ITL BULLETIN FOR JULY 2018

ASSESSING IMPLEMENTATION OF CONTROLLED UNCLASSIFIED INFORMATION (CUI) SECURITY REQUIREMENTS

Ned Goren, Jody Jacobs, Larry Feldman,[1] and Greg Witte,[1] Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

The protection of Controlled Unclassified Information (CUI)[2] that resides in nonfederal information systems and organizations is of utmost importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations. It is vitally important to protect federal CUI in nonfederal systems – that is, in information systems *other than* those directly used or operated by or on behalf of a federal agency.

Executive Order 13556, *Controlled Unclassified Information,* established the National Archives and Records Administration (NARA) as the CUI Executive Agent. As CUI Executive Agent, NARA is responsible for developing and issuing such directives as are necessary to implement the CUI Program to establish uniform policies and practices across the federal government. NARA issued a final federal regulation in 2016 establishing the required controls and markings for CUI governmentwide. This federal regulation, 32 CFR Part 2002, binds agencies throughout the executive branch to uniformly apply the standard safeguards, markings, dissemination, and decontrol requirements established by the CUI Program.

The CUI Program, as implemented by NARA, is designed to address several deficiencies in managing and protecting unclassified information to include inconsistent markings, inadequate safeguarding, and needless restrictions, both by standardizing procedures and by providing common definitions through a CUI Registry (see https://www.archives.gov/cui/registry/category-list). The CUI Registry is the online repository for information, guidance, policy, and requirements on handling CUI, including issuances by the CUI Executive Agent (NARA). Among other information, the CUI Registry identifies approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls,

[1] Larry Feldman and Greg Witte are NIST Associates from G2, Inc.
[2] Controlled Unclassified Information is any information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, *Classified National Security Information*, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

and sets out procedures for the use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, reusing, and disposing of the information.

In addition to defining safeguarding requirements for CUI within the federal government, NARA partnered with NIST and the Department of Defense to develop Special Publication (SP) 800-171, Revision 1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. NIST SP 800-171 specifies the security requirements for protecting the *confidentiality*[3] of CUI at the moderate impact level when the CUI is resident in a nonfederal system or organizations.

The target audience of NIST SP 800-171 includes individuals both in the public and private sector with responsibilities pertaining to acquisition or procurement, security assessors and independent verifiers/validators, analysts, and system, security or risk managers with oversight responsibilities.

Nonfederal organizations implement the security requirements in SP 800-171 and document the implementation details in a system security plan. Nonfederal organizations then assess the effectiveness of the implementations to help ensure that security requirements are met.

Assessing Security Requirements for CUI

Although the set of requirements described in SP 800-171 are fixed, nonfederal organizations have some flexibility in how those requirements are implemented. Organizations need consistent methods to assess and document the extent to which an implementation satisfies the CUI security requirements in SP 800-171. To help nonfederal organizations develop assessment plans and conduct efficient, effective, and cost-effective assessments of the CUI security requirements, NIST published SP 800-171A, *Assessing Security Requirements for Controlled Unclassified Information*. SP 800-171A provides generalized assessment procedures that can be used to develop specific procedures to assess the implementation of the CUI security requirements. These procedures also produce relevant evidence to determine if the security safeguards employed by organizations are implemented correctly, are operating as intended, and satisfy the CUI security requirements in SP 800-171.

The assessment process is an information-gathering and evidence-producing activity to determine the effectiveness of the safeguards intended to meet the set of security requirements specified in SP 800-171. In this context, the information gathered and the evidence produced can be used by a nonfederal organization to:

[3] NIST SP 800-171 states that, "In addition to the security objective of confidentiality, the objectives of integrity and availability remain a high priority for organizations that are concerned with establishing and maintaining a comprehensive information security program. While the primary purpose of SP 800-171 is to define requirements to protect the confidentiality of CUI, there is a close relationship between confidentiality and integrity since many of the underlying security mechanisms at the system level support both security objectives."

- Identify potential problems or shortfalls in the organization's security and risk management programs;
- Identify security weaknesses and deficiencies in its systems and in the environments in which those systems operate;
- Prioritize risk mitigation decisions and activities;
- Confirm that identified security weaknesses and deficiencies in the system and in the environment of operation have been addressed; and
- Support continuous monitoring activities and provide information security situational awareness.

Basic Concepts

The CUI assessment procedures are flexible and can be customized to the needs of the organizations and the assessors conducting the assessments. Security assessments can be conducted as self-assessments; independent, third-party assessments; or government-sponsored assessments and can be applied with various degrees of rigor, based on customer-defined depth and coverage attributes.

In SP 800-171, security requirements are organized into fourteen families that provide comprehensive protection of the confidentiality of CUI in nonfederal systems and organizations. Each family, as shown in Table 1, contains the requirements related to the general security topic of the family. The families are closely aligned with the minimum-security requirements for federal information and systems as described in Federal Information Processing Standard (FIPS) 200. The contingency planning, system and services acquisition, and planning requirements are not included within the scope of 800-171 due to the tailoring criteria.[4]

FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

Table 1: CUI Security Requirement Families

Each assessment procedure consists of an assessment *objective* and a set of potential assessment *methods* and assessment *objects* that are used to conduct the assessment. Each assessment objective

[4] Organizations can use NIST SP 800-53 to obtain additional, non-prescriptive information related to the security requirements (e.g., supplemental guidance related to each of the referenced security controls, mapping tables to ISO/IEC security controls, and a catalog of optional controls that can be used to help specify additional security requirements if needed).

includes a determination statement related to the CUI security requirement that is the subject of the assessment. The determination statements are linked to the content of the CUI security requirements to ensure traceability of the assessment results to the requirements. The application of an assessment procedure to a security requirement produces assessment *findings*. These findings reflect, or are subsequently used to help determine, whether the security requirement has been satisfied.

Assessment objects are the specific items being assessed and include specifications, mechanisms, activities, and individuals. Specifications are the document-based artifacts (e.g., policies, procedures, security plans, security requirements, functional specifications, architectural designs) associated with a system. Mechanisms are the specific hardware, software, or firmware safeguards employed within a system. Activities are the protection-related actions supporting a system that involve people (e.g., conducting system backup operations, exercising a contingency plan, and monitoring network traffic). Individuals, or groups of individuals, are people applying the specifications, mechanisms, or activities described above.

The assessment methods define the nature of the assessor's actions. The methods include *examine*, *interview*, and *test*. The *examine* method is the process of reviewing, inspecting, observing, studying, or analyzing assessment objects (i.e., specifications, mechanisms, activities). The purpose of the *examine* method is to facilitate understanding, achieve clarification, or obtain evidence. The *interview* method is the process of holding discussions with individuals or groups of individuals to facilitate understanding, achieve clarification, or obtain evidence. And finally, the *test* method is the process of exercising assessment objects (i.e., activities, mechanisms) under specified conditions to compare actual with expected behavior. In all three assessment methods, the results are used in making specific determinations called for in the determination statements and thereby achieving the objectives for the assessment procedure.

The assessment methods, described in SP 800-171A, Appendix D, have associated attributes of *depth* and *coverage*, which define the level of effort for the assessment. These attributes provide a means to define the rigor and scope of the assessment for increased assurance of the effectiveness of security requirement implementation. Figure 1 illustrates an example of an assessment procedure for CUI security requirement 3.1.3 from SP 800-171.

3.1.3	**SECURITY REQUIREMENT** Control the flow of CUI in accordance with approved authorizations.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.3[a]	*information flow control policies are defined.*
	3.1.3[b]	*methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c]	*designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d]	*authorizations for controlling the flow of CUI are defined.*
	3.1.3[e]	*approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].	

Figure 1: Assessment Procedure for CUI Security Requirement

Organizations are not expected to employ *all* assessment methods and objects contained within the assessment procedures identified in the publication. Organizations have the flexibility to specialize the assessment procedures by selecting the specific assessment methods and the set of assessment objects to achieve the assessment objectives. There is no expectation that all assessment methods and all objects will be used for every assessment. There is also significant flexibility on the scope of the assessment and the degree of rigor applied during the assessment process. The assessment procedures and methods can be applied across a continuum of approaches including self-assessments, independent, third-party assessments, and assessments conducted by sponsoring organizations (e.g., government agencies). Such approaches may be specified in contracts or in agreements by participating parties.

Assurance Cases

Building an effective assurance case for determining compliance to CUI security requirements is a process that involves compiling evidence from a variety of sources and conducting different types of activities during an assessment. An assurance case is a body of evidence organized into an argument demonstrating that some claim about a system is true. For assessments conducted using the procedures

in this publication, that claim is *compliance* with the security requirements specified in SP 800-171. Assessors gather evidence during the assessment process to allow designated officials to make objective determinations about compliance to the CUI security requirements. The evidence needed to make such determinations can be obtained from various sources including self-assessments, independent third-party assessments, or other types of assessments, depending on the needs of the organization establishing the requirements and the organization conducting the assessments.

Assessment Procedures

Organizations conducting CUI security requirement assessments can build assessment plans using the information provided in the assessment procedures—selecting the specific assessment methods and objects that meet the organization's needs. Organizations also have flexibility in defining the level of rigor and detail associated with the assessment based on the assurance requirements of the organization. Appendix D of SP 800-171A provides additional information on the different levels of rigor and detail for assessments.

The assessment objective defined for each assessment procedure is achieved by applying the designated assessment methods to the selected assessment objects and compiling/producing the evidence necessary to make the determination associated with each assessment objective. Each determination statement contained within an assessment procedure produces one of the following findings: *satisfied* or *other than satisfied*. A finding of "satisfied" indicates that, for the security requirement addressed by the determination statement, the assessment information obtained (i.e., the evidence collected) indicates that the assessment objective has been met producing a fully acceptable result. A finding of "other than satisfied" indicates that, for the security requirement addressed by the determination statement, the assessment findings obtained indicate potential anomalies that may need to be addressed by the organization. A finding of "other than satisfied" may also indicate that for reasons specified in the assessment report, the assessor was unable to obtain sufficient information to make the determination called for in the determination statement.[5]

For assessment findings that are other than satisfied, organizations may define subcategories of findings indicating the severity or criticality of the weaknesses or deficiencies discovered and the potential adverse effects of those weaknesses or deficiencies on organizational missions and/or business functions. Defining such subcategories can help to establish priorities for needed risk mitigation actions.

[5] The broad range of potential assessment methods and objects listed in 800-171A do not necessarily reflect, and are not directly associated with, actual compliance or noncompliance. They can help generate a picture of overall satisfaction of CUI security requirements. Organizations have the flexibility to determine the specific methods and objects sufficient to obtain the needed evidence to support claims of compliance.

Supplemental Materials

Drafts of SP 800-171A included an Appendix that provided supplemental information about the CUI security requirements in NIST SP 800-171. The supplemental information was deemed more useful for implementation of the safeguards employed to protect CUI, and thus has been moved to an appendix in SP 800-171 Revision 1 (Appendix F).

In addition to the guidance provided in SP 800-171A, NIST has provided several example templates (i.e., CUI System Security Plan, CUI Plan of Action) to assist with planning and assessments. While there is no prescribed format or specified level of detail for system security plans or plans for action, by using these templates, or organization-specific derivatives of these, nonfederal organizations can ensure that the required information (i.e., from SP 800-171 Requirements 3.12.2 *Develop and implement plans of action* and 3.12.4 *Develop, document, and periodically update system security plans*) is conveyed.

Upcoming Workshop

On October 18, 2018, NIST, in coordination with the Department of Defense (DoD) and the National Archives and Records Administration (NARA), will host an informational workshop providing detailed information about many of the areas described above. Topics will include an overview of CUI, the Defense Federal Acquisition Regulation Supplement (DFARS) Safeguarding Covered Defense Information and Cyber Incident Reporting Clause, and NIST SPs 800-171 and 800-171A. Panels of federal government representatives will discuss expectations for evaluating evidence and implementing the CUI security requirements, and industry representatives will share best practices and lessons learned.

The CUI Security Requirements Workshop is open to all interested stakeholders and is free to attend. To register for on-site participation, please visit: https://www.nist.gov/news-events/events/2018/10/controlled-unclassified-information-security-requirements-workshop. The workshop will also be available via webcast, for which advanced registration is not required. More information will be available in upcoming months through the same URL.

Conclusion

NIST SP 800-171A provides assessment procedures for the CUI security requirements defined in SP 800-171. SP 800-171A provides flexible methods to customize assessments based on organizational policies and requirements, known threat and vulnerability information, system and platform dependencies, operational considerations, and tolerance for risk. The findings and evidence produced during the security assessments can facilitate risk-based decisions by organizations related to the CUI requirements. Any nonfederal organization that collects, processes, stores, or transmits CUI can plan for and conduct assessments using these procedures to help determine the effectiveness of implemented

CUI security requirements; to identify actions to mitigate security related risks; and to ensure CUI security requirements are being met.

Additional Resources

SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, April 30, 2013

Executive Order 13556, *Controlled Unclassified Information*, https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information, November 2010.

Executive Order 13526, *Classified National Security Information*, https://www.archives.gov/isoo/policy-documents/cnsi-eo.html, December 2009.

Atomic Energy Act of 1954, 2 U.S.C. §§ 2011-2021, 2022-2286i, 2296a-2297h-13 https://science.energy.gov/~/media/bes/pdf/nureg_0980_v1_no7_june2005.pdf, August 1954.

NARA CUI Registry
https://www.archives.gov/cui/registry/category-list

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov