From:	[redacted] via 800-171comments
To:	800-171comments@list.nist.gov
Subject:	[800-171 Comments] NIST SP 800-172r3 Comments
Date:	Thursday, January 9, 2025 2:34:39 PM
Attachments:	NIST SP 800-172r3-ipd-CRM_CROWS.xlsx

To whom it may concern,

please see the attached comments from members of the AFLCMC/EN-C/ASB/SSE & /CRST of the CROWS department.

Please continue to inform us for future comment items.

V/R,

Corbin Conwell
[redacted]
AFLCMC/EN-C/ASB/SSE
Systems Security Engineer
KBR | Mission Technology Solutions

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Jeffrey King, USAF/AFLCMC/EN-EZC-CROWS	G	1	160	E.O. 13566 only states, "establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies…….	Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and Federal Information Security Modernization (FISMA) Act of 2014, Public Law 113–283 drive CUI computing protection.
2	Jeffrey King, USAF/AFLCMC/EN-EZC-CROWS	G	1	172	The CUI regulation requires federal agencies that use federal information systems to process, store, or transmit CUI to comply with NIST standards and guidelines.	"The CUI regulation requires federal agencies that use federal information systems to process, store, or transmit CUI to comply with NIST standards and guidelines according to proper engineering and information sensitivity levels".
3	Jeffrey King, USAF/AFLCMC/ EN-EZC-CROWS	G	1	175	"a similar level of protection is needed when CUI is processed, stored, or transmitted by nonfederal organizations using nonfederal systems" should have a term instead of "similar" use "having the same security level".	"nonfederal systems having the same security level of protection is needed when CUI is processed, stored, or transmitted by nonfederal organizations using nonfederal systems"…
4	Jeffrey King, USAF/AFLCMC/ EN-EZC-CROWS	G	1	179	The requirements are derived from the controls in NIST Special Publication (SP) 800-53	There should be additional information found in the Federal Information Security Modernization (FISMA) Act of 2014, Public Law 113–283 that provides information protection authority instead of NIST SP 800-53.
5	Jeffrey King, USAF/AFLCMC/ EN-EZC-CROWS	G	2	210	"[11] System components include workstations, servers," ….. is not sufficient.	Propose "[11] System components include but not limited to workstations, servers, notebook computers, smartphones, tablets, input and output devices, operating systems, network components, virtual machines, database management systems, firmware, "plug-ins", and applications."

6	Jeffrey King, USAF/AFLCMC/ EN-EZC-CROWS	G	2	211	The footnote [10] for "penetration-resistant architecture, damage-limiting operations, and cyber resiliency" does not align with the entire problem. Insider Threat is not being addressed here given damage-limiting operations do not work when email is included in these system architectures. Email is the source of over 80% of external attacks. Multi-Factor Authentication (MFA) will not stop a crafted email for system intrusion.	Insider Threat is not being addressed here given damage-limiting operations do not work when email is included in these system architectures. Email is the source of over 80% of external attacks. Multi-Factor Authentication (MFA) will not stop a crafted email for system intrusion.
7	Jeffrey King, USAF/AFLCMC/ EN-EZC-CROWS	G	4	271	"Penetration-resistant architecture: An architecture that uses technology and procedures" is not sufficient.	Should read "Penetration-resistant architecture: An architecture that uses technology, engineering, and procedures" to align with other NIST documents like NIST SP 800-160, Vol.1, Rev.1, "Engineering Trustworthy Secure Systems, and SP 800-160, Vol.2, Rev.1, "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach"

8	Jeffrey King, USAF/AFLCMC/ EN-EZC-CROWS	G	5	278	Cyber resiliency-should be more aligned all all NIST documents, NIST SP 800-39 and 800-160, Vol.2, Rev. 1 conflict for the 'resilient' system definition. There should be a definition external to NIST documentation given the concept is not from NIST before 2011.	This definition should be derived from Resilience Engineering: Concepts and Precepts by David Woods, Erik Hollnagel, and Nancy Leveson, 2006. Given NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, Rev. 1, dated, March 2011, the definition of resilience is as follows, "The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs", there needs a revisiting of the term "cyber resiliency" and "information system resiliency" for multiple documents from NIST and CNSSI 4009 OPRs. NIST SP 800-160, Vol.1, "Engineering Trustworthy Secure Systems", should align with NIST SP 800-39, 800-53, and 800-160 Vol.2, Rev.1 information.
9	Jeffrey King, USAF/AFLCMC/ EN-EZC-CROWS	G	5	315	"Applying a threat-centric approach to" is another vague term.	Propose this, "Applying a 'cyber resilient' approach to", instead of "threat-centric".
10	Jeffrey King, USAF/AFLCMC/ EN-EZC-CROWS	G	6	325	The statement "Employing a security operations center with advanced analytics to support continuous monitoring and the protection of systems" is driving a significant cost to an organization's mission.	Suggest, "Employing a security and continuous montoring capability with advanced analytics for the protection of systems with required incident response planning…." is more likely.
11	Jeffrey King, USAF/AFLCMC/ EN-EZC-CROWS	G	8	382	"Organizations can select the enhanced security requirements either comprehensively"….. where "enhanced requirements" is not a proper descriptor.	Should read…. "select the enhanced security controls"…… as requirements would not be allowed to be omitted.

12	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	G	All	All	Why do we need CUI as it does not provide real security beyond the marking of documents that could have been marked as CONFIDENTIAL under existing Classified Material Handling mandates?	Where is the cost-benefit study to justify this added administrative burden on federal offices to include the DoD? If anyone violates a CUI marking, where is the legal means to prosecute them under?
13	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	E	All	All	All acronyms should have their first letter capitalized upon their first instance of use (i.e., "advanced persistent threat" that should read "Advanced Persistent Threat (APT)".	Use of proper grammer and style.
14	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	G	6	28	Is Congress and other USG departments, agencies and offices subject to CUI?	Cybersecurity risks along with senstive material spills occur outside of the "Audience" as cited herein this standard. For Congressional level documents we use along with those in NSA and the State Department, why are thye exempt from this CUI marking standard, if not CMMC?
15	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	T	7	64	The DoD already has long standing data markings (e.g. Controlled) for CTI in the SCRM.	Before NIST drafts these standards, I strongly recmmend you have some of our SMEs who actually use documents daily are invited to the NIST committee tables. Since 2019, the USAF CROWS Office staff SSE Cyber Guidebook team has commented on every NIST Standard, as we are the practical high-level guidance for all DAF Users of documents mandated by the Congressional DFARS for the AAF.

16	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	T	All	All	The DoD CIO office staff are not the mainstream NSS (e.g., Weapons Systems, Mission Essential Systems, Critical Information Systems) SMEs.	The majority of the DoD weapon systems engineering staff work within the extremely regulated Adaptive Acqusition Framework (AAF) requirements that involves all other engineering data, drawings, and documentation beyond the smaller Cybersecurity artifacts footprint. Most strongly request that the DoD CTO esp. OUSD (R&E and A&S if not AT&L) and DASD have an input to these NIST standards, not just the DoD CIO office.
17	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	T	All	All	Explain how CUI protects data and drawings when they use the same DoD NIPR systems?	I see CUI only valid and practically implemented with measurable protection if and only if it is hosted on secure enterprises.

18	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	T	13	196	Cyber Physical Systems (CPS) are not new except to the Cybersecurity mindset. Strongly recommend to use the OUSD SE experts for covering anything outside of Cybersecurity for all CPS in terms of requirements with specifications, manufacturing processes and real-world documentation.	Since the 1970's DoD weapon systems have used analog, digital and software components. Digital Engineering like the Cloud are jargon for existing systems & terms. CPS demand more than the limited protection afforded by RMF Controls as we System, Electronic and Control Systems engineers have known for decades. For manufacturing processes for weapon systems, these employ what we now term as CPI. For SCRM, and the maintenance and operating manuals used by military personnel, they contain CTI for Critical Technology Elements (correct acronym for Critical Components [CC]).
19	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	T	13	209	"cyber resiliency" is not as cited; but in terms of real engineering of systems, the ability to recover a capability within a specific mission or safety Steady State Response Time. Cyber Resiliency has nothing to do with protecting data.	The OUSD (R&E) Cyber Resiliency Team with the USAF CROWS SSECG Team and the US Army ARL addressed this already for NSS CPS Weapon Systems with actually measurable metrics.

20	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	T	14	220	We are confusing those E.O. FARS/DFARS IS versus their NSS delineated terms.	For the DoD IS that are designed not by FISMA, but under legal and regulatory USG legal language, the MDA/PEO, … can designate IS (i.e. Defense Business Systems [DBS]) as NSS. If not, CMMC covers the contractor systems as they are. If NSS, we are in a different place that this CUI data should have been marked as classified. For CUI, the costs and practical reality of data systems are not going to redesign their architectures. CMMC currently is being held in abeyance by the USG House.
21	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	G	14	231	NIST is not a regulatory or legal body that can specify requirements in its strict USG legal sense. NIST can only promulgate standards as with all of the standards we professional commericanl, industrial or DoD engineers use.	Change: "… requirements '"'" to read: "… standards …"
22	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	G	15	250	Recommend that NIST use the designations for systems as either IS or NSS.	Federal vv. Non-Federal systems does not reaily fit into existing E.O., FARS/cFARS, DFARS and NSA/DHS system designations.
23	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	G	15	268	This section reads for IT-centric, non-DoD personnel. We have requirements that are already a part of several DoD legally required documents (i.e., SSP, PPIP, CSP, …)	Explain the difference for federal NIPR systems from what this paragraph is calling out; and along with what already is required for DoD contractor data systems.

24	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	G	15	268	As a useful and effective standard, we need to approach these items interms of IS vv NSS for all federal systems, terms legally required.	Note: this definition is the correct one as opposed to the earlier wrong definition for "Cyber Resiliency."
25	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	T	16	311 - 329	These line items could have been collated under existing formal acronyms (e.g., "… periodically refreshing …" vice "… Cyber Hygiene …"	A reoccuring problem is that NIST standards committees rarely rely on or use the other NIST standards terminologies making these standards verbose and not portable for their practical implementation by those in the real world. NIST standards bodies - please use your own existing formal definitions to eliminate overlapping standard recommendations or terms that differ in acronym labeling and their definitions.
26	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	G	17	321	Note: Most large and mid-sized defense contractors already fall under and comply with CM standards. Why is NIST trying to address CM that is covered by ISO/IEC and several DoD CM standards already in use? In any program esp. DoD that SSE is intergated into SE and not allowed to run parallel or outside of the Congresionally mandated AAF or FARS/cFARS/DFARS, all Cybersecurity associated items are in one CM plan as are Cybersecurity requirements.	NIST Standards should realize that other regulatory and standard bodies exist that industry, commercial and USG/DoD comply with. All CTE and CPI and CTI are already designated as Configuration Items (CI). Cybersecurity needs to be integrated into existing standards and SE processes, and not allowed to be an independent process or with its own documents, databases or new acronyms for what already exists.

27	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	T	17	334	Again, NIST is not an authoritative USG body, but standards body.	Repalce "requirements" with "standards" as with all other commerical, industrial, DoD and international standards. If these are Congressionally approved requirements, change all NIST standards language for complaince with "shall" statements.
28	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	T	17	338	ODPs are not standard System Engineering terms or concepts as per the other USG, industiral and academic standards. Requirements are derived from operational/mission documents that specify their performance using measurable metrics. RMF requirements as used in the real-world for DoD CPS weapon systems require measurebale specifications. The ODPs are already defined using historically standardized acronyms in these high-level customer created documents. Laws are useless for engineering requirements as they rarely target specific mission, operational or safety requirements as regualtions, standards and national and international agreements do in the real-world.	Strongly recommend that NIST comply wsith existing System Engineering requirements workflow processes irregardless of the RMF Controls and their disassociated concepts and processes, SSE must be integrated into SE otherwise the costs and extra resources required will continue not to provide measurable data for their justification beyond specific Cyber Events identified. Lines 367 through 380 are not how requirements are written - added the problem with RMF remains as demostrated herein there are no threshold for their proven performance or effectiveness. Engineers do not write requirements without providing metrics that can be cost estimated, and provide mission and safety functionality related means of their validation and verification. Direct Cybersecurity requirements be brought back under the rest of the engineering world's acronyms, workflow processes and derivation methods.

29	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	T	19	381	This paragraph does not address the NSA guidance for all NSS that includes the DoD NSS.	Add in this apragraph that all NSS must utilize CNSSI Technical Controls or NIST RMF Controls on the HIGH-HIGH side until otherwise proven otherwise or with a formal SSO exemption.
30	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	G	20	399	Many paragraphs repeat themselves throughout ths document rather than this standard presenting content in a workflow format.	Reqrite this standard in a workflow format that will reduce the page count and eliminate too much philosophical-like repetitve material.
31	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	E	20	418	This section is current and needs no revisions other than when NIST SP800-53 and CNSSI 1253 are updated.	Comment only. The most useful section of this entire standard.

32	Joseph D. Yuna USAF/AFLCMC/ EN-C/CRST	T	99	Table 3	Most strongly disagree with the table Cyber Resiliency Attributes and underlining, unspecified techniques. Cyber Resiliency is a SE not SSE Cybersecurity discipline. Even for IS vv. CPS NSS, what is prsented affords little to no real engineering guidance. Cyber Resiliency within the military IS (or designated IS to be NSS) deals with the ability to recover partial to full capabilities within a specified timeframe. Prevention as specified in this table is not resiliency in commerical, industrial, military or academic terms. This is why the USAF and other military services integrate SSE into SE, meaning a system's resilienmce depends on its inherent design and customer specified requirements.	Refer NIST to the Resiliency SME (Scott Jackson) or the GAO, Congressionally and OUSD recognized USAF SSE Cyber Guidebook v5.0 for what Cyber Resiliency is.
33	Corbin Conwell USAF/AFLCMC/EN-EZC-CROWS	G	1	160	Using the 13556 makes it seem like this isn't going to apply to main user (DoD). "..how the executive branch handles CUI). The 13556 only says it establishes a policy for the need of a standard practice.	Consider the use of DoDI 5200.48 or NIST SP800-171 as these show actual policy/procedure and standards
34	Corbin Conwell USAF/AFLCMC/EN-EZC-CROWS	G	1	160-180	This publication is using the same introduction from NIST SP 800-171R3 Need to include an introduction as to why enhanced controls should be considered	Removing the original introduction that is a copy and keeping the secondary portion looks to be a good reasoning if the idea is to focus on APT.

35	Corbin Conwell USAF/AFLCMC/EN-EZC-CROWS	G	1	188	The APT makes no mention of the goal of the APT being to remain active while attempting to avoid detection	APT objectives include establishing a foothold and remaining undetected for as long as possible….
36	Corbin Conwell USAF/AFLCMC/EN-EZC-CROWS	G	2	204	Confidentiality, integrity, availability Add in the acronym.CIA is a common acronym in the IT/IS/CS…etc	Add acronym CIA.
37	Corbin Conwell USAF/AFLCMC/EN-EZC-CROWS	G	All	All	NIST SP 800-171 This needs to be updated to the latest version.	NIST SP 800-171R3
38	Corbin Conwell USAF/AFLCMC/EN-EZC-CROWS	G	All	All	SP 800-53 Needs updated to latest version in many areas.	NIST SP 800-53R5
39	Corbin Conwell USAF/AFLCMC/EN-EZC-CROWS	G	6	Table 1	Address the missing controls as done in SP-171	Explain why the the 800-53 includes 53 controls and what ones were left from/changed and why.