and	ensures the integrity of c	changes	to the process and/or tools	5	
3306 3307 3308 3309		b. F [. a	Reviews the development Assignment: organizati and tool options/configu- defined security require	nt procest ion-define trations st ments].	ss, standards, tools, and <i>led frequency</i>] to determ selected and employed of	tool opt nine if th can satis	tions/configurations te process, standards, tools fy [Assignment: organiza	s, tion-	

3310 3311 3312 3313 3314 3315 3316		<u>Supplemental Guidance</u> : Developm computer-aided design (CAD) system example, the use of maturity models Maintaining the integrity of changes assessment and mitigation, and require (including design, development, tran- authorized changes and prevent unau-	ent tools include, for example, p ms. Reviews of development pro- to determine the potential effect to tools and processes enables a irres robust configuration contro- isport, delivery, integration, and athorized changes. Related contro-	programming languages and occesses can include, for tiveness of such processes. accurate supply chain risk l throughout the life cycle maintenance) to track rols: SA-3, SA-8.
3317		Control Enhancements:		
3318 3319	SA-15 (3)	DEVELOPMENT PROCESS, STANDAI ANALYSIS	RDS, AND TOOLS / CRITICALITY	[BACK TO SCRM CONTROL]
3320 3321 3322 3323 3324 3325 3326 3327 3328 3329 3330		The organization requires the or information system service organization-defined breadth/d points in the system development Supplemental Guidance: This c analysis performed by organizat because organizations may not l system components that are dev technology products (e.g., funct source code/hardware schematic	developer of the information to perform a criticality analys <i>(epth)</i> and at [Assignment: orgont <i>life cycle]</i> . ontrol enhancement provides de tions in SA-14. Developer input have access to detailed design de eloped as commercial off-the-sl ional specifications, high-level cs). Related controls: SA-4, SA-	system, system component, sis at [Assignment: anization-defined decision eveloper input to the criticality is essential to such analysis ocumentation for information helf (COTS) information designs, low-level designs, and 14.
3331 3332	SA-15 (4)	DEVELOPMENT PROCESS, STANDA MODELING / VULNERABILITY ANAL	RDS, AND TOOLS THREAT YSIS	[BACK TO SCRM CONTROL]
3333 3334 3335		The organization requires tha analysis for the information sy that:	t developers perform threat m //stem at [<i>Assignment: organize</i>	nodeling and a vulnerability ntion-defined breadth/depth]
3336 3337		(a) Uses [Assignment: organiz of operations, known or as	ation-defined information consumed threats, and acceptable	cerning impact, environment risk levels];
3338		(b) Employs [Assignment: org	anization-defined tools and me	ethods]; and
3339		(c) Produces evidence that m	eets [Assignment: organization	-defined acceptance criteria].
3340		Supplemental Guidance: Relate	ed control: SA-4.	
3341 3342	SA-15 (8)	DEVELOPMENT PROCESS, STANDAI THREAT / VULNERABILITY INFORM	RDS, AND TOOLS REUSE OF ATION	[BACK TO SCRM CONTROL]
3343 3344 3345 3346		The organization requires the or information system service similar systems, components, Supplemental Guidance: Analy	developer of the information to use threat modeling and vu or services to inform the curre sis of vulnerabilities found in si	system, system component, Inerability analyses from ent development process. milar software applications
3347 3348 3349 3350		can inform potential design or in development. Similar information organizations. Authoritative vul private sector sources including	nplementation issues for inform on systems or system componen nerability information is availab , for example, the National Vult	hation systems under tts may exist within developer ble from a variety of public and herability Database.
3351		References: None.		
3352		Priority and Baseline Allocation:		
		P2 LOW Not Selected	MOD Not Selected	HIGH SA-15
3353				

3354 [Back to SCRM Control] SA-16 **DEVELOPER-PROVIDED TRAINING** 3355 Control: The organization requires the developer of the information system, system component, 3356 or information system service to provide [Assignment: organization-defined training] on the 3357 correct use and operation of the implemented security functions, controls, and/or mechanisms. 3358 Supplemental Guidance: This control applies to external and internal (in-house) developers. 3359 Training of personnel is an essential element to ensure the effectiveness of security controls 3360 implemented within organizational information systems. Training options include, for example, 3361 classroom-style training, web-based/computer-based training, and hands-on training. 3362 Organizations can also request sufficient training materials from developers to conduct in-house 3363 training or offer self-training to organizational personnel. Organizations determine the type of 3364 training necessary and may require different types of training for different security functions, 3365 controls, or mechanisms. Related controls: AT-2, AT-3, SA-5. 3366 3367 References: None. 3368 Priority and Baseline Allocation: P2 LOW Not Selected MOD Not Selected HIGH SA-16 3369 3370 SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN [Back to SCRM Control] 3371 3372 Control: The organization requires the developer of the information system, system component, 3373 or information system service to produce a design specification and security architecture that: 3374 Is consistent with and supportive of the organization's security architecture which is a 3375 established within and is an integrated part of the organization's enterprise architecture; 3376 Accurately and completely describes the required security functionality, and the allocation of b. 3377 security controls among physical and logical components; and 3378 c. Expresses how individual security functions, mechanisms, and services work together to 3379 provide required security capabilities and a unified approach to protection. 3380 Supplemental Guidance: This control is primarily directed at external developers, although it could 3381 also be used for internal (in-house) development. In contrast, PL-8 is primarily directed at internal 3382 developers to help ensure that organizations develop an information security architecture and such 3383 security architecture is integrated or tightly coupled to the enterprise architecture. This distinction 3384 is important if/when organizations outsource the development of information systems, information 3385 system components, or information system services to external entities, and there is a requirement 3386 to demonstrate consistency with the organization's enterprise architecture and information security 3387 architecture. Related controls: PL-8, PM-7, SA-3, SA-8. 3388 3389 References: None. 3390 Priority and Baseline Allocation: **P**1 LOW Not Selected MOD Not Selected HIGH SA-17 3391 3392 [Back to SCRM Control] **SA-18** TAMPER RESISTANCE AND DETECTION 3393

3394 3395		<u>Control</u> : The organization implements a tamper protection program for the information system, system component, or information system service.				
3396 3397 3398 3399 3400 3401		<u>Supplemental Guidance</u> : Anti-tamper technologies and techniques provide a level of protection for critical information systems, system components, and information technology products against a number of related threats including modification, reverse engineering, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting information systems, components, and products during distribution and when in use. Related controls: PE-3, SA-12, SI-7.				
3402		Control Enhancements:				
3403 3404	SA-18 (1)	TAMPER RESISTANCE AND DETECTION MULTIPLE PHASES OF SDLC [BACK TO SCRM CONTROL]				
3405 3406 3407 3408 3409		The organization employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including design, development, integration, operations, and maintenance. Supplemental Guidance: Organizations use a combination of hardware and software				
3410 3411 3412 3413 3414		techniques for tamper resistance and detection. Organizations employ obfuscation and self- checking, for example, to make reverse engineering and modifications more difficult, time- consuming, and expensive for adversaries. Customization of information systems and system components can make substitutions easier to detect and therefore limit damage. Related control: SA-3.				
3415 3416	SA-18 (2)	TAMPER RESISTANCE AND DETECTION / INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES[BACK TO SCRM CONTROL]				
3417 3418 3419 3420 3421		The organization inspects [Assignment: organization-defined information systems, system components, or devices] [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering.				
3422 3423 3424 3425 3426		Supplemental Guidance: This control enhancement addresses both physical and logical tampering and is typically applied to mobile devices, notebook computers, or other system components taken out of organization-controlled areas. Indications of need for inspection include, for example, when individuals return from travel to high-risk locations. Related control: SI-4				
3427		References: None.				
3428		Priority and Baseline Allocation:				
		P0 LOW Not Selected MOD Not Selected HIGH Not Selected				
3429						
3430	SA-19	COMPONENT AUTHENTICITY [Back to SCRM Control]				
3431						
3432		<u>Control</u> : The organization:				
3433 3434		a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; and				
3435 3436 3437		b. Reports counterfeit information system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]].				

3438 3439 3440 3441		<u>Supp</u> devel resist repor	lemental Guidance: Sources of lopers, vendors, and contractors ance and provide a level of pro- ting organizations include, for e	counterfeit components includ Anti-counterfeiting policy and tection against the introduction example, US-CERT. Related co	e, for example, manufacturers, l procedures support tamper of malicious code. External ontrols: PE-3, SA-12, SI-7.
3442		Cont	rol Enhancements:		
3443	SA-19 (1)	(COMPONENT AUTHENTICITY ANT	I-COUNTERFEIT TRAINING	[BACK TO SCRM CONTROL]
3444 3445 3446] c f	The organization trains [<i>Assig</i> counterfeit information systen ïrmware).	nment: organization-defined p n components (including hard	<i>personnel or roles</i>] to detect lware, software, and
3447 3448	SA-19 (2)	(COMPONENT AUTHENTICITY CON COMPONENT SERVICE / REPAIR	FIGURATION CONTROL FOR	[BACK TO SCRM CONTROL]
3449 3450 3451 3452			The organization maintains co defined information system con components awaiting return to	onfiguration control over [<i>Ass ponents</i>] awaiting service/rej o service.	<i>ignment: organization-</i> pair and serviced/repaired
3453	SA-19 (3)	(COMPONENT AUTHENTICITY COM	IPONENT DISPOSAL	[BACK TO SCRM CONTROL]
3454					
3455 3456] 6	The organization disposes of in organization-defined technique	nformation system componen as and methods].	ts using [Assignment:
3457 3458		<u>2</u> S	Supplemental Guidance: Proper such components from entering	r disposal of information system the gray market.	n components helps to prevent
3459	SA-19 (4)	(COMPONENT AUTHENTICITY ANT	I-COUNTERFEIT SCANNING	[BACK TO SCRM CONTROL]
3460 3461 3462] 6	The organization scans for cou organization-defined frequency	unterfeit information system o	components [Assignment:
3463		Refer	ences: None.		
3464		<u>Priorit</u>	y and Baseline Allocation:		
		P0	LOW Not Selected	MOD Not Selected	HIGH Not Selected
3465					
3466	SA-20	CUST	OMIZED DEVELOPMENT OF CR	ITICAL COMPONENTS	[Back to SCRM Control]
3467 3468 3469		<u>Cont</u> <i>critic</i>	rol: The organization re-impler al information system compone	nents or custom develops [Assignts].	gnment: organization-defined
3470 3471 3472 3473 3474 3475 3476 3477		Supp likely which imple highe hardy succe re-im	lemental Guidance: Organizati v cannot be trusted due to specif h there are no viable security co ementation or custom developm er assurance. This is accomplish ware, software, and firmware) sp eed. In situations where no alter plement or custom develop crit	ons determine that certain infor fic threats to and vulnerabilities ontrols to adequately mitigate the ent of such components helps t ued by initiating changes to syst uch that the standard attacks by native sourcing is available and ical information system compo	mation system components in those components, and for re resulting risk. Re- o satisfy requirements for em components (including adversaries are less likely to l organizations choose not to nents, additional safeguards

3478 3479		can be employed (e.g., enhanced auditing, restrictions on source code and system utility access, and protection from deletion of system and application files. Related controls: CP-2, SA-8, SA-14.					
3480		Control Enhancements: None.					
3481		References: None.					
3482		Priority and Baseline Allocation					
3483		PO	LOW	Not Selected	MOD Not Selected	HIGH Not Selected	
3484	SA-21	DEVEI	LOPER	SCREENING		[Back to SCRM Control]	
3485 3486 3487		<u>Contro</u> inform	<u>ol</u> : Th nation	e organization requires t system, system compone	hat the developer of [Assignment nt, or information system service	nt: organization-defined re]:	
3488 3489		а. Н <i>de</i>	ave ap efined	propriate access authoriz	zations as determined by assign <i>es</i>]; and	ed [Assignment: organization-	
3490		b. Sa	atisfy	Assignment: organization	on-defined additional personnel	screening criteria].	
3491 3492 3493 3494 3495 3496 3497 3498 3497 3500 3501 3502 3503 3504 3505 3506 3507 3508 3509	Control SA-21 (1)	 b. Satisfy [Assignment: organization-defined additional personnel screening criteria]. <u>Supplemental Guidance</u>: Because the information system, system component, or information system service may be employed in critical activities essential to the national and/or economic security interests of the United States, organizations have a strong interest in ensuring that the developer is trustworthy. The degree of trust required of the developer may need to be consisten with that of the individuals accessing the information system/component/service once deployed. Examples of authorization and personnel screening criteria include clearance, satisfactory background checks, citizenship, and nationality. Trustworthiness of developers may also include review and analysis of company ownership and any relationships the company has with entities potentially affecting the quality/reliability of the systems, components, or services being developed. Related controls: PS-3, PS-7. <u>Control Enhancements:</u> SA-21 (1) DEVELOPER SCREENING / VALIDATION OF SCREENING <u>The organization requires the developer of the information system, system component or information system service take [Assignment: organization-defined actions] to ensurt that the required access authorizations and screening criteria are satisfied. Supplemental Guidance: Satisfying required access authorizations and personnel screening</u> 					
3510 3511		system service so that organizations can validate that the developer has satisfied the necessary authorization and screening requirements.					
3512		References: None.					
3513		Priority	and Ba	aseline Allocation:			
		PO	LOW	Not Selected	MOD Not Selected	HIGH Not Selected	
3514							
3515	SA-22	UNSUP	PORT	ED SYSTEM COMPONENT	ſS	[Back to SCRM Control]	
3516 3517		<u>Contro</u>	<u>ol</u> : Th	e organization:			

3518 3519		a. R a	eplaces information system convailable from the developer, ve	mponents when support for the ndor, or manufacturer; and	components is no longer	
3520 3521		b. P c	rovides justification and docun omponents required to satisfy r	nents approval for the continued nission/business needs.	d use of unsupported system	
3522 3523 3524 3525 3526 3527 3528 3528 3529		Suppl softw comp substa install examp not av option	emental Guidance: Support for are patches, firmware updates, onents (e.g., when vendors are antial opportunity for adversarie led components. Exceptions to ple, systems that provide critica vailable or where the systems ar h. Related controls: PL-2, SA-3	r information system componer replacement parts, and mainten no longer providing critical sof es to exploit new weaknesses di replacing unsupported system o al mission/business capability w re so isolated that installing rep	ts includes, for example, ance contracts. Unsupported tware patches), provide a iscovered in the currently components may include, for there newer technologies are lacement components is not an	
3530		Contr	ol Enhancements:			
3531 3532	SA-22 (1)	U F	NSUPPORTED SYSTEM COMPONE FOR CONTINUED SUPPORT	NTS ALTERNATIVE SOURCES	[BACK TO SCRM CONTROL]	
3533 3534 3535 3536 3537 3538 3539 3540 3541 3542 3543		The organization provides [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]] for unsupported information system components. Supplemental Guidance: This control enhancement addresses the need to provide continued support for selected information system components that are no longer supported by the original developers, vendors, or manufacturers when such components remain essential to mission/business operations. Organizations can establish in-house support, for example, by developing customized patches for critical software components or secure the services of external providers who through contractual relationships, provide ongoing support for the designated unsupported components. Such contractual relationships can include, for example, Onen Source Software value-added vendors				
3544		Refere	ences: None.			
3545		Priority	vand Baseline Allocation:			
		PO	LOW Not Selected	MOD Not Selected	HIGH Not Selected	

3548 FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

3549 3550	SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES Back to SCRM Control]			
3551		Control: The organization:			
3552 3553		a. Develops, documents, and disseminates to [<i>Assignment: organization-defined personnel or roles</i>]:			
3554 3555 3556		1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and			
3557 3558		2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and			
3559		b. Reviews and updates the current:			
3560 3561		1. System and communications protection policy [Assignment: organization-defined frequency]; and			
3562 3563		2. System and communications protection procedures [<i>Assignment: organization-defined frequency</i>].			
3564 3565 3566 3567 3568 3569 3570 3571 3572 3573		<u>Supplemental Guidance</u> : This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policies and procedures. Belated control: PM 0.			
3574		Control Enhancements: None.			
3575		References: NIST Special Publications 800-12, 800-100.			
3576		Priority and Baseline Allocation:			
		PL LOW SC.1 MOD SC.1 HIGH SC 1			

3577

3578 sc-4 information in shared resources

[Back to SCRM Control]

3579 <u>Control</u>: The information system prevents unauthorized and unintended information transfer via shared system resources.

3581 Supplemental Guidance: This control prevents information, including encrypted representations 3582 of information, produced by the actions of prior users/roles (or the actions of processes acting on 3583 behalf of prior users/roles) from being available to any current users/roles (or current processes) 3584 that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those 3585 resources have been released back to information systems. The control of information in shared 3586 resources is also commonly referred to as object reuse and residual information protection. This 3587 control does not address: (i) information remanence which refers to residual representation of data 3588 that has been nominally erased or removed; (ii) covert channels (including storage and/or timing 3589 channels) where shared resources are manipulated to violate information flow restrictions; or (iii) 3590 components within information systems for which there are only single users/roles. Related 3591 controls: AC-3, AC-4, MP-6.

3592								
3593		References: None.						
3594		Priorit	y and Baseline Allocatio	on:				
		P1	LOW Not Selected		MOD SC-4		HIGH SC-4	
3595								
3596	SC-5	DENL	AL OF SERVICE PROT	TECTION				
3597 3598 3599 3600		<u>Contro</u> denia <i>refere</i> secur	<u>bl</u> : The information s l of service attacks: [ence to source for suc ity safeguards].	ystem prot Assignmer ch informa	ects against or limits t at: organization-define tion] by employing [A	the effects ed types of assignmen	s of the following types of f denial of service attacks or t: organization-defined	
3601 3602 3603 3604 3605 3606 3607		Supple effect types from bandy servic	<u>Supplemental Guidance</u> : A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect information system components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks. Related controls: SC-6, SC-7.					
3608		Contr	ol Enhancements:					
3609 3610	SC-5 (2)	L /	DENIAL OF SERVICE PR REDUNDANCY	OTECTION	EXCESS CAPACITY / BAN	NDWIDTH	[BACK TO SCRM CONTROL]	
3611 3612 3613 3614 3615 3616 3617		T li <u>S</u> a e <u>Refere</u> <u>Priorit</u>	The information system imit the effects of in Supplemental Guidan available to counter flestablishing selected to ences: None. y and Baseline Allocation	tem mana formation <u>ce</u> : Manaş looding att usage prior on:	ges excess capacity, h flooding denial of se ging excess capacity en acks. Managing excess ities, quotas, or partiti	bandwidt ervice att: nsures tha s capacity ioning.	h, or other redundancy to acks. at sufficient capacity is 7 may include, for example,	
		P1	LOW SC-5		MOD SC-5		HIGH SC-5	
3618								
3619	SC-7	BOUN	DARY PROTECTION				[Back to SCRM Control]	
3620 3621		<u>Control</u> : The information system:						
3622 3623		a. N	Monitors and controls nternal boundaries w	s communi ithin the sy	cations at the external vstem;	boundary	y of the system and at key	
3624 3625		b. Implements subnetworks for publicly accessible system components that are [<i>Selection: physically; logically</i>] separated from internal organizational networks; and						
3626 3627 3628		c. C c s	Connects to external a consisting of boundar ecurity architecture.	networks o y protectic	r information systems n devices arranged in	only thro accordan	ough managed interfaces ce with an organizational	
3629 3630 3631		Suppl guard imple	lemental Guidance: I ls, network-based ma emented within a secu	Managed i licious coo urity archit	nterfaces include, for le analysis and virtual ecture (e.g., routers pr	example, ization sy cotecting f	gateways, routers, firewalls, stems, or encrypted tunnels firewalls or application	

3632 3633 3634 3635 3636 3637 3638 3639 3640 3641 3642		gatew separa prohil extern traffic comm with t netwo custor Such provis	vays residing ated from in biting interfa- nal web traff that appear nercial teleco- the use of su ork compone- mers, and m transmission sions. Related	g on protect ternal netw aces within fic to design to be sport communication ch services ents and co ay also incon- a services field controls	ted subnetworks). Subnetworks are referred to as der organizational information nated web servers within r ofing internal addresses. C ions services in the impler s. Commercial telecommunity nsolidated management sy lude third party-provided in may represent sources of in the commercial telecommunity and the commercial telecommunity and the commercial telecommunity services of the community and the commercial telecommunity and the commercial telecommunity and the community and the community and the commercial telecommunity and the commercial telecommunity and the community and the commercial telecommunity and the commercial telecommunity and the community and the commercial telecommunity and the community and the commercial telecommunity and the community and the community and the community and the commercial telecommunity and the community and the commercial telecommunity and the community and the	works tha militarize on system managed Organizat mentation nications ystems sh access lin ncreased A-7, CP-8	t are physically or logically d zones or DMZs. Restricting or is includes, for example, restricting interfaces and prohibiting external ions consider the shared nature of n of security controls associated services are commonly based on ared by all attached commercial hes and other service elements. risk despite contract security 8, IR-4, RA-3, SC-5, SC-13.
3643		Contr	ol Enhancer	nents:			
3644 3645	SC-7 (13)	B N	OUNDARY PR IECHANISMS	ROTECTION / SUPPORT	ISOLATION OF SECURITY TO COMPONENTS	OOLS /	[BACK TO SCRM CONTROL]
3646 3647 3648 3649 3650		T n c t	The organize nechanisms, omponents o other com	ation isola , <i>and supp</i> by impler iponents o	tes [Assignment: organize ort components] from oth nenting physically separa f the system.	<i>ation-def</i> her intern ate subne	<i>ined information security tools,</i> nal information system etworks with managed interfaces
3651 3652 3653 3654		S f n o	upplementa or example, etworks to p organizations	<u>l Guidance</u> in isolatin prevent adv s. Related o	2: Physically separate sub- g computer network defen- versaries from discovering controls: SA-8, SC-2, SC-3	networks uses from the analy 3.	with managed interfaces are useful, critical operational processing /sis and forensics techniques of
3655 3656	SC-7 (19)	B C	OUNDARY PR DRGANIZATIO	ROTECTION NALLY CON	BLOCKS COMMUNICATION FIGURED HOSTS	FROM NO	N- [BACK TO SCRM CONTROL]
3657 3658 3659 3660 3661 3662 3663 3664 3665 3665 3666		T bb in S e d a <u>Refere</u>	The information of the informati	ation syste signment: ly configu l Guidance ice provide ly to comm nctions.	m blocks both inbound a organization-defined com red by end users and ext organization clients communication clients rs include, for example, in nunication clients that are of 99; NIST Special Publications	and outbo mmunicat ternal ser independ nstant me configure s 800-41, 8	bund communications traffic <i>ion clients</i>] that are vice providers. lently configured by end users and ssaging clients. Traffic blocking ed by organizations to perform
3667		Priority	y and Baseline	e Allocation			
3668		P1	LOW SC-7		MOD SC-7 (3) (4) (5) (7)	HIG	H SC-7 (3) (4) (5) (7) (8) (18) (21)
3669	SC-8	TRAN	SMISSION C	ONFIDENT	IALITY AND INTEGRITY		[Back to SCRM Control]
3670 3671 3672		<u>Contr</u> of tra	<u>ol</u> : The info nsmitted inf	ormation s formation.	stem protects the [Selection	ion (one o	r more): confidentiality; integrity]
3673 3674 3675 3676		<u>Suppl</u> of inf mobil Comr	<u>emental Gu</u> ormation system le devices, n nunication p	idance: The stem composition of the stem composition of the stem composition of the stem o	his control applies to both onents from which inform omputers, printers, copiers le the physical protection	internal a nation car s, scanner of a contr	nd external networks and all types to be transmitted (e.g., servers, s, facsimile machines). colled boundary are exposed to the

3677 3678 3679 3680 3681 3682 3683 3684 3685 3684 3685 3686 3687 3688		possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing physical distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk. Related controls: AC-17, PE-4.				
3689						
3690 3691		Refere Policy	ences: FIPS Publications 140-2, 19 15; NSTISSI No. 7003.	7; NIST Special Publications 800-5	2, 800-77, 800-81, 800-113; CNSS	
3692		<u>Priorit</u>	y and Baseline Allocation:			
		P1	LOW Not Selected	MOD SC-8 (1)	HIGH SC-8 (1)	
3693						
3694	SC-18	MOBI	ILE CODE		[Back to SCRM Control]	
3695 3696		<u>Conti</u>	<u>col</u> : The organization:			
3697		a. I	Defines acceptable and unaccept	table mobile code and mobile c	ode technologies;	
3698 3699		b. H r	Establishes usage restrictions an nobile code technologies; and	d implementation guidance for	acceptable mobile code and	
3700		c . <i>A</i>	Authorizes, monitors, and contro	ols the use of mobile code within	in the information system.	
3701 3702 3703 3704 3705 3706 3707 3708 3709		Supp organ system Activ and in serve smart acqui system	lemental Guidance: Decisions n izational information systems a ms if used maliciously. Mobile eX, Postscript, PDF, Shockwav mplementation guidance apply t rs and mobile code downloaded phones). Mobile code policy as sition, or introduction of unacce ms. Related controls: AU-2, AU	regarding the employment of m re based on the potential for the code technologies include, for over we movies, Flash animations, an to both the selection and use of and executed on individual wo and procedures address preventing eptable mobile code within organ J-12, CM-2, CM-6, SI-3.	obile code within e code to cause damage to the example, Java, JavaScript, d VBScript. Usage restrictions mobile code installed on orkstations and devices (e.g., ng the development, anizational information	
3710		<u>Cont</u>	ol Enhancements:			
3711	SC-18(2)	1	MOBILE CODE ACQUISITION / DE	VELOPMENT / USE	[BACK TO SCRM CONTROL]	
3712 3713 3714			The organization ensures that leployed in the information sy code requirements].	the acquisition, development, stem meets [Assignment: org	, and use of mobile code to be anization-defined mobile	
3715		Refere	ences: NIST Special Publication 80	0-28; DoD Instruction 8552.01.		
3716		<u>Priorit</u>	y and Baseline Allocation:			
		P2	LOW Not Selected	MOD SC-18	HIGH SC-18	

3718 SC-27 PLATFORM-INDEPENDENT APPLICATIONS [Back to SCRM Control] 3719 <u>Control</u>: The information system includes: [Assignment: organization-defined platform-3720 independent applications]. 3721 Supplemental Guidance: Platforms are combinations of hardware and software used to run 3722 software applications. Platforms include: (i) operating systems; (ii) the underlying computer 3723 architectures, or (iii) both. Platform-independent applications are applications that run on multiple 3724 platforms. Such applications promote portability and reconstitution on different platforms, 3725 increasing the availability of critical functions within organizations while information systems 3726 with specific operating systems are under attack. Related control: SC-29. 3727 Control Enhancements: None. 3728 References: None. 3729 Priority and Baseline Allocation: **P0** LOW Not Selected MOD Not Selected HIGH Not Selected 3730 3731 SC-28 PROTECTION OF INFORMATION AT REST [Back to SCRM Control] 3732 Control: The information system protects the [Selection (one or more): confidentiality; integrity] 3733 of [Assignment: organization-defined information at rest]. 3734 Supplemental Guidance: This control addresses the confidentiality and integrity of information at 3735 rest and covers user information and system information. Information at rest refers to the state of 3736 information when it is located on storage devices as specific components of information systems. 3737 System-related information requiring protection includes, for example, configurations or rule sets 3738 for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator 3739 content. Organizations may employ different mechanisms to achieve confidentiality and integrity 3740 protections, including the use of cryptographic mechanisms and file share scanning. Integrity 3741 protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) 3742 technologies. Organizations may also employ other security controls including, for example, 3743 secure off-line storage in lieu of online storage when adequate protection of information at rest 3744 cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest. 3745 Related controls: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7. 3746 3747 References: NIST Special Publications 800-56, 800-57, 800-111. 3748 Priority and Baseline Allocation: LOW Not Selected MOD SC-28 HIGH SC-28 P1 3749 3750 SC-29 HETEROGENEITY [Back to SCRM Control] 3751 Control: The organization employs a diverse set of information technologies for [Assignment: 3752 organization-defined information system components] in the implementation of the information 3753 system. 3754 Supplemental Guidance: Increasing the diversity of information technologies within 3755 organizational information systems reduces the impact of potential exploitations of specific 3756 technologies and also defends against common mode failures, including those failures induced by

technologies and also defends against common mode failures, including those failures induced by
supply chain attacks. Diversity in information technologies also reduces the likelihood that the
means adversaries use to compromise one information system component will be equally effective
against other system components, thus further increasing the adversary work factor to successfully

3760 3761 3762		complete planned cyber attacks. Ar overhead which could ultimately le controls: SA-12, SA-14, SC-27.	n increase in diversity may ad ad to mistakes and unauthorized ad to mistakes and unauthorized and the second seco	d complexity and management zed configurations. Related		
3763		Control Enhancements:				
3764		eferences: None.				
3765		Priority and Baseline Allocation:				
3766		DO LOW Net Selected	MOD Net Selected	HICH Net Selected		
3767		P0 LOW Not Selected	MOD Not Selected	HIGH NOT Selected		
5707						
3768	SC-30	CONCEALMENT AND MISDIRECTIO	N	[Back to SCRM Control]		
3769 3770 3771		<u>Control</u> : The organization employs misdirection techniques] for [Assign [Assignment: organization-defined]	[Assignment: organization-d nment: organization-defined time periods] to confuse and	<i>defined concealment and information systems</i>] at mislead adversaries.		
3772 3773 3774 3775 3776 3777 3778 3779 3780 3780 3781 3782		Supplemental Guidance: Concealm targeting capability of adversaries (initiate and complete cyber attacks. with the ability to disguise informat attacks without the cost of having m techniques including, for example, confuse and mislead adversaries an tradecraft. Concealment/misdirection successfully perform core missions to support concealment/misdirection used by organizations on a very lim	nent and misdirection techniq i.e., window of opportunity a For example, virtualization t tion systems, potentially redu nultiple platforms. Increased randomness, uncertainty, and d subsequently increase the r on techniques may also provid and business functions. Beca n techniques, it is anticipated nited basis. Related controls: S	ues can significantly reduce the nd available attack surface) to echniques provide organizations cing the likelihood of successful use of concealment/misdirection virtualization, may sufficiently isk of discovery and/or exposing de organizations additional time to use of the time and effort required that such techniques would be SC-26, SC-29, SI-14.		
3783		Control Enhancements:				
3784	SC-30(2)	CONCEALMENT AND MISDIRECTION / R	ANDOMNESS	[BACK TO SCRM CONTROL]		
3785 3786 3787		The organization employs [A randomness into organization	ssignment: organization-definal operations and assets.	ined techniques] to introduce		
3788 3789 3790 3791 3792 3793 3794 3795		Supplemental Guidance: Ranc adversaries regarding the action actions may impede the ability organizations supporting critica adversaries to hesitate before in involving randomness include, times of day, employing differen using different suppliers, and r	lomness introduces increased ns organizations take in defer of adversaries to correctly ta al missions/business function nitiating or continuing attacks for example, performing cert ent information technologies otating roles and responsibilit	levels of uncertainty for nding against cyber attacks. Such rget information resources of s. Uncertainty may also cause s. Misdirection techniques tain routine actions at different (e.g., browsers, search engines), ties of organizational personnel.		
3796 3797	SC-30(3)	CONCEALMENT AND MISDIRECTIC STORAGE LOCATIONS	ON / CHANGE PROCESSING /	[BACK TO SCRM CONTROL]		
3798 3799 3800		The organization changes the and/or storage] [Selection: [A. time intervals]].	e location of [Assignment: or ssignment: organization-defi	rganization-defined processing ined time frequency]; at random		
3801 3802 3803 3804 3804 3805		Supplemental Guidance: Adve functions and the information r same time, trying to minimize homogeneous, and determinist adversaries, make such system	ersaries target critical organiz resources supporting those mi exposure of their existence ar ic nature of organizational int s more susceptible to cyber ar	ational missions/business issions and functions while at the nd tradecraft. The static, formation systems targeted by ttacks with less adversary cost and		

3806 3807 3808 3809 3810 3811 3812 3813 3814 3815		e ru oo c s u oo ti t	ffort to be successful. Changing eferred to as moving target defe echniques such as virtualization rganizations to relocate the info ritical missions and business fu torage sites introduces uncertain ncertainty increases the work fa rganizational information syste he chances that adversaries may polocate critical organizational r	g organizational processing and ense) addresses the advanced per a distributed processing, and re- portation resources (i.e., process nctions. Changing locations of nty into the targeting activities la actor of adversaries making cor- ms much more difficult and time inadvertently disclose aspects resources.	storage locations (sometimes ersistent threat (APT) using plication. This enables sing and/or storage) supporting processing activities and/or by adversaries. This npromises or breaches to ne-consuming, and increases of tradecraft while attempting
3816	SC-30 (4)	(CONCEALMENT AND MISDIRECTIO	N MISLEADING INFORMATION	[BACK TO SCRM CONTROL]
3817 3818 3819		Т <i>о</i> р	The organization employs real <i>rganization-defined information posture.</i>	istic, but misleading informat on system components] with re	tion in [<i>Assignment:</i> egard to its security state or
3820 3821 3822 3823 3824 3825 3826 3827 3828		<u>S</u> tl a n s a h s	Supplemental Guidance: This con- be nature and extent of security dversaries may employ incorre- nisleading adversaries is for org pecific security controls deploy ccessed or targeted by adversar oneynets, virtualized environm ystems but use, for example, ou	ontrol enhancement misleads po safeguards deployed by organi ct (and as a result ineffective) a ganizations to place misleading ed in external information syste ies. Another technique is the us ents) that mimic actual aspects it-of-date software configuratio	otential adversaries regarding zations. As a result, ttack techniques. One way of information regarding the ems that are known to be se of deception nets (e.g., of organizational information ns.
3829 3830	SC-30(5)	C	CONCEALMENT AND MISDIRECTIO! COMPONENTS	N CONCEALMENT OF SYSTEM	[BACK TO SCRM CONTROL]
3831 3832 3833		Т с	The organization employs [Asson onceal [Assignment: organization]	signment: organization-defined tion-defined information syster	d techniques] to hide or n components].
3834 3835 3836 3837 3838		S s ta a o	Supplemental Guidance: By hid ystem components, organizatio arget and successfully compron nd/or conceal information syste r the use of honeynets or virtua	ling, disguising, or otherwise cons may be able to decrease the phise those assets. Potential mean em components include, for exa lization techniques.	oncealing critical information probability that adversaries ns for organizations to hide mple, configuration of routers
3839 3840		<u>Refere</u>	ences: None.		
5040			Vand Dasenne Anocation.		
3841		PO	LOW Not Selected	MOD Not Selected	HIGH Not Selected
3842	SC-36	DISTR	RIBUTED PROCESSING AND STO	RAGE	[Back to SCRM Control]
3843 3844		<u>Contr</u> across	ol: The organization distribute s multiple physical locations.	s [Assignment: organization-de	fined processing and storage]
3845 3846 3847 3848 3849		Suppl provie factor contro parall	emental Guidance: Distributin des some degree of redundancy of adversaries to adversely imp bl does not assume a single prin el processing and storage. Rela	g processing and storage across or overlap for organizations, an pact organizational operations, nary processing or storage locat ted controls: CP-6, CP-7.	s multiple physical locations nd therefore increases the work assets, and individuals. This tion, and thus allows for

3851		References: None.				
3852		Priority and Baseline Allocation:				
		P0 LOW Not Selected	MOD Not Selected	HIGH Not Selected		
3853						
3854	SC-37	OUT-OF-BAND CHANNELS				
3855 3856 3857 3858		<u>Control</u> : The organization employs [A the physical delivery or electronic tra <i>information system components, or d information systems</i>].	ssignment: organization-define insmission of [Assignment: org evices] to [Assignment: organiz	ed out-of-band channels] for anization-defined information, zation-defined individuals or		
3859 3860 3861 3862 3863 3864 3865 3866 3867 3868 3867 3868 3869 3870		<u>Supplemental Guidance</u> : Out-of-band c information systems, network paths p traffic, or nonelectronic paths such as same channels (i.e., in-band channels do not have the same vulnerability/ex integrity, or availability compromises channels. Organizations may employ organizational items including, for ex changes for hardware, firmware, or s updates, system/data backups, mainter Related controls: AC-2, CM-3, CM-5	channels include, for example, l bysically separate from network is the US Postal Service. This is by that carry routine operational goosure as in-band channels, and s of in-band channels will not c out-of-band channels will not c out-of-band channels in the de cample, identifiers/authenticato offware, cryptographic key man enance information, and malicio 5, CM-7, IA-4, IA-5, MA-4, SC	ocal (nonnetwork) accesses to rk paths used for operational in contrast with using the traffic. Out-of-band channels d hence the confidentiality, ompromise the out-of-band livery or transmission of many rs, configuration management nagement information, security bus code protection updates. 2-12, SI-3, SI-4, SI-7.		
3871		Control Enhancements:				
3872	SC-37(1)	OUT-OF-BAND CHANNELS ENSURE	DELIVERY / TRANSMISSION	[BACK TO SCRM CONTROL]		
3873 3874 3875 3876 2877		The organization employs [Ass ensure that only [Assignment: receive the [Assignment: organ components, or devices].	ignment: organization-defined organization-defined individud ization-defined information, in	l security safeguards] to Ils or information systems] Iformation system		
3878 3879 3880 3881 3882		<u>Supplemental Guidance</u> : Techniques and/or methods employed by organizations to ensure that only designated information systems or individuals receive particular information, system components, or devices include, for example, sending authenticators via courier service but requiring recipients to show some form of government-issued photographic identification as a condition of receipt.				
3883		References: None.				
3884		Priority and Baseline Allocation:				
		P0 LOW Not Selected	MOD Not Selected	HIGH Not Selected		
3885						
3886	SC-38	OPERATIONS SECURITY		[Back to SCRM Control]		
3887						
3888 3889 3890		<u>Control</u> : The organization employs [<i>safeguards</i>] to protect key organization cycle.	Assignment: organization-defin onal information throughout the	ned operations security e system development life		

3891	Supplemental Guidance: Operations security (OPSEC) is a systematic process by which potential
3892	adversaries can be denied information about the capabilities and intentions of organizations by
3893	identifying, controlling, and protecting generally unclassified information that specifically relates
3894	to the planning and execution of sensitive organizational activities. The OPSEC process involves
3895	five steps: (i) identification of critical information (e.g., the security categorization process); (ii)
3896	analysis of threats; (iii) analysis of vulnerabilities; (iv) assessment of risks; and (v) the application
3897	of appropriate countermeasures. OPSEC safeguards are applied to both organizational information
3898	systems and the environments in which those systems operate. OPSEC safeguards help to protect
3899	the confidentiality of key information including, for example, limiting the sharing of information
3900	with suppliers and potential suppliers of information system components, information technology
3901	products and services, and with other non-organizational elements and individuals. Information
3902	critical to mission/business success includes, for example, user identities, element uses, suppliers,
3903	supply chain processes, functional and security requirements, system design specifications, testing
3904	protocols, and security control implementation details. Related controls: RA-2, RA-5, SA-12.
3905	Control Enhancements: None.
3906	References: None.
3907	Priority and Baseline Allocation:

MOD Not Selected

HIGH Not Selected

3908

P0

LOW Not Selected

39093910 FAMILY: SYSTEM AND INFORMATION INTEGRITY

3911 3912	SI-1	SYSTEM AND INFORMATION INTEG PROCEDURES	RITY POLICY AND	[Back to SCRM Control]		
3913		Control: The organization:				
3914 3915		a. Develops, documents, and disse <i>roles</i>]:	eminates to [Assignment: organi	ization-defined personnel or		
3916 3917 3918		 A system and information responsibilities, manageme and compliance; and 	integrity policy that addresses point commitment, coordination ar	urpose, scope, roles, nong organizational entities,		
3919 3920		2. Procedures to facilitate the and associated system and	implementation of the system a information integrity controls; a	nd information integrity policy and		
3921		b. Reviews and updates the curren	t:			
3922 3923		1. System and information in and	egrity policy [Assignment: orgo	inization-defined frequency];		
3924 3925		2. System and information in <i>frequency</i>].	tegrity procedures [Assignment.	organization-defined		
3926 3927 3928 3929 3930 3931 3932 3933 3934 3935 3936 3937 3938		<u>Supplemental Guidance</u> : This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SI family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.				
3730		Phonty and Baseline Allocation.				
2020		P1 LOW SI-1	MOD SI-1	HIGH SI-1		
3939						
3940	SI-2	FLAW REMEDIATION		[Back to SCRM Control]		
3941 3942		Control: The organization:				
3943		a. Identifies, reports, and corrects	information system flaws;			
3944 3945		b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;				
3946 3947		c. Installs security-relevant softwa <i>defined time period</i>] of the release	are and firmware updates within ase of the updates; and	[Assignment: organization-		
3948		d. Incorporates flaw remediation i	nto the organizational configura	tion management process.		

 3949 3950 3951 3952 3953 3954 3955 3956 3957 3958 3959 3960 3961 3962 3963 3964 3965 3966 3967 		Supplemental Guidance: Organizati software flaws including potential vu information to designated organizati Security-relevant software updates in anti-virus signatures. Organizations a continuous monitoring, incident resp advantage of available resources suc Vulnerabilities and Exposures (CVE information systems. By incorporatin processes, required/anticipated reme actions that can be tracked and verifi follow US-CERT guidance and Infor time periods for updating security-re- factors including, for example, the se- the update (i.e., severity of the vulne remediation may require more testin type of testing needed for the specifi also the types of changes that are to may determine that the testing of sof	ons identify information system ulnerabilities resulting from tho onal personnel with information nclude, for example, patches, se also address flaws discovered d oonse activities, and system error thas the Common Weakness Er databases in remediating flaw ng flaw remediation into ongoin diation actions can be tracked a ied include, for example, detern rmation Assurance Vulnerabilit elevant software and firmware n ecurity category of the informat erability related to the discovere g than other types. Organization ic type of flaw remediation activ be configuration-managed. In so ftware and/or firmware updates	as affected by announced se flaws, and report this a security responsibilities. rvice packs, hot fixes, and uring security assessments, r handling. Organizations take numeration (CWE) or Common s discovered in organizational ag configuration management nd verified. Flaw remediation nining whether organizations y Alerts. Organization-defined hay vary based on a variety of ion system or the criticality of d flaw). Some types of flaw ns determine the degree and vity under consideration and ome situations, organizations is not necessary or practical,
3968		for example, when implementing sin	nple anti-virus signature update	s. Organizations may also
3969		consider in testing decisions, whethe	er security-relevant software or	firmware updates are obtained
3970 3971		CM-5, CM-8, MA-2, IR-4, RA-5, S/	A-10. SA-11. SI-11.	control: CA-2, CA-7, CM-3,
3972 3973	SI-2(5)	FLAW REMEDIATION AUTOMATIC UPDATES	SOFTWARE / FIRMWARE	[BACK TO SCRM CONTROL]
3974 3975 3976 3977		The organization installs [Assi and firmware updates] automa system components].	ignment: organization-defined tically to [Assignment: organiz	security-relevant software zation-defined information
3978 3979 3980 3981 3982		Supplemental Guidance: Due to organizations give careful consi updates. Organizations must bal as possible with the need to mai operational impacts that automa	o information system integrity a deration to the methodology use lance the need to ensure that the intain configuration managemen- tic updates might impose.	nd availability concerns, ed to carry out automatic updates are installed as soon it and with any mission or
3983		References: NIST Special Publications 8	300-40, 800-128.	
3984		Priority and Baseline Allocation:		
		P1 LOW SI-2	MOD SI-2 (2)	HIGH SI-2 (1) (2)
3985				
3986	SI-4	INFORMATION SYSTEM MONITORIN	G	[Back to SCRM Control]
3987		Control: The organization:		
3988		a. Monitors the information system	n to detect:	
3989 3990		1. Attacks and indicators of po defined monitoring objectiv	otential attacks in accordance w ves]; and	ith [Assignment: organization-
3991		2. Unauthorized local, network	k, and remote connections;	
3992 3993		b. Identifies unauthorized use of the <i>defined techniques and methods</i>	ne information system through [i];	Assignment: organization-
3994 3995 3996		c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;		
---	-----------	--		
3997 3998		d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;		
3999 4000 4001 4002		e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;		
4003 4004		f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and		
4005 4006 4007		g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].		
$\begin{array}{r} 4008\\ 4009\\ 4010\\ 4011\\ 4012\\ 4013\\ 4014\\ 4015\\ 4016\\ 4017\\ 4018\\ 4019\\ 4020\\ 4021\\ 4022\\ 4023\\ 4024\\ 4025\\ 4024\\ 4025\\ 4026\\ 4027\\ 4028\\ 4029\\ 4030\\ 4031\\ 4032\\ \end{array}$		<u>Supplemental Guidance</u> : Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device of wireless. Relate control: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-		
4033		Control Enhancements:		
4034 4035	SI-4 (17)	INFORMATION SYSTEM MONITORING INTEGRATED SITUATIONAL AWARENESS [BACK TO SCRM CONTROL]		
4036 4037		The organization correlates information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.		
4038 4039 4040 4041 4042 4043 4044		<u>Supplemental Guidance</u> : This control enhancement correlates monitoring information from a more diverse set of information sources to achieve integrated situational awareness. Integrated situational awareness from a combination of physical, cyber, and supply chain monitoring activities enhances the capability of organizations to more quickly detect sophisticated cyber attacks and investigate the methods and techniques employed to carry out such attacks. In contrast to SI-4 (16) which correlates the various cyber monitoring information, this control enhancement correlates monitoring beyond just the cyber domain. Such monitoring may help		

4045 4046		r c	eveal attacks on organizations t ontrol: SA-12.	hat are operating across multip	le attack vectors. Related
4047 4048	SI-4 (19)	i C	NFORMATION SYSTEM MONITORI GREATER RISK	NG INDIVIDUALS POSING	[BACK TO SCRM CONTROL]
4049 4050 4051		T o P	The organization implements of individuals who have been i posing an increased level of right	[Assignment: organization-def dentified by [Assignment: org sk.	fined additional monitoring] anization-defined sources] as
4052		<u>S</u>	Supplemental Guidance: Indica	tions of increased risk from ind	lividuals can be obtained from
4053		a	variety of sources including, for	or example, human resource rec	cords, intelligence agencies,
4054		la	aw enforcement organizations,	and/or other credible sources. T	The monitoring of individuals
4055		i	s closely coordinated with man	agement, legal, security, and hu	man resources officials within
4056		C	rganizations conducting such r	nonitoring and complies with fe	ederal legislation, Executive
4057		(Orders, policies, directives, regu	ilations, and standards.	
4058					
4059		Refere	ences: NIST Special Publications 8	00-61, 800-83, 800-92, 800-94, 800)-137.
4060		Priorit	y and Baseline Allocation:		
		P1	LOW SI-4	MOD SI-4 (2) (4) (5)	HIGH SI-4 (2) (4) (5)
4061					
4062	SI-5	SECU	RITY ALERTS, ADVISORIES, AN	D DIRECTIVES	[Back to SCRM Control]
4063		Contr	<u>ol</u> : The organization:		
4064 4065		a. F	Receives information system se organization-defined external of	curity alerts, advisories, and dir rganizations] on an ongoing ba	ectives from [Assignment: sis;
4066		b. (Generates internal security alert	s, advisories, and directives as	deemed necessary;
4067 4068 4069 4070		c. Disseminates security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]: and			ection (one or more): ment: organization-defined lefined external
4071 4072		d. I is	mplements security directives i ssuing organization of the degree	n accordance with established t ee of noncompliance.	ime frames, or notifies the
4073 4074 4075 4076 4077 4078 4079 4080 4081 4082		<u>Supplemental Guidance</u> : The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations. Related control: SI-2.			
4083		<u>Refer</u> e	ences: NIST Special Publication 80	0-40.	
4084		Priorit	y and Baseline Allocation:		
		P1	LOW SI-5	MOD SI-5	HIGH SI-5 (1)

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

4087Control: The organization employs integrity verification tools to detect unauthorized changes to
[Assignment: organization-defined software, firmware, and information].

4089 Supplemental Guidance: Unauthorized changes to software, firmware, and information can occur 4090 due to errors or malicious activity (e.g., tampering). Software includes, for example, operating 4091 systems (with key internal components such as kernels, drivers), middleware, and applications. 4092 Firmware includes, for example, the Basic Input Output System (BIOS). Information includes 4093 metadata such as security attributes associated with information. State-of-the-practice integrity-4094 checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and 4095 associated tools can automatically monitor the integrity of information systems and hosted 4096 applications. Related controls: SA-12, SC-8, SC-13, SI-3.

4097 <u>Control Enhancements:</u>

4098 SI-7 (14) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE

[BACK TO SCRM CONTROL]

- 4100 The organization:
- 4101 (a) Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and
- 41034104(b) Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.
- 4105 Supplemental Guidance: This control enhancement applies to all sources of binary or 4106 machine-executable code including, for example, commercial software/firmware and open 4107 source software. Organizations assess software products without accompanying source code 4108 from sources with limited or no warranty for potential security impacts. The assessments 4109 address the fact that these types of software products may be very difficult to review, repair, 4110 or extend, given that organizations, in most cases, do not have access to the original source 4111 code, and there may be no owners who could make such repairs on behalf of organizations. 4112 Related control: SA-5.
- 4113 SI-7 (15) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / CODE AUTHENTICATION

[BACK TO SCRM CONTROL]

The information system implements cryptographic mechanisms to authenticate [Assignment: organization-defined software or firmware components] prior to installation.

<u>Supplemental Guidance</u>: Cryptographic authentication includes, for example, verifying that software or firmware components have been digitally signed using certificates recognized and approved by organizations. Code signing is an effective method to protect against malicious code.

- 4123References:None.4124References:NIST Special Publications 800-147, 800-155.
- 4125 Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SI-7 (1) (7)	HIGH SI-7 (1) (2) (5) (7) (14)
----	------------------	------------------	--------------------------------

4126

4115

4116

4117

4118

4119

4120

4121

4122

4127 SI-12 INFORMATION HANDLING AND RETENTION

[Back to SCRM Control]

4128 4129 4130	<u>Control</u> : The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.					
4131 4132 4133 4134	Supplemental Guidance: Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The National Archives and Records Administration provides guidance on records retention. Related controls: AC-16, AU-5, AU-11, MP-2, MP-4.					
4135	Control Enhancements: None.					
4136	References: None.					
4137 4138	Priority and Baseline Allocation:					
	P2	LOW SI-12	MOD SI-12	HIGH SI-12		

 $\begin{array}{c} 4140\\ 4141 \end{array}$

4142 **FAMILY: PLANNING**

PL-1	SECUR	ITY PLANNING POLICY AND P	ROCEDURES	[Back to SCRM Control]
	Contro	<u>l</u> : The organization:		
	a. De rol	evelops, documents, and disse les]:	minates to [Assignment: organ	ization-defined personnel or
	1.	A security planning policy to management commitment, and	that addresses purpose, scope, r coordination among organizatio	oles, responsibilities, onal entities, and compliance;
	2.	Procedures to facilitate the security planning controls;	implementation of the security and	planning policy and associated
	b. Re	views and updates the current	t:	
	1.	Security planning policy [A	ssignment: organization-define	d frequency]; and
	2.	Security planning procedure	es [Assignment: organization-d	lefined frequency].
	Supple effectiv Policy policies level m be inclu be repr procedu system policy a	mental Guidance: This control ve implementation of selected and procedures reflect applica s, standards, and guidance. Se aay make the need for system- uded as part of the general inf esented by multiple policies r ures can be established for the s, if needed. The organization and procedures. Related control I Enhancements: None	ol addresses the establishment of security controls and control e able federal laws, Executive Or curity program policies and pro- specific policies and procedure formation security policy for or reflecting the complex nature of e security program in general ar all risk management strategy is rol: PM-9.	of policy and procedures for the nhancements in the PL family. ders, directives, regulations, ocedures at the organization as unnecessary. The policy can ganizations or conversely, can Certain organizations. The nd for particular information a key factor in establishing
	<u>Contro</u>	<u>I Enhancements:</u> None.		
	Priority	ces. NIST Special Publications o	500-12, 800-18, 800-100.	
	<u>i nonty a</u>	and Bascine Allocation.		
	P1 1	LOW PL-1	MOD PL-1	HIGH PL-1
PL-2	SYSTEM	A SECURITY PLAN		[Back to SCRM Control]
	<u>Control</u>	: The organization:		
	 a. Develops a security plan for the information system that: Is consistent with the organization's enterprise architecture; Explicitly defines the authorization boundary for the system; Describes the operational context of the information system in terms of missions and business processes; Provides the security categorization of the information system including supporting rationale; Describes the operational environment for the information system and relationships with or connections to other information systems; Provides an overview of the security requirements for the system; Identifies any relevant overlays, if applicable; Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and Is reviewed and approved by the authorizing official or designated representative prior to 			
	PL-1	PL-1SECURIControla.Derivea.Deriveb.Re1.2.b.b.Re1.2.b.Re1.2.b.Re1.2.SuppleeffectivePolicypolicie:level mbe includebe reprivationpolicy and controlReferenPriority and controla.Derive1.2.3.4.	PL-1 SECURITY PLANNING POLICY AND P Control: The organization: a. Develops, documents, and disservelos]: 1. A security planning policy management commitment, and 2. Procedures to facilitate the security planning controls; b. Reviews and updates the current 1. Security planning policy [A 2. Security planning procedure Supplemental Guidance: This control effective implementation of selected Policy and procedures reflect applica: policies, standards, and guidance. Selevel may make the need for systems be included as part of the general infibe represented by multiple policies r procedures can be established for the systems, if needed. The organization policy and procedures. Related control Control Enhancements: None. References: NIST Special Publications & Priority and Baseline Allocation: P1 P1 LOW PL-1 PL-2 SYSTEM SECURITY PLAN Control: The organization: a. Develops a security plan for the 1. Is consistent with the organization: 2. Describes the operational consumption of security categories and consumption of security categories and sec	PL-1 SECURITY PLANNING POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organ: roles]: 1. A security planning policy that addresses purpose, scope, r management commitment, coordination among organizatio and 2. Procedures to facilitate the implementation of the security security planning controls; and b. Reviews and updates the current: 1. Security planning procedures [Assignment: organization-define] 2. Security planning procedures [Assignment: organization-define] 3. Security planning procedures [Assignment: organization-define] 2. Security planning procedures [Assignment: organization-define] 3. Security planning procedures [Assignment: organization-define] 4. Supplemental Guidance: This control addresses the establishment of effective implementation of selected security controls and control e Policy and procedures reflect applicable federal laws, Executive Or policies, standards, and guidance. Security program policies and procedures to the general information security policy for or be represented by multiple policies reflecting the complex nature of procedures can be established for the security program in general at systems, if needed. The organizational risk management strategy is policy and procedures. Related control: PM-9. Control Enhancements: None. Priority and Baseline Allocation: Pl.2 SYSTEM SECURITY PLAN PL2

4186		b. Distributes copies of the security	plan and communicates subset	quent changes to the plan to
4187		[Assignment: organization-define	ed personnel or roles];	
4188		c. Reviews the security plan for the	information system [Assignme	ent: organization-defined
4189		frequency];		
4190		d. Updates the plan to address change	ges to the information system/e	environment of operation or
4191		problems identified during plan in	mplementation or security con	trol assessments; and
4192		e. Protects the security plan from ur	nauthorized disclosure and mod	diffication.
4193				
4194		Supplemental Guidance: Security pla	ans relate security requirements	s to a set of security controls
4195		and control enhancements. Security p	lans also describe, at a high lev	vel, how the security controls
4196		and control enhancements meet those	security requirements, but do	not provide detailed, technical
419/		descriptions of the specific design of	implementation of the controls	enhancements. Security plans
4198		contain sufficient information (includ	ing the specification of parame	eter values for assignment and
4199		selection statements either explicitly (or by reference) to enable a des	sign and implementation that is
4200		unamoiguousiy compilant with the ini	tent of the plans and subsequer	nt determinations of fisk to
4201		organizational operations and assets, I	individuals, other organization	s, and the Nation II the plan is
4202		hageling in Annendiv E and CNSS In	ons can also apply tanoling gui	relation for community wide use
4203		or to address specialized requirements	technologies or missions/on	vironments of operation (a g
4204		DoD tactical Federal Public Key Infr	astructure or Federal Identity	Credential and Access
4205		Management space operations) App	endix I provides guidance on d	eveloping overlays
4200		Wanagement, space operations). App	endix i provides guidance on d	eveloping overlays.
4207		Security plans need not be single docu	uments; the plans can be a coll	ection of various documents
4208		including documents that already exis	st. Effective security plans mak	e extensive use of references
4209		to policies, procedures, and additional	l documents (e.g., design and i	mplementation specifications)
4210		where more detailed information can	be obtained. This reduces the c	locumentation requirements
4211		associated with security programs and	maintains security-related inf	ormation in other established
4212		management/operational areas related	to enterprise architecture, syst	tem development life cycle,
4213		systems engineering, and acquisition.	For example, security plans do	o not contain detailed
4214		reference sufficient information to de	fina what needs to be second	lished by these plans. Pelated
4215		controls: AC_2 AC 6 AC-14 AC-17	A = 20 CA = 2 CA = 3 CA = 7 (CM = 0 CP-2 IR-8 MA-4
4210		MA-5 MP-2 MP-4 MP-5 PI -7 PM	, AC-20, CA-2, CA-5, CA-7, C	1 SA-5 SA-17
4218		Control Enhancements	, , , , , , , , , , , , , , , , , , ,	1, 011 0, 011 17.
4210		Contor Enhancements.		
4219	PL-2 (3)	SYSTEM SECURITY PLAN / PLAN / CO	ORDINATE WITH OTHER	
4220		ORGANIZATIONAL ENTITIES		[BACK TO SCRM CONTROL]
4221		The organization plans and coo	ordinates security-related act	ivities affecting the
4222		information system with [Assign	nment: organization-defined i	individuals or groups] before
4223		conducting such activities in or	der to reduce the impact on (other organizational entities.
4224		Supplemental Guidance: Securit	v-related activities include for	evample security
4225		assessments audits hardware and	d software maintenance natch	management and contingency
4226		plan testing Advance planning a	nd coordination includes emerge	gency and nonemergency (i e
4227		planned or nonurgent unplanned)	situations The process define	d by organizations to plan and
4228		coordinate security-related activity	ties can be included in security	plans for information systems
4229		or other documents, as appropriat	te. Related controls: CP-4, IR-4	4.
4230		References: NIST Special Publication 800)-18.	
4231		Priority and Pasoline Allocation:		
¬∠J1		Thomy and baseline Allocation.		
		P1 LOW PL-2	MOD PL-2 (3)	HIGH PL-2 (3)
4232				
1732	DI 0	NEADMANIA CEATINING A DATAMPA	PUDE	[Dools to SCDM Control]
4233	rl-ð	INFORMATION SECURITY ARCHITECT	UKE	DACK IN SCRIVE CONTROL

4234	Control: The organization:
4235	a. Develops an information security architecture for the information system that:
4236 4237	1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
4238 4239	2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
4240 4241	3. Describes any information security assumptions about, and dependencies on, external services;
4242 4243	b. Reviews and updates the information security architecture [<i>Assignment: organization-defined frequency</i>] to reflect updates in the enterprise architecture; and
4244 4245 4246	c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.
4247 4248 4249 4250 4251 4252 4253 4254 4255 4255 4256 4257 4258	<u>Supplemental Guidance</u> : This control addresses actions taken by organizations in the design and development of information systems. The information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture described in PM-7 that is integral to and developed as part of the enterprise architecture. The information security architecture includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security architecture can include other important security requirements, the types of information processed, stored, and transmitted by the information system, restoration priorities of information and information system services, and any other specific protection needs.
$\begin{array}{r} 4259\\ 4260\\ 4261\\ 4262\\ 4263\\ 4264\\ 4265\\ 4266\\ 4265\\ 4266\\ 4267\\ 4268\\ 4269\\ 4270\\ 4271\\ 4272\\ 4273\\ 4274\\ 4275\\ 4276\\ 4277\end{array}$	In today's modern architecture, it is becoming less common for organizations to control all information resources. There are going to be key dependencies on external information services and service providers. Describing such dependencies in the information security architecture is important to developing a comprehensive mission/business protection strategy. Establishing, developing, documenting, and maintaining under configuration control, a baseline configuration for organizational information systems is critical to implementing and maintaining an effective information security architecture. The development of the information security architecture is coordinated with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) to ensure that security controls needed to support privacy requirements are identified and effectively implemented. PL-8 is primarily directed at organizations (i.e., internally focused) to help ensure that organizations develop an information security architecture. In contrast, SA-17 is primarily directed at external information technology product/system developers and integrators (although SA-17 could be used internally within organizations for in-house system development). SA-17, which is complementary to PL-8, is selected when organizations outsource the development of information systems or information system components to external entities, and there is a need to demonstrate/show consistency with the organization's enterprise architecture and information security architecture. Related controls: CM-2, CM-6, PL-2, PM-7, SA-5, SA-17, Appendix J.
4278 4279 4280	Control Enhancements:

4281 PL-8 (2) INFORMATION SECURITY ARCHITECTURE / SUPPLIER DIVERSITY [BACK TO SCRM CONTROL]

- 4282 The organization requires that [Assignment: organization-defined security safeguards] 4283 allocated to [Assignment: organization-defined locations and architectural layers] are 4284 obtained from different suppliers. 4285 Supplemental Guidance: Different information technology products have different strengths 4286 and weaknesses. Providing a broad spectrum of products complements the individual 4287 offerings. For example, vendors offering malicious code protection typically update their 4288 products at different times, often developing solutions for known viruses, Trojans, or worms 4289 according to their priorities and development schedules. By having different products at 4290 different locations (e.g., server, boundary, desktop) there is an increased likelihood that at 4291 least one will detect the malicious code. Related control: SA-12.
- 4292 <u>References</u>: None.
- 4293 Priority and Baseline Allocation:

LOW Not Selected	MOD PL-8	HIGH PL-8
------------------	----------	-----------

4296 4297 4298	FAMIL	Y: PROGRAM MANAGEMENT	
4299	PM-1	INFORMATION SECURITY PROGRAM PLAN	[Back to SCRM Control]
4300		Control: The organization:	
4301		a. Develops and disseminates an organization-wide information security pro-	ogram plan that:
4302 4303 4304		 Provides an overview of the requirements for the security program a the security program management controls and common controls in meeting those requirements; 	nd a description of place or planned for
4305 4306		2. Includes the identification and assignment of roles, responsibilities, responsibilities, and complexity commitment, coordination among organizational entities, and complexity of the second	management liance;
4307 4308		 Reflects coordination among organizational entities responsible for t of information security (i.e., technical, physical, personnel, cyber-ph 	the different aspects sysical); and
4309 4310 4311		 Is approved by a senior official with responsibility and accountabilit incurred to organizational operations (including mission, functions, reputation), organizational assets, individuals, other organizations, a 	y for the risk being image, and nd the Nation;
4312 4313		b. Reviews the organization-wide information security program plan [Assig defined frequency];	nment: organization-
4314 4315		c. Updates the plan to address organizational changes and problems identified implementation or security control assessments; and	ied during plan
4316 4317		d. Protects the information security program plan from unauthorized disclosmodification.	sure and
4318 4319 4320 4321 4322 4323 4324 4325		<u>Supplemental Guidance</u> : Information security program plans can be represent documents or compilations of documents at the discretion of organizations. T the program management controls and organization-defined common controls security program plans provide sufficient information about the program man controls/common controls (including specification of parameters for any <i>assi</i> , statements either explicitly or by reference) to enable implementations that ar compliant with the intent of the plans and a determination of the risk to be into implemented as intended.	tted in single The plans document s. Information hagement gnment and selection re unambiguously curred if the plans are
4326 4327 4328 4329 4330 4331 4332 4333		The security plans for individual information systems and the organization-w security program plan together, provide complete coverage for all security co within the organization. Common controls are documented in an appendix to information security program plan unless the controls are included in a separa an information system (e.g., security controls employed as part of an intrusion providing organization-wide boundary protection inherited by one or more or information systems). The organization-wide information security program p which separate security plans contain descriptions of common controls.	ide information ntrols employed the organization's ate security plan for n detection system rganizational lan will indicate
4334 4335 4336 4337 4338 4339 4340 4341 4342 4343		Organizations have the flexibility to describe common controls in a single do documents. In the case of multiple documents, the documents describing comincluded as attachments to the information security program plan. If the infor program plan contains multiple documents, the organization specifies in each organizational official or officials responsible for the development, implement authorization, and monitoring of the respective common controls. For examplinary require that the Facilities Management Office develop, implement, assess continuously monitor common physical and environmental protection controls when such controls are not associated with a particular information system but multiple information systems. Related control: PM-8.	cument or in multiple mon controls are mation security a document the ntation, assessment, le, the organization as, authorize, and ls from the PE family at instead, support

4344		Control Enhancements: None.	
4345		References: None.	
4346	PM-2	SENIOR INFORMATION SECURITY OFFICER	[Back to SCRM Control]
4347 4348 4349 4350		<u>Control</u> : The organization appoints a senior information secures to coordinate, develop, implement, and maintain ar security program.	urity officer with the mission and n organization-wide information
4351 4352 4353 4354 4355		<u>Supplemental Guidance</u> : The security officer described in th For a federal agency (as defined in applicable federal laws, E or regulations) this official is the Senior Agency Information also refer to this official as the Senior Information Security C Officer.	is control is an organizational official. Executive Orders, directives, policies, Security Officer. Organizations may Officer or Chief Information Security
4356		Control Enhancements: None.	
4357		References: None.	
4358	PM-3	INFORMATION SECURITY RESOURCES	[Back to SCRM Control]
4359 4360		Control: The organization:	
4361 4362 4363		a. Ensures that all capital planning and investment requests implement the information security program and docume requirement;	s include the resources needed to ents all exceptions to this
4364		b. Employs a business case/Exhibit 300/Exhibit 53 to recor	d the resources required; and
4365		c. Ensures that information security resources are available	e for expenditure as planned.
4366 4367 4368 4369 4370		<u>Supplemental Guidance</u> : Organizations consider establishing efforts and as part of including the necessary resources, assig as needed. Organizations may designate and empower an Inv group) to manage and provide oversight for the information s planning and investment control process. Related controls: P	g champions for information security on specialized expertise and resources vestment Review Board (or similar security-related aspects of the capital M-4, SA-2.
4371		Control Enhancements: None.	
4372		References: NIST Special Publication 800-65.	
4373	PM-11	MISSION/BUSINESS PROCESS DEFINITION	[Back to SCRM Control]
4374 4375		Control: The organization:	
4376 4377 4378		a. Defines mission/business processes with consideration for resulting risk to organizational operations, organizationa organizations, and the Nation; and	or information security and the l assets, individuals, other
4379 4380		b. Determines information protection needs arising from th and revises the processes as necessary, until achievable r	e defined mission/business processes protection needs are obtained.
4381 4382 4383		<u>Supplemental Guidance</u> : Information protection needs are te capabilities to counter threats to organizations, individuals, o of information (i.e., loss of confidentiality, integrity, or available)	chnology-independent, required r the Nation through the compromise ability). Information protection needs

- 4384 are derived from the mission/business needs defined by the organization, the mission/business 4385 processes selected to meet the stated needs, and the organizational risk management strategy. 4386 Information protection needs determine the required security controls for the organization and the 4387 associated information systems supporting the mission/business processes. Inherent in defining an 4388 organization's information protection needs is an understanding of the level of adverse impact that 4389 could result if a compromise of information occurs. The security categorization process is used to 4390 make such potential impact determinations. Mission/business process definitions and associated 4391 information protection requirements are documented by the organization in accordance with 4392 organizational policy and procedure. Related controls: PM-7, PM-8, RA-2.
- 4393 <u>Control Enhancements:</u> None.
- 4394 <u>References</u>: FIPS Publication 199; NIST Special Publication 800-60.

4395 PM-16 THREAT AWARENESS PROGRAM

[Back to SCRM Control]

4396

4397Control: The organization implements a threat awareness program that includes a cross-
organization information-sharing capability.

4399 Supplemental Guidance: Because of the constantly changing and increasing sophistication of 4400 adversaries, especially the advanced persistent threat (APT), it is becoming more likely that 4401 adversaries may successfully breach or compromise organizational information systems. One of 4402 the best techniques to address this concern is for organizations to share threat information. This 4403 can include, for example, sharing threat events (i.e., tactics, techniques, and procedures) that 4404 organizations have experienced, mitigations that organizations have found are effective against 4405 certain types of threats, threat intelligence (i.e., indications and warnings about threats that are 4406 likely to occur). Threat information sharing may be bilateral (e.g., government-commercial 4407 cooperatives, government-government cooperatives), or multilateral (e.g., organizations taking 4408 part in threat-sharing consortia). Threat information may be highly sensitive requiring special 4409 agreements and protection, or less sensitive and freely shared. Related controls: PM-12, PM-16.

4410 <u>Control Enhancements:</u> None.

4411 <u>References</u>: None

1 APPENDIX F

2 ICT SUPPLY CHAIN THREAT EVENTS

threat analysis described in Chapter 2, if appropriate.

3

4 This appendix provides examples of ICT supply chain threat events. These examples are based on NIST 5 SP 800-30 Revision 1, Guide for Conducting Risk Assessments, Appendix E, Threat Events. Specifically, 6 Tables E-2, Representative Examples – Adversarial Threat Events, and E-3, Representative Examples – 7 *Non-Adversarial Threat Events*, were used to create the two corresponding tables in this document. It 8 should be noted that the threat events in NIST SP 800-30 Revision, 1 Appendix E, are generic threat 9 events that were tailored to information security rather than ICT SCRM context. The tables used as source 10 material for this appendix contain 2 columns – Threat Events and Description. 11 12 The generic threats in NIST SP 800-30 Revision 1, Appendix E, are at times quite broad and needed to be 13 further specified to be ICT supply chain-specific for use in this document. This document lists only those 14 threats events that are relevant to ICT supply chain in all or under some circumstances. To indicate when 15 the threat events are relevant only under some but not all circumstances, a comment is included in the 16 third column, Comments, to provide the rationale for when the specific threat event is relevant to ICT supply chain.

22

23

Threat Events (Characterized by TTPs)	Description	Comments
Perform	reconnaissance and gather information.	
Perform malware- directed internal reconnaissance.	Adversary uses malware installed inside the organizational perimeter to identify targets of opportunity. Because the scanning, probing, or observation does not cross the perimeter, it is not detected by externally placed intrusion detection systems.	
	Craft or create attack tools.	
Craft phishing attacks.	Adversary counterfeits communications from a legitimate/trustworthy source to acquire sensitive information such as usernames, passwords, or SSNs. Typical attacks occur via email, instant messaging, or comparable means, commonly directing users to websites that appear to be legitimate sites, while actually stealing the entered information.	
Craft attacks specifically based on deployed information technology environment.	Adversary develops attacks (e.g., crafts targeted malware) that take advantage of adversary knowledge of the organizational information technology environment.	

Table F-1: Adversarial ICT Supply Chain Threat Events

Organizations may use the examples of ICT supply chain threat events provided in this appendix during

Threat Events (Characterized by TTPs)	Description	Comments
Create counterfeit/spoof website.	Adversary creates duplicates of legitimate websites; when users visit a counterfeit site, the site can gather information or download malware.	
Craft counterfeit certificates.	Adversary counterfeits or compromises a certificate authority, so that malware or connections will appear legitimate.	
Create and operate false front organizations to inject malicious components into the supply chain.	Adversary creates false front organizations with the appearance of legitimate suppliers in the critical life cycle path that then inject corrupted/malicious information system components into the organizational supply chain.	
Deliv	er/insert/install malicious capabilities.	
Deliver known malware to internal organizational information systems (e.g., virus via email).	Adversary uses common delivery mechanisms (e.g., email) to install/insert known malware (e.g., malware whose existence is known) into organizational information systems.	
Deliver modified malware to internal organizational information systems.	Adversary uses more sophisticated delivery mechanisms than email (e.g., web traffic, instant messaging, FTP) to deliver malware and possibly modifications of known malware to gain access to internal organizational information systems.	
Deliver targeted malware for control of internal systems and exfiltration of data.	Adversary installs malware that is specifically designed to take control of internal organizational information systems, identify sensitive information, exfiltrate the information back to adversary, and conceal these actions.	
Deliver malware by providing removable media.	Adversary places removable media (e.g., flash drives) containing malware in locations external to organizational physical perimeters but where employees are likely to find the media (e.g., facilities parking lots, exhibits at conferences attended by employees) and use it on organizational information systems.	
Insert untargeted malware into downloadable software and/or into commercial information technology products.	Adversary corrupts or inserts malware into common freeware, shareware, or commercial information technology products. Adversary is not targeting specific organizations, simply looking for entry points into internal organizational information systems. Note that this is particularly a concern for mobile applications.	

Threat Events (Characterized by TTPs)	Description	Comments
Insert targeted malware into organizational information systems and information system components.	Adversary inserts malware into organizational information systems and information system components (e.g., commercial information technology products), specifically targeted to the hardware, software, and firmware used by organizations (based on knowledge gained via reconnaissance).	
Insert specialized malware into organizational information systems based on system configurations.	Adversary inserts specialized, non-detectable malware into organizational information systems based on system configurations, specifically targeting critical information system components based on reconnaissance and placement within organizational information systems.	
Insert counterfeit or tampered hardware into the supply chain.	Adversary intercepts hardware from legitimate suppliers. Adversary modifies the hardware or replaces it with faulty or otherwise modified hardware.	
Insert tampered critical components into organizational systems.	Adversary replaces, though supply chain, subverted insider, or some combination thereof, critical information system components with modified or corrupted components.	
Insert malicious scanning devices (e.g., wireless sniffers) inside facilities.	Adversary uses postal service or other commercial delivery services to deliver to organizational mailrooms a device that is able to scan wireless communications accessible from within the mailrooms and then wirelessly transmit information back to adversary.	
Insert subverted individuals into organizations.	Adversary places individuals within organizations who are willing and able to carry out actions to cause harm to organizational missions/business functions.	YES, if the individual is placed by an external party.
Insert subverted individuals into privileged positions in organizations.	Adversary places individuals in privileged positions within organizations that are willing and able to carry out actions to cause harm to organizational missions/business functions. Adversary may target privileged functions to gain access to sensitive information (e.g., user accounts, system files, etc.) and may leverage access to one privileged capability to get to another capability.	
	Exploit and compromise.	

Threat Events (Characterized by TTPs)	Description	Comments
Exploit split tunneling.	Adversary takes advantage of external organizational or personal information systems (e.g., laptop computers at remote locations) that are simultaneously connected securely to organizational information systems or networks and to nonsecure remote connections.	YES, if information systems are those belonging to external organization.
Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	Adversary launches attacks on organizations in a time and manner consistent with organizational needs to conduct mission/business operations.	YES, if the threat is to ICT supply chain.
Exploit insecure or incomplete data deletion in multi- tenant environment.	Adversary obtains unauthorized information due to insecure or incomplete data deletion in a multi-tenant environment (e.g., in a cloud computing environment).	
Violate isolation in multi-tenant environment.	Adversary circumvents or defeats isolation mechanisms in a multi-tenant environment (e.g., in a cloud computing environment) to observe, corrupt, or deny service to hosted services and information/data.	
Compromise information systems or devices used externally and reintroduced into the enterprise.	Adversary installs malware on information systems or devices while the systems/devices are external to organizations for purposes of subsequently infecting organizations when reconnected.	
Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware).	Adversary compromises the design, manufacture, and/or distribution of critical information system components at selected suppliers.	
Conduct an attac	k (i.e., direct/coordinate attack tools or activities).	
Conduct physical attacks on infrastructures supporting organizational facilities.	Adversary conducts a physical attack on one or more infrastructures supporting organizational facilities (e.g., breaks a water main, cuts a power line).	

Threat Events (Characterized by TTPs)	Description	Comments			
Conduct internally based session hijacking.	Adversary places an entity within organizations in order to gain access to organizational information systems or networks for the express purpose of taking control (hijacking) an already established, legitimate session either between organizations and external entities (e.g., users connecting from remote locations) or between two locations within internal networks.	YES, for critical systems.			
Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware.	nduct supply chain acks targeting and bloiting critical dware, software, or mware. Adversary targets and compromises the operation of software (e.g., through malware injections), firmware, and hardware that performs critical functions for organizations. This is largely accomplished as supply chain attacks on both commercial off-the-shelf and custom information systems and components				
Achieve results	(i.e., cause adverse impacts, obtain information)				
Cause unauthorized disclosure and/or unavailability by spilling sensitive information.	Adversary contaminates organizational information systems (including devices and networks) by causing them to handle information of a classification/sensitivity for which they have not been authorized. The information is exposed to individuals who are not authorized access to such information, and the information system, device, or network is unavailable while the spill is investigated and mitigated.	YES, because this may be related to information- sharing agreements.			
Obtain information by externally located interception of wireless network traffic.	Adversary intercepts organizational communications over wireless networks. Examples include targeting public wireless access or hotel networking connections, and drive-by subversion of home or organizational wireless routers.	YES, because this originates externally.			
Obtain unauthorized access.	Adversary with authorized access to organizational information systems, gains access to resources that exceeds authorization.	YES, if an adversary is not an employee.			
Obtain information by opportunistically stealing or scavenging information systems/components.	Adversary steals information systems or components (e.g., laptop computers or data storage media) that are left unattended outside of the physical perimeters of organizations, or scavenges discarded components.				
Maii	ntain a presence or set of capabilities.				
Coordinate campaigns across multiple organizations to acquire specific information or achieve desired outcome.	Adversary does not limit planning to the targeting of one organization. Adversary observes multiple organizations to acquire necessary information on targets of interest.	YES, if these are multiple organizations composing ICT supply chain.			

Threat Events (Characterized by TTPs)	Description	Comments
Coordinate cyber attacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors.	Adversary employs continuous, coordinated attacks, potentially using all three attack vectors for the purpose of impeding organizational operations.	

Table F-2: Non-Adversarial ICT Supply Chain Threat Events

Threat Event	Description	Comments
Spill sensitive information	Authorized user erroneously contaminates a device, information system, or network by placing on it or sending to it information of a classification/sensitivity, which it has not been authorized to handle. The information is exposed to access by unauthorized individuals, and as a result, the device, system, or network is unavailable while the spill is investigated and mitigated.	
Mishandling of critical and/or sensitive information by authorized users	Authorized privileged user inadvertently exposes critical/sensitive information.	YES, if user is not an employee.
Incorrect privilege settings	Authorized privileged user or administrator erroneously assigns a user exceptional privileges or sets privilege requirements on a resource too low.	YES, if user is not an employee.
Resource depletion	Degraded processing performance due to resource depletion.	YES, if physical resources are being depleted. YES, if resources of an external service provider are being depleted.
Introduction of vulnerabilities into software products	Due to inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into commonly used software products.	
Pervasive disk error	Multiple disk errors due to aging of a set of devices all acquired at the same time, from the same supplier.	

1 APPENDIX G

2 SUPPLY CHAIN THREAT SCENARIOS AND ANALYSIS 3 FRAMEWORK

4

13 14

15 16

17

18

19

20 21

22

23

5 ICT supply chain risk management is an organization process with a significant number of moving parts 6 that simultaneously and sequentially impact various systems and elements through both manual and 7 automated processes. Because the supply chain covers the entire life cycle of a system/element, there are 8 numerous opportunities for vulnerabilities that impact the environment or the system/element to be 9 intentionally or unintentionally inserted, created, or exploited. A Threat Scenario is a summary of 10 potential consequence(s) of the successful exploitation of a specific vulnerability or vulnerabilities 11 by a threat agent. Analyzing threat scenarios can help organizations determine the likelihood and impact 12 a specific event or events would have on an organization and identify appropriate mitigating strategies.

Threat scenarios are generally used in two ways:

- To translate the often disconnected information garnered from a risk assessment, such as described in NIST SP 800-30, into a more tangible, story-like situation for further evaluation. These stories can help organizations discover additional vulnerabilities requiring mitigation and used for training; and
- To determine the impact that the successful exercise of a specific vulnerability would have on the organization and identify the benefits of mitigating strategies.

Information garnered from these scenarios can be used to help identify areas requiring increased controls and also for training purposes. The Threat Scenario analysis may be conducted in conjunction with or as part of ongoing risk assessment processes. By performing an in-depth analysis of how a specific event will impact an organization using a threat scenario, critical relationships and dependencies that might otherwise be overlooked during an initial criticality analysis or risk assessment can become visible and appropriate mitigating strategies employed.

Because threat scenarios focus on specific, often hypothetical, events, they should not be used to replace a more traditional, holistic risk assessment. Rather, they should be used as a tool to further evaluate specific vulnerabilities or areas of concern. Due to the infinite number of possible scenarios and directions into which a threat scenario can evolve, it is important to have a structured approach with well-defined goals and scope.

- 37 This section provides an example of a generic threat scenario analysis framework for ICT SCRM that can
- 38 be used by organizations to develop a framework that best suits their needs. It also contains four examples
- 39 of how this framework may be used. The examples differ slightly in their implementation of the
- 40 framework so as to show how the framework may be tailored. Each example identifies one or more
- 41 vulnerabilities, describes a specific threat source, identifies the expected impact on the organization, and
- 42 proposes SP 800-161 SCRM controls that would help mitigate resulting risk.

DEVELOPING AND ANALYZING THREAT SCENARIOS & IDENTIFYING APPLICABLE CONTROLS

45 46

47

48

49

50

51

52

55

56

57

58

59

60

61

62

65

66

67 68

69

70

71

72

73

74

75

76

Step 1: Create a Plan for Developing and Analyzing Scenarios

- Identify the purpose of the threat scenario analysis in terms of the objectives, milestones, and expected deliverables;
- Identify the scope of organizational applicability, level of detail, and other constraints;
- Identify resources to be used, including personnel, time, and equipment; and
 - Define a framework to be used for analyzing scenarios.

53 Step 2: Characterize the Environment 54 Identify core mission/business

- Identify core mission/business processes and key organizational dependencies;
- Describe threat sources that are relevant to the organization. Include the motivation and resources available to the threat source, if applicable;
- List known vulnerabilities or areas of concern (Note: Examples of areas of concern include the planned outsourcing of a manufacturing plant, the pending termination of a maintenance contract, or the discontinued manufacture of an element.);
 - Identify existing and planned controls; and
 - Identify related regulations, standards, policies, and procedures.

63 Step 3: Develop and Select Threat Event(s) for Analysis 64 List possible ways threat sources could exploit kn

- List possible ways threat sources could exploit known vulnerabilities or impact areas of concern to create a list of events (Note: Historical data is useful in determine this information.);
- Briefly outline the series of consequences that could occur as a result of each threat event. These may be as broad or specific as necessary. If applicable, estimate the likelihood and impact of each event;
- Eliminate those events that are clearly outside the defined purpose and scope of the analysis;
- Describe in more detail the remaining threat events. Include the tactics, techniques, and procedures used to carry out attacks (Note: The level of detail in the description is dependent on the needs of the organization.); and
- Select for analysis those events that best fit the defined purpose and scope of the analysis. More likely events, events of special concern, and an event that can represent several of the other listed events are generally useful candidates.

77 Step 4: Conduct the Threat Scenario Analysis

- For each threat event, note any immediate consequences of the event and identify those organizational units and processes that would be affected, taking into account existing and planned controls, and applicable regulations, standards, policies, and procedures;
- Estimate the impact these consequences would have on the mission/business processes as well as the organizational units affected, preferably in quantitative terms from historical data and taking into account existing and planned controls, and applicable regulations, standards, policies and procedures (Note: It may be beneficial to identify a "most likely" impact level and a "worst-case" or "100-year" impact level.); and
- Identify those organizational units or processes that would be subsequently affected, the
 consequences and the impact levels, until each affected process has been analyzed, taking into
 account existing and planned controls, and applicable regulations, standards, policies and
 procedures (e.g., If a critical server goes down, one of the first processes affected may be the
 technology support department, but if they determine a new part is needed to bring the server
 backup, the procurement department may become involved.).

92	
93	Step 5: Determine Applicable Controls
94	• Determine the level of risk (impact and likelihood) that is acceptable to the organization for each
95	analyzed threat event (Note: In some cases, the level of acceptable risk may be dependent on the
96	cost of mitigating strategies.);
97	• Compare the level of acceptable risk to the existing level of risk as determined by the threat
98	scenario analysis;
99	 Identify potential mitigating controls (Note: Using a list of standard or recommended controls
100	such as those found in NIST SP 800-53 can make this process simpler.). Furthermore, factoring
101	any available FedRAMP certifications for the organization and any other applicable recognized
102	external assessments for system integrators, suppliers, and external service providers, as
103	recommended by SCRM_CA-2 (2), in the mitigating control identification process may eliminate
104	duplicate resources without compromising the effectiveness of the resultant mitigation.);
105	• Estimate the effectiveness of those controls at reducing the risk of a scenario;
106	• Estimate the resources needed (in terms of money, personnel, time) to implement potential
10/	controls; and
108	• Identify those controls or combinations of controls that would cause the estimated residual risk of
109	a threat event to drop to an acceptable level in the most resource-effective manner, taking into
110	account any rules or regulations that may apply (Note: Consideration should be given to the
111	potential that one control will help initigate the fisk from more than one event, of that a control may increase the risk of a separate event.)
112	may increase the risk of a separate event.).
11 <i>3</i> 11 <i>4</i>	Sten 6. Fyaluate / Feedback
115	• Develop a plan to implement the selected controls and evaluate their effectiveness: and
116	 Evaluate the effectiveness of the threat scenario analysis and make improvements as needed
117	• Evaluate the effectiveness of the threat scenario analysis and make improvements as needed.

- 119
- 120 121

Figure G-1: Sample Threat Scenario Analysis Framework

	Threat Source	
ario	Vulnerability	
cena	Threat Event	
at S	Description	
Threa	Outcome	
Orga	nizational units /	
proc	esses affected	
	Impact	
	Likelihood	
	Risk Score	
	(Impact x	
	Likelihood)	
×	Acceptable	
Ris	Level of Risk	
	Potential	
	Mitigating	
	Strategies /	
	SCRM Controls	
	Estimated Cost	
	of Mitigating	
	Strategies	
	Change in	
	Likelihood	
	Change in	
	Impact	
	Selected	
itior	Strategies	
tiga	Estimated	
Ĭ	Residual Risk	

122

123 SAMPLE SCENARIOS

124

This section provides four example threat scenarios specific to the U.S. government using the generic framework described above. The examples purposely vary in level of specificity and detail to show that threat scenarios can be as broad or specific, as detailed or generic, as necessary. While these scenarios use basic scoring measures (High, Moderate, Low) for likelihood, impact, and risk, organizations may use any of a number of different units of measure (e.g., percentage, CVSS score, etc.). Additionally, these scenarios vary slightly in implementation of the framework to show that the framework can be adapted as needed.

133 SCENARIO 1: Telco Counterfeits

134

135 **Background**:

136

137 A large organization has developed a system that is maintained through contract by an external

- 138 integration company. The system requires a common telecommunications element that is no longer
- 139 available from the Original Equipment Manufacturer (OEM). The OEM has offered a newer product as a 140 replacement, but it would require modifications to the system at a cost of approximately \$1 million. If the
- 141 element is not upgraded, the agency and system integrator would have to rely on secondary market
- 142 suppliers for replacements. The newer product provides no significant improvement on the element
- 143 currently being used.
- 144

145 The organization has decided to perform a threat scenario analysis to determine whether to modify the 146 system to accept the new product, or accept the risk of continuing to use a product that is no longer in 147 production.

148

152

153

154

155

156

149 Environment

- 150 151 The environment is characterized as follows:
 - The system is expected to last ten more years without any major upgrades/modifications and has a 99.9% uptime requirement.
 - Over 1,000 of the \$200 elements are used throughout the system and approximately 10% are replaced every year due to regular wear-and-tear, malfunctions, or other reasons. The integrator has approximately a three-month supply on hand at any time.
- 157 • The element is continuously monitored for functionality, and efficient procedures exist to reroute 158 traffic and replace the element should it unexpectedly fail.
- 159 • Outages resulting from unexpected failure of the element are rare, localized, and last only a few 160 minutes. More frequently, when an element fails, the system's functionality is severely reduced 161 for approximately one-to four-hours while the problem is diagnosed and fixed or the element 162 replaced. 163
 - Products such as the element in question have been a common target for counterfeiting.
 - The integrator has policies restricting the purchase of counterfeit goods and a procedure to follow if a counterfeit is discovered [Ref. SCRM SA-16].
 - The integrator and acquiring agency have limited testing procedures to ensure functionality of the • element before acceptance [Ref. SCRM SA-10 (4)].

169 **Threat Event**

170

164

165

166

167 168

171 To support the threat scenario, the agency created a fictitious threat source described as a group motivated 172

- by profit with vast experience creating counterfeit solutions. The counterfeiter is able to make a high 173 profit margin by creating and selling as genuine, products that are visually identical to their genuine
- 174 counterparts but which use lower-quality materials. They have the resources to copy most trademark and
- 175 other identifying characteristics and insert counterfeits into a supply chain commonly used by the
- 176 organization with little to no risk of detection. The counterfeit product is appealing to unaware purchasing
- 177 authorities as it is generally offered at a discount - sold as excess inventory or as stockpile.
- 178
- 179 If an inferior quality element was inserted into the system, it would likely fail more often than expected,
- 180 causing reduced functionality of the system. In the event a large number of counterfeit products were
- 181 mixed in with genuine parts and integrated into the system randomly, the number and severity of
- 182 unexpected outages could grow significantly. The agency and integrator decided that the chances a

- 183 counterfeit product could be purchased to maintain the system and the estimated potential impact of such 184 an event were high enough to warrant further evaluation.
- 185

186 Threat Scenario Analysis

187

188 The person(s) purchasing the element from a supplier will be the first affected by a counterfeit product.

189 Policy dictates that they attempt to purchase a genuine product from vetted suppliers. This person will

190 have to be led to believe that the product is genuine. As the counterfeit product in question is visually

- identical to the element desired, and at a discount, there is a high chance the counterfeit will be purchased.One will be tested to ensure functionality, and then the items will be placed into storage.
- 192 193

When one of the elements in the system needs to be replaced, an engineer will install a counterfeit, quickly test to ensure it is running properly, and record the change. It could take two years for the

195 quickly test to ensure it is fullning property, and record the change. It could take two years for the 196 counterfeit product to fail, so up to 200 counterfeit elements could be inserted into the system before the

- first one fails. If all the regularly replaced elements are substituted for counterfeits and each counterfeit
- fails after two years, the cost of the system would increase by \$160,000 in ten years. The maintenance
- time required would also cost the integration company in personnel and other expenses.
- 200

When a counterfeit fails, it will take approximately one-to four hours to diagnose and replace the element.
During this time, productivity is severely reduced. If more than one of the elements fails at the same time,
the system could fail. This could cause significant damage to agency operations and violate the 99.9%
uptime requirements set forth in the contract. Plus, if it is determined that the element failed because it

was a counterfeit, there would be additional costs associated with reporting the counterfeit.

206

209

210 211

212

213

214

215

216

217

218

221

222

223

224

225

226

227

207 *Mitigation Strategy:*208

The following were identified as potential mitigating activities (from NIST SP 800-161):

- Require developers to perform security testing/evaluation at all post-design phases of the SDLC [SCRM_SA-9];
- Validate that the information system or system component received is genuine and has not been altered [SCRM_SA-10 (7)];
- Incorporate security requirements into the design of information systems (defensive design) [SCRM_PL-3, SCRM_SC-13]; and
- Employ supplier diversity requirements [SCRM_PL-3(1)].

Based on these controls, the agency was able to devise a strategy that would include:

- Acceptance testing: Examination of elements to ensure that they are new, genuine, and that all associated licenses are valid. Testing methods include, where appropriate: physical inspection by trained personnel using digital imaging, digital signature verification, serial/part number verification, and sample electrical testing;
- Increase security requirements into the design of the system by adding redundant elements along more critical paths (as determined by a criticality analysis) in order to minimize the impact of an element failure; and
- 228 229
- Search for alternative vetted suppliers/trusted components.

It was determined that this strategy would cost less than accepting the risk of allowing counterfeits into the system or modifying the system to accept the upgraded element. The estimated cost for implementing

- 232 233 234 a more rigorous acquisition and testing program was \$80,000; the cost for increasing defensive design requirements was \$100,000.

- 235

	Threat Source:	Counterfeit telecommunications element introduced into supply chain.					
enario	Vulnerability:	Element no longer produc Purchasing authorities un genuine elements.	Element no longer produced by OEM. Purchasing authorities unable / unwilling to identify and purchase only genuine elements.				
Threat Sc	Threat Event Description:	Threat agent inserts their counterfeit element into a trusted distribution chain. \rightarrow Purchasing authorities buy the counterfeit element. \rightarrow Counterfeit elements installed into the system.					
	Outcome: The element fails more frequently than before, increasing the numb outages.						
Organizational units /		Acquisitions Maintenance					
		Mission-essential function	IS				
	Impact:	High - Outages increase by 80%	Medium increase	– Outages by 40%	Low – outages increase by 10%		
	Likelihood:	15%	40%		45%		
Risk	Risk Score (Impact x Likelihood):	High					
	Acceptable Level of Risk:	Low					
	Potential Mitigating Strategies / SCRM Controls:	Increase acceptance testir capabilities [SCRM_SA-9; SCRM_SA-10 (7)], increase security requirements in d systems [SCRM_PL-3, SCRI 13], and employ supplier of requirements [SCRM_PL-3	esign of M_SC- liversity (1)].	Modify the sys upgrade.	tem to accept element		
gation	Estimated Cost of Mitigating Strategies:	\$180,000		\$1million			
Miti	Change in Likelihood:	Low		Large			
	Change in Impact:	Moderate		None			
	Selected Strategies:	Agency-level examination and testing. Place elements in escrow until they pass defined acceptance testing criteria Increase the defensive design.					
	Estimated Residual Risk:	Low					

237 SCENARIO 2: Industrial Espionage.

238

239 **Background**: 240

241 Harlow Inc., a semiconductor (SC) company used by the organization to produce military and aerospace 242 systems, is considering a partnership with a KXY Co. to leverage their fabrication facility. This would 243 represent a significant change in the supply chain related to a critical system element. A committee was 244 formed including representatives from the organization, Harlow Inc., and the integration company to help 245 identify the impact that the partnership would have on the organization and risk-appropriate mitigating 246 practices to enact when the partnership is completed.

247

248 **Environment:** 249

250 The systems of concern are vital to the safety of military and aerospace missions. While not classified, the

251 element that KXY would be expected to manufacture is unique, patented, and critical to the operational

252 status of the systems. Loss of availability of the element while the system is operational could have

253 significant, immediate impact across multiple agencies and the civilian populous, including loss of life 254 and millions of dollars in damages. An initial Risk Assessment was accomplished using NIST SP 800-30

255 and the existing level of risk for this is was given a score of "Moderate."

256

257 KXY currently produces a state-of-the-art, low-cost wafer fabrication whose focus is primarily

258 commercial. The nation-state in which KXY operates has a history of conducting industrial espionage to 259 gain IP / technology. They have shown interest in semiconductor technology and provided a significant

grant to KXY to expand into the military and aerospace markets. While KXY does not currently have the

260 261 testing infrastructure to meet U.S. industry compliance requirements, the nation-state's resources are 262 significant, including the ability to provide both concessions as well as incentives to help KXY meet

- 263 those requirements.
- 264

265 The key area of concern was that the nation-state in which KXY operates would be able to use its 266 influence to gain access to the element or the element's design.

267

268 The committee reviewed current mitigation strategies in place and determined that Harlow, Inc., the 269 integration company, and the organization had several existing practices to ensure that the system and all 270 critical elements, as determined by a criticality analysis, met specific functionality requirements. For 271 example, the system and critical elements are determined compliant with relevant industry standards. As 272 part of their requirements under NIST SP 800-53 rev. 4, the agency had some information protection 273 requirements (ref. SCRM PM-4). In addition, Harlow, Inc. had a sophisticated inventory tracking system 274 that required that most elements be uniquely tagged using RFID technology or otherwise identified for traceability (ref. SCRM SA-10 (11)).

- 275
- 276 277

278 Threat Scenario:

279

280 Based on past experience, the organization decided that KXY's host nation would likely perform one of

281 two actions if given access to the technology: sell it to interested parties or insert / identify vulnerabilities

282 for later exploitation. For either of these threat events to be successful, the host nation would have to

understand the purpose of the element and be given significant access to the element or element's design. 283

284 This could be done with cooperation of KXY's human resources department, through deception, or by

285 physical or electronic theft. Physical theft would be difficult given existing physical control requirements 286 and inventory control procedures. For a modified element to be purchased and integrated with the system,

287 it would need to pass various testing procedures at both the integrator and agency levels. Testing methods

288 currently implemented include radiographic examination, material analysis, electrical testing, and sample

289 accelerated life testing. Modifications to identification labels/schemes would need to be undetectable in a

290 basic examination. In addition, KXY would need to pass routine audits, which would check KXY's processes for ensuring the quality and functionality of the element.

291 292

293 The committee decided that, despite existing practices, there was a 30% chance that the host nation would 294 have the motivation and ability to develop harmful modifications to the element without detection, exploit 295 previously unknown vulnerabilities, or provide the means for one of their allies to do the same. This could 296 result in a loss of availability or integrity of the system, causing significant harm. Using information from 297 an initial Risk Assessment accomplished using NIST SP 800-30, the committee identified this as the 298 worst-case scenario with an impact score of "High."

299

300 There is approximately a 40% chance that the host nation could and would sell the technology to

301 interested parties, resulting in a loss of technological superiority. If this scenario occurred, friendly

- 302 military and civilian lives could be at risk, intelligence operations would be damaged, and more money
- 303 would be required to invest in a new solution. The committee assigned an impact score for this scenario 304 of "Moderate."
- 305 306 The committee determined that the overall combined risk score for the vulnerability of concern was 307 "High."
- 308

309 Mitigating strategies:

310 311

312 Using NIST SP 800-161 as a base, three broad strategies were identified by the committee: (1) improve 313 traceability capabilities, (2) increase provenance and information requirements, and (3) choose another

314 supplier. These three options were analyzed in more detail to determine specific implementation

315 strategies, their impact on the scenarios and their estimated cost to implement. (Specific technologies and 316 techniques are not described in this case, but would be useful in an actual threat scenario evaluation.)

317

320

321

324

- 318 Improve traceability and monitoring capabilities. 319
 - SCRM CM-8 INFORMATION SYSTEM COMPONENT INVENTORY
 - SCRM IA-1 IDENTIFICATION AND AUTHENCITCATION POLICY AND PROCEDURES
- SCRM SA-8 (1) DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE / 322 FIRMWARE INTEGRITY VERIFICATION 323
 - SCRM SA-8 (3) DEVELOPER CONFIGURATION MANAGEMENT | HARDWARE INTEGRITY VERIFICATION
- SCRM_SA-10 (7) SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT 325 326 ALTERED
- 327 • SCRM SA-10 (11) - SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY
- 328 Cost = 20% increase
- 329 Impact = 10% decrease
- 330

- 331 Increase provenance and information control requirements.
- 332 SCRM AC-11 - COLLABORATION AND INFORMATION SHARING • 333
 - SCRM PV-1 PROVENANCE POLICY AND PROCEDURES •
 - SCRM PV-2 - BASELINING AND TRACKING PROVENANCE
- 335 Cost = 20% increase

336	Impact = 20% decrease
337	•
338	Choose another supplier.
339	 SCRM_SA-10 (2) - SUPPLY CHAIN PROTECTION SUPPLIER REVIEWS
340	Cost = 40% increase
341	Impact = 80% decrease
342	
343	Based on this analysis, the committee decided to implement a combination of practices:
344	• Develop and require unique, difficult-to-copy labels or alter labels to discourage cloning or
345	modification of the component. [Ref. SCRM_SA-10 (3)]
346	• Minimize the amount of information that is shared to suppliers. Require that the information be
347	secured. [Ref. SCRM AC-11]
348	• Require provenance be kept and updated throughout the SDLC. [Ref. SCRM PV-1]
349	
350	With this combination of controls, the estimated residual risk was determined to be equivalent with the
351	existing risk without the partnership at a cost increase that is less than if the organization changed
352	suppliers.
353	

	steal IP						
	Vulnerability:	Supplier considering part threat source.	tnership	with company t	hat has relationship with		
scenario	Threat Event Description:	Nation-state helps KXY meet industry compliance requirements. Harlow, Inc. partners with KXY to develop chips.					
	Existing Practices:	Strong contractual requirements as to the functionality of the system and elements Comprehensive inventory tracking system at Harlow, Inc. Industry compliance requirements					
Threat	Outcome:	Nation-state extracts tec exploits previously unkno	hnology own vulr	threat actor mo nerability	odifies technology or		
Organ	izational units / sses affected:	KXY Supplier Harlow, Inc. / integrator Technology users Other federal agencies /	KXY Supplier Harlow, Inc. / integrator functionality testing Technology users Other federal agencies / customers				
	Impact:	Technology modified / vulnerabilities exploited	– High	Technology so Moderate	d to interested parties -		
	Likelihood:	Moderate		Moderate			
	Risk Score (Impact x Likelihood):	High					
Risk	Acceptable Level of Risk:	Moderate					
	Potential Mitigating Strategies / SCRM Controls:	(1) Improve traceability and monitoring capabilities	(2) Increase provenance and information control requirements		(3) choose another supplier		
	Estimated Cost of Mitigating Strategies:	20% increase	20% increase		40% increase		
	New Risk Score:	Moderate	Moder	ate	Moderate		
	Selected Strategies:	Develop and require unique, difficult-to-copy labels or alter labels to discourage cloning or modification of the component. [SCRM_SA-10 (3)] Minimize the amount of information that is shared to suppliers. Require that the information be secured. [SCRM AC-11] Require provenance be kept and updated throughout the SDLC. [SCRM_PV-1]					
Mitigatid	Estimated Residual Risk:	Moderate - The residual risk was determined to be equivalent with the existing risk without the partnership.					

355 SCENARIO 3: Malicious Code Insertion

356

357 *Background:* 358

An organization has decided to perform a threat scenario analysis on a traffic control system. The
 scenario is to focus on software vulnerabilities and should provide general recommendations regarding
 mitigating practices.

- 362363 *Environment:*
- 364

The system runs nearly automatically and uses computers running a commonly available operating system along with centralized servers. The software was created in-house and is regularly maintained and updated by an integration company on contract for the next five years. The integration company is large, frequently used by the organization in a variety of projects, and has significant resources to ensure that the system maintains its high availability and integrity requirements.

370

Threats to the system could include: loss of power to the system, loss of functionality, or loss of integrity causing incorrect commands to be processed. Some threat sources could include nature, malicious

373 outsiders, and malicious insiders. The system is equipped with certain safety controls such as back-up

374 generator power, redundancy of design, and contingency plans if the system fails.

375

376 Threat Event:

377

The organization decided that the most concerning threat event would be if a malicious insider were to compromise the integrity of the system. Possible attacks were that the threat actor could insert a worm or a virus into the system, reducing its ability to function, or they could manually control the system from one of the central servers or by creating a back-door in the server to be accessed remotely. Depending on the skillfulness of the attack, an insider could gain control of the system, override certain fail-safes, and cause significant damage.

384

387

388

389

390

391

392

393

398

Based on this information, the organization developed the following fictitious threat event to be analyzed: 386

John Poindexter, a disgruntled employee of the integration company, decides to insert some open source malware into a component of the system. He then resigns from the firm, leaving no traceability of his work. The malware has the ability to call home to John and provides him access to stop or allow network traffic at any or all 50 of the transportation stations. As a result, there would be unpredictable, difficult-to-diagnose disruptions, causing significant monetary losses and safety concerns.

After a Risk Assessment was accomplished using NIST SP 800-30, management has decided that the
 acceptable level of risk for this scenario is "Moderate."

397 Threat Scenario Analysis:

399 If John were successful, a potential course of events would be as follows: 400

401John conducts a trial run – shutting off the services of one station for a short time. It would be402discounted as a fluke and have minimal impact. Later, John would create increasingly frequent403disruptions at various stations. These disruptions would cause anger among employees and404customers and some safety concerns. The integration company would be made aware of problem

405 and begin to investigate the cause. They would create a work-around, assuming there was a bug 406 in the system. However, because the malicious code would be buried and difficult to identify, the 407 integration company wouldn't discover it. John would then create a major disruption across 408 several transportation systems at once. The work-around created by the integration company 409 would fail due to the size of the attack, and all transportation services would be halted. Travelers 410 would be severely impacted, and the media alerted. The method of attack would be identified and 411 the system modified to prevent John from accessing the system again. However, the underlying 412 malicious code would remain. Revenue would decrease significantly for several months. Legal 413 questions would be raised. Resources would be invested in ensuring the public that the system 414 was safe. 415

416 *Mitigating Practices:*

417

419 420

421

424

425

426

418 The organization identified the following as potential areas for improvement:

- Establish and retain identification of supply chain elements, processes, and actors SCRM_SA-10 (11);
- Control access and configuration changes within the SDLC and require periodic code reviews SCRM AC-1, SCRM AC-2, SCRM CM-3;
 - Require static code testing SCRM SA-11 (1); and
 - Incident Response Handling SCRM_IR-2.

427 428

	Threat Source:	Integrator– Malicious Code Insertion
t Scenario	Vulnerability:	Minimal oversight of integrator activities - no checks and balances for any individual inserting a small piece of code.
	Threat Event Description:	Disgruntled employee of an Integrator company inserts malicious functionality into traffic navigation software, and then leaves the company.
Threa	Existing Practices:	Integrator: peer-review process Acquirer: Contract that sets down time, cost, and functionality requirements
	Outcome:	50 large metro locations and 500 instances affected by malware. When activated, the malware causes major disruptions to traffic.
Organizational units / processes affected:		Traffic Navigation System Implementation company Legal Public Affairs
	Impact:	High – Traffic disruptions are major and last for two weeks while a work- around is created. Malicious code is not discovered and remains a vulnerability.
k	Likelihood:	High
Ris	Risk Score (Impact x Likelihood):	High
	Acceptable Level of Risk:	Moderate
	Potential Mitigating Strategies / SCRM Controls:	SCRM_AC-1; SCRM_AC-2; SCRM_CM-3; SCRM_IR-2; SCRM_SA-10(11); SCRM_SA-11(1)
on	Estimated Cost of Mitigating Strategies:	\$2.5Mil
Aitigati	Change in Impact:	Large
2	Change in Likelihood:	Large
	Selected Strategies:	Combination of strategies using the mitigation noted
	Estimated Residual Risk:	Moderate

432 SCENARIO 4: Unintentional Compromise

433

434 **Background**: 435

436 Uninformed insiders replace components with more cost-efficient solutions without understanding the 437 implications to performance, safety, and long-term costs.

438

439 An organization has concerns about its acquisition policies and has decided to conduct a threat scenario 440 analysis to identify applicable mitigating practices. Any practices selected must be applicable to a variety 441 of projects and have significant success within a year.

443 Environment:

444

442

445 The agency acquires many different systems with varying degrees of requirements. Because of the 446 complexity of the environment, agency officials decided that they should use a scenario based on an actual past event.

447

448 449

- **Threat Event:** 450
- 451

Using an actual event as a basis, the agency designed the following threat event narrative: 452

453 Gill, a newly hired program manager, is tasked with reducing the cost of a \$5 million system 454 being purchased to support complex research applications in a unique physical environment. The 455 system would be responsible for relaying information regarding temperature, humidity, and toxic 456 chemical detection as well as for storing and analyzing various data sets. There must not be any 457 unscheduled outages more than 10 seconds long or there will be serious safety concerns and 458 potential destruction of research. The agency's threat assessment committee determined that the 459 acceptable level of risk for this type of event has a score of 2/10. 460

461 Gill sees that a number of components in the system design are priced high compared with similar 462 components he has purchased in the commercial acquisition space. Gill asks John, a junior 463 engineer with the integration company, to replace several load balancer / routers in the system 464 design to save costs.

466 **Threat Scenario Analysis:**

468 The agency decided that there were three potential outcomes to the scenario:

- 469 1. It is determined that the modifications are inadequate before any are purchased (30% chance, no 470 impact); 471
 - 2. It is determined that the modifications are inadequate during testing (40% chance, low impact); or
 - 3. The inadequacy of the modifications is undetected, the routers are installed in the system, begin to fail, and create denial of service incidents (30% chance, high impact).

474 475

472

473

465

467

476 Mitigating strategies: 477

478 Three potential mitigating strategies were identified:

- 479 Improve the existing training program (Ref. SCRM AT-1) and add configuration management 480 controls to monitor all proposed changes to critical systems. (Ref. SCRM CM-1);
- 481 Improve the testing requirements (Ref. SCRM SA-9); and •

- 482 Require redundancy and heterogeneity in the design of systems (Ref. SCRM SC-13, SCRM SC-• 483 10).
- 485 Adding configuration management controls would increase the likelihood that the modifications are 486 rejected either at the initial stage or during testing, but it was determined that a \$200,000 investment in 487 training alone could not bring the level of risk to an acceptable level in the time required.
- 488 489 Improving the testing requirements would increase the likelihood that the modifications are rejected
- 490 during testing, but it was determined that no amount of testing alone could bring the level of risk to an 491 acceptable level.
- 492 493 Requiring redundancy and heterogeneity in the design of the system would significantly reduce the 494 impact of this and other events of concern, but could double the cost of a project. In this scenario, it was 495 determined that an investment of \$2 million would be required to bring the risk to an acceptable level.

484

- 497 As a result of this analysis, the agency decided to implement a combination of practices:
- 498 A mandatory, day-long training program for those handling the acquisition of critical systems and 499 adding configuration management controls requiring changes be approved by a configuration 500 management board (CMB) (\$80,000 initial investment); 501
 - \$60,000 investment in testing equipment and software for critical systems and elements; and •
 - Redundancy and diversity of design requirements as deemed appropriate for each project. •
- 504 It was determined that this combination provided a series of practices that would be most cost-effective 505 for a variety of projects and would also help mitigate the risk from a variety of threats.
- 506 507

502

503

PAGE G-17

	Threat Source:	Internal	Employee	e – Unint	entional	Compro	mise			
Threat Scenario	Vulnerability:	Lax trair	ning pract	ices						
	Threat Event Description:	A new acquisition officer (AO) with experience in commercial acquisition is tasked with reducing hardware costs. The AO sees that a number of components are priced high and works with an engineer to change the purchase order.								
	Existing Practices:	Minima Basic te	l training sting requ	orogram irements	that is n s for syst	ot consid em comp	lered man ponents	datory		
	Outcome:	Change is found unsuitable before purchase Char			nge is found uitable in testing Change p installed a denial c			basses testing, routers and start to fail, causing of service situation.		
Org p	anizational units / rocesses affected:	nits / None Acquisitions Acquisitions, System						em, User	ſS	
	Impact:	None		Low			High			
	Likelihood:	30%		30%			40%			
Risk	Risk Score (Impact x Likelihood):	High								
	Acceptable Level of Risk:	Low								
	Potential Mitigating Strategies / SCRM Controls:	Improve training program and require changes be approved by CMB.			Improve acquisition testing			Improve design of system		
	Estimated Cost of Mitigating Strategies:	\$200,000						\$2 million		
tion	Change in Impact:	None			None		Significant		ant	
Mitiga	Change in Likelihood:	+10%	+10%	-20%	0	+20%	-20%	0	0	0
	New Risk Score:	4/10								
	Selected Strategies:	Make tr require board. ((aining pro changes to Cost = \$10	ogram ma o critical 00,000)	andatory systems	for thos be appro	e working ved by a c	on critica onfigurat	al system ion mana	s and agement
	Residual Risk:	Low								
1 APPENDIX H

2 ICT SCRM PLAN TEMPLATE

The following template is an example of the sections and the type of information that the federal agency should include in their ICT SCRM Plans. Guidance for specific Tiers is provided, where applicable.

Agencies should have at least one ICT SCRM Plan. Depending on their governance structure and size,
agencies can have multiple ICT SCRM Plans, one for Tier 1, several for Tier 2, and several for Tier 3.²²
Regardless of the total number of plans, the ICT SCRM requirements and controls at the higher tiers will
flow down to the lower tiers and should be used to guide the development of the lower tier ICT SCRM
Plans. Conversely, the ICT SCRM controls and requirements at the lower tiers should be considered in
developing and revising requirements and controls applied at the higher tiers.

13

3 4

5

- 14 ICT SCRM controls in the ICT SCRM Plan can be applied in different life cycle processes, for example,
- 15 the incident response (IR) control can be applied in both Infrastructure Management life cycle process
- 16 and Operations life cycle process. Figure H-2 lists ISO/IEC 15288 life cycle processes.
- 17

r

Agreement Process	Project Process	Technical Process
Acquisition	Project Planning	Stakeholder Requirements
Supply	Project Assessment and Control	Definition Requirements Analysis
	Decision Management	Requirements Analysis
Organizational Project-	Diele Management	Architectural Design
Enabling Processes	Risk Management	Implementation
Life Cycle Model Management	Configuration Management	Integration
Infrastructure Management	Information Management	Verification
Project Portfolio Management	Measurement	Vermeation
		Transition
Human Resource Management		Validation
Quality Management		
		Operation

Figure H-1: ISO/IEC 15288 Life Cycle Processes

When addressing security concerns within an ICT SCRM Plan, agencies may choose to integrate their
 Tier 3 ICT SCRM controls into the applicable System Security Plans or create individual ICT SCRM
 Plans for Tier 3 that reference corresponding System Security Plans.

Plans for Tier 3 that reference corresponding System Security Plans.

²² Description of Tiers is provided in Section 2.

25 ICT SCRM Plans should cover the full life cycle of ICT systems and programs, including research and

- 26 development, design, manufacturing, acquisition, delivery, integration, operations, and
- 27 disposal/retirement. The ICT SCRM Plan activities should be integrated into the organization's system
- 28 and software life cycle processes to ensure that ICT SCRM activities are integrated into those processes.
- 29 Figure H-2 shows how the ICT SCRM plan activities can be integrated into various example life cycles.
- 30



31 32 33 34 35

Figure H-2: ICT SCRM Plan and Life Cycles

These ICT SCRM Plans should include as attachments relevant agreements provided by system integrators, suppliers, and external service providers as part of the contracting process.²³ It is expected

36 that these agreements will be mostly attached at Tier 3 ICT SCRM Plans, but they may also be attached to

37 Tier 1 and Tier 2 ICT SCRM Plans for acquisitions that span multiple systems. Review and update ICT

38 SCRM Plans on a schedule that includes life cycle milestones or gate reviews and significant²⁴

39 contracting activities.

²³ Such agreements, which also can be referred to as supplier ICT SCRM Plans, may describe details of risk management activities performed on behalf of the end user by supply chain participants.

²⁴ Agencies should define thresholds for significant contracting activities based on agency needs and environment. Those may include how critical the specific contracting activity is to the agency mission, mission functions, or a contractual value threshold.

40 41 42 43 Italicized explanations for some template sections are provided to explain the intent of the paragraph.

44 1 INTRODUCTION

45

52

54

61 62

63

64

65

66

67

68

46 Describe the purpose of the ICT SCRM Plan. Tier 1 and 2 ICT SCRM Plans may need to be derived in 47 whole or in part from existing policies or other guidance. Tier 3 Plans may be closely tied to system 48 security plans (SSPs). 49

50 For all tiers, provide a general statement that conveys the intent of the organizational leadership to adhere 51 to the Plan, enforce its controls, and ensure that it remains current.

53 1.1 **Purpose and Scope**

55 Include: Agency name, tier for which this plan applies. 56

57 For Tier 1, list all Tier 2 ICT SCRM Plans within the scope of the Tier 1 ICT SCRM Plan. (This list is an 58 attachment to the ICT SCRM Plan. In the event of organizational changes, it would be preferable to make 59 changes to the Tier 1 attachment than to each individual System Security Plan.) For Tier 1, describe the 60 scope of the applicable organization to which this ICT SCRM Plan applies.

For Tier 2:

- List a unique identifier given to the mission/business. This may be names of acquisition • programs, IT acquisition (e.g., listed in applicable OMB Exhibit 300), or any other designator that describes the scope of the ICT SCRM Plan at Tier 2.
 - Provide a brief explanation of what this mission/business encompasses, including a high-level summary of systems within the scope of this ICT SCRM Plan.
- List all Tier 3 ICT SCRM Plans and/or System Security Plans within the scope of this Tier 2 ICT • SCRM Plan.
- 69 70

For Tier 3, if creating a separate ICT SCRM Plan, include a unique identifier and name given to the

71 72 system. (For consideration: List all essential supporting systems and interfaces (such as network

73 infrastructure) and their relevant SCRM data from their ICT SCRM Plans if such a Plan exists. This

74 provides the opportunity for the agency to find missing, overlapping, and redundant controls. Most, if not

75 all supporting systems will require as a minimum, replacements, supplies, and upgrades,) 76

77 1.2 Authority

78

79 Include: Authorities and references to relevant agency documents such as policies; strategic plan(s); 80 acquisition guidelines; processes; procedures; etc. Policies may include ICT SCRM policy, security 81 policy, acquisition policy, or any other policy applicable in the context of this ICT SCRM Plan. 82

- 83 For Tier 2, include applicable Tier 1 ICT SCRM Plan title.
- 85 For Tier 3, include applicable Tier 1 and Tier 2 ICT SCRM Plan titles.

86 87 1.3 Audience

88

84

89 For all three tiers, include any agency organizational units that should be active participants or interested

- 90 parties in this ICT SCRM Plan and that should be using it to inform their activities. These may include
- 91 legal, acquisition, IT security, supply chain and logistics, human resources, finance, etc. and specific

92 individual roles such as CISO, procurement personnel, program managers, etc., as appropriate. 93 94

95

2 ROLES AND RESPONSIBILITIES

For all three tiers, state those responsible for the ICT SCRM Plan and key contributors to ICT SCRM.
See Section 2.1 for more detail.

- 99 2.1 Responsibility for the Plan
- 100 101

102 103

104

105

106

2.1 Responsibility for the P

State the role and name of the individual or group responsible for the ICT SCRM Plan.

- For Tier 1, an example may be Risk Executive (function), CEO, or CIO
- For Tier 2, an example may be CIO or Program Manager
- For Tier 3, this is the System Owner and, if integrated into the System Security Plan, also the Authorizing Official.

Include the name, title, organizational affiliation, address, email address, and phone number of each
 person.

110 2.2 Key Contributors

111 112

113 114

115

116

117

118

123

127

128

129

130

131

133

137

Identify key contributors to the ICT SCRM Plan.

- For Tier 1, an example may be Agency CFO, COO, Acquisition/Contracting
- For Tier 2, an example may be Acquisition/Contracting, Operations Manager, System Architect
 - For Tier 3, an example may be System Engineer, Security Engineer, Developer/Maintenance Engineer.

119 Include the name, title, organizational affiliation, address, email address, and phone number of eachperson.

121 122 **3 ICT SCRM CONTROLS**

List applicable (per tier) ICT SCRM controls resulting from the Evaluation of Alternatives (in Respond,
 Task 3-3). Description of each control should include the following:

- Title;
- How the ICT SCRM control is being implemented or planned to be implemented;
- Applicable scoping guidance; and
- Tailoring decisions with justifications.

132 For Tier 2, reference applicable Tier 1 ICT SCRM Plan that provides common controls.

134 For Tier 3, reference applicable Tier 2 ICT SCRM Plan that provides common controls.

135136 4 USING AND REVISING ICT SCRM PLAN

ICT SCRM Plans are living documents that must be updated and communicated to all appropriate individuals - government staff, contractors, and suppliers.

141 4.1 Communicating ICT SCRM Plan

142

Describe processes by which this ICT SCRM Plan will be communicated to other Tiers to ensure that ICT
 supply chain interdependencies are addressed. Examples include:

145 146

148

149

150

151

- Posting on appropriate Agency portal(s);
- Communicating via email;
 - Briefing appropriate individuals including those responsible for addressing deficiencies; and
 - Including information contained in the ICT SCRM Plan in applicable training and outreach materials.

152 4.2 Revision and Improvement

153

158

160

Tier 1 and 2 ICT SCRM Plans should be reviewed at a minimum on an annual basis since changes to
 laws, policies, standards, guidelines, and controls are dynamic and evolving. As a minimum, review and
 update Tier 3 ICT SCRM plans at life cycle milestones, gate reviews, and significant contracting
 activities, and verify for compliance with upper tier plans as appropriate.

- 159 State the required frequency for ICT SCRM Plan reviews to consider updates.
- 161 Define criteria that would trigger ICT SCRM Plan revisions. This may include:
- 162Change of authorities that apply to the ICT SCRM Plan;
- Change of policies that apply to the ICT SCRM Plan;
- Significant ICT SCRM events;
- Introduction of new technologies;
- Shortcomings in the ICT SCRM Plan;
- For Tiers 2 and 3, change of governing ICT SCRM Plan for the Tiers above;
- Change of scope; and
 - Other Agency-specific criteria.
- 170 171

If deemed helpful, ICT SCRM Plan owners can use ICT SCRM Plan of Action and Milestones (POAM)
to assess the impact of the changes and guide ICT SCRM Plan revisions and to ensure that the updated
Plan does not leave a gap in coverage from the previous version. Describe ICT SCRM POA&M process
and resolution steps.

177 **4.3 Implementing and Assessing Effectiveness of ICT SCRM Plans**

178

- 179 Agencies should use their ICT SCRM Plans during the budgeting and planning process particularly with
- 180 respect to acquisition and procurement activities. This includes the operations staff procuring
- 181 replacement parts and ancillary services that may not be aware of the potential ICT supply chain risks
- associated with such procurements without following applicable ICT SCRM plans. Each Tier's ICT

- SCRM Plan should describe ICT supply chain risk management monitoring and enforcement activities
 (including auditing if appropriate) applicable to the scope of each specific Plan.
- 185

186 If appropriate, ICT SCRM Plan owners may decide to use qualitative or quantitative measures to support

- 187 implementation of the Plan and to assess effectiveness of this implementation.²⁵ If measures are used,
- 188 *they should be stated in the Plan.*
- 189
- 190 Contractor and supplier-provided plans, associated with Tier 3 systems, should be included if such plans
- are part of contractual agreements. Figure H-3 depicts an example process flow for implementing Agency
- 192 ICT SCRM Plan(s).
- 193



194 195

196

Figure H-3: Agency Implementation of ICT SCRM Plan

197 Describe general details about the use of the ICT SCRM Plan such as when to initiate collaboration with
 engineering and contracting activities, the condition under which ICT SCRM Plan audit is performed, and
 permissible steps to enforce the conditions of ICT SCRM Plans.
 200

For Tier 3, describe the significant elements and the impacts to those elements from contractor or supplier–provided ICT SCRM Plans.

²⁵ NIST SP 800-55 provides guidance on developing information security measures. Agencies can use general guidance in that publication to develop specific measures for their ICT SCRM plans.

- 204 A useful approach to implementing the SCRM plan is to ensure the various activities are mapped and
- tracked as part of an SDLC. This ensures full coverage of SCMT activities since these activities may
- 206 requires repeating and reintegrating (using spiral or agile techniques) which is a common effort in an
- 207 SDLC. SCRM plan activities are necessarily needed as early as in the concept and R&D steps of an
- SDLC and certainly continue into the various SDLC steps including development, production, utilization,
 support and retirement steps.
- 210

There are a number of SDLCs that have been described by various organizations. And each federal

- 212 agency may have its own variant that may have been defined and is currently implemented. What is 213 important is the general understanding and definition of the various SCRM plan activities and how they
- are mapped in the agency specific SDLC.
- 215

216 To provide some guidance on how SCRM activities can be mapped to an SDLC, three example SDLCs

- 217 are provided with SCRM plan activities mapped (see figure H-4). These SDLCs are from NIST, DHS,
- and an example SDLC described in ISO/IEC15288. These SDLCs and the mapping are provided only as
- an example and should be used as a guideline for agency specific SCRM plan implementation. We are
 not endorsing or recommending any one SDLC.
- 220 221



Use of the following paragraphs is optional. Agencies should decide whether to use them depending on

mission criticality, applicable threats, and other factors per agency determination.

222 223 224 225 226

228 4.4 Use of ICT SCRM Plan during Contingencies and Emergencies

229

In the event of contingency or emergency operations, the agency may need to bypass normal acquisition
 processes to allow for mission continuity. Contracting activities that are not vetted using approved ICT
 SCRM Plan processes introduce unknown risk to the organization.

- 232 SCRM Plan processes introduce unknown risk to the org
- When appropriate at Tier 1, 2, or 3, describe abbreviated acquisition procedures to follow during contingencies and emergencies, such as the contact information for ICT SCRM subject matter experts who can provide advice absent a formal tasking and approval chain of command.
- 237
- 238 For Tier 1, describe agency procedures and waiver processes.
- For Tier 2, describe mission/business procedures and waiver processes in addition to Tier 1.
- For Tier 3, describe system-specific procedures and waiver processes in addition to Tiers 1 and 2.
- 241

242 **ATTACHMENTS**

- 243
- For Tier 1, attach or provide links to applicable Tier 2 ICT SCRM Plans.
- For Tier 2, attach or provide links to applicable Tier 3 ICT SCRM Plans.
- For Tier 3, attach or provide links to applicable plans for essential supporting systems.
- For Tier 3, attach applicable contractual agreements or ICT SCRM Plans provided by contractors or suppliers.
- 249
- 250