aia-aerospace.org

AIA
AEROSPACE
INDUSTRIES
ASSOCIATION

August 2, 2019

National Institute of Standards and Technology
Computer Security Division
Computer Security Resource Center
Email to: sec-cert@nist.gov

RE: Docket ID: NIST-2019-0002, Request for Comments on NIST Special Publication (SP) 800-171B (800-171B), Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations – Enhanced Security Requirements for Critical Programs and High Value Assets

Dear NIST:

I am pleased to offer the following comments and attached documentation on the subject NIST call for comments on behalf of the Aerospace Industries Association of America (AIA), the premier trade association representing more than 340 of the nation's leading aerospace and defense manufacturers and suppliers. For 100 years, AIA has been the industry voice shaping the policies that matter most to our members. AIA's expertise represents the interests of manufacturers and suppliers of civil, military, and business aircraft, helicopters, unmanned aerial systems, space systems, aircraft engines, missiles, materiel, and related components, equipment, services, and information technology.

Beginning with the first notification of public DFARS rulemaking in March 2010, AIA and other industry partners have submitted comments on proposed cyber-related requirements applicable to contractors' internal information systems. Lessons learned have demonstrated that requirements and processes in cybersecurity are mutually beneficial when shared through robust collaboration across sector business operations representing all stakeholders. AIA looks forward to following and providing additional feedback as 800-171B and other 800-171 series publications progress to the next step of drafting and adjudicating the public comments in support of collective cybersecurity and protection strategies.

Before addressing the proposed enhanced controls, we note that the draft does not adequately identify when these enhanced controls would apply to programs or assets. The 800-171B only states that the enhanced controls shall apply "when the designated CUI is contained in a critical program or high value asset." While NIST identifies reference documents for "high value asset," it provides no definition or reference documents with respect to what will constitute a "critical program" or any guidance regarding how such a determination will or should be made. Further, the 800-171B does not provide any detail as to when all the enhanced controls would be required versus a subset of those requirements. The lack of clarity in this area significantly impacts the ability of AIA and other organizations to provide effective comments on the controls themselves and to be able assess the full financial impacts of the proposed enhanced controls on contractors. More importantly, the resulting uncertainty will likely result in inconsistent application by agencies, a lack of predictability for the contracting community, increased costs for programs that may not be critical, and less than desired overall effectiveness of the NIST publication.

The lack of this crucial information in the 800-171B draft will lead reviewers to formulate assumptions in interpreting the NIST, DOD and other federal agencies objectives with respect to the proposed enhanced security requirements. Categorization of programs and data is essential in determining the CUI protections in global nonfederal environments.

The unpublished status of twenty of the NIST SP 800-53 security control mappings in Appendix D and the identification of 30 NIST publications as references for guidance in the Chapter Three requirements discussion sections further complicates the ability of reviewers to fully analyze and comment on the proposed enhanced controls. While we understand NIST has numerous new 800-53 controls in draft form, the draft of this future revision of 800-53 has not been released for review and thus reviewers have no ability to review these controls. It is noted that several controls in 800-171B map to the same 800-53 controls mapped in 800-171. Since 800-171B is “enhanced,” its control mapping should not duplicate those already in 800-171. Contractors rely heavily on these mappings. Duplication between 800-171 and 800-171B makes it difficult to determine what more needs to be done that isn’t already accomplished under 800-171. Additionally, given the significant costs associated with implementing many of these controls, AIA questions the effectiveness of the Government imposing enhanced controls on contractor systems that have not yet been imposed, no less implemented, on the Government’s own systems.

With the publication touching many aspects of DFARS Clause 252.204-7012, 800-171, & 800-171A, AIA is submitting comments not only on the draft publication but also to address industry concerns for the following 800-171B areas with respect to cybersecurity significance, acquisition processes, and the tiered supply chain.

Enhanced Protections & Cybersecurity Risk

- Many of the enhanced requirements address risk avoidance and result in limited protection value associated with Advanced Persistent Threats (APT) in nonfederal environments. Close to 30% of the controls are static, excessive, non-mitigating, and misaligned to nonfederal entities’ state of operations across global computing environments benefiting from dynamic computing established through cloud services, artificial intelligence, and increased cybersecurity.

- Requirements associated with isolation/enclaves, diverse systems and services, and cross domain security solutions are generally equated with closed, classified environments normally specified through programs associated with national security and governance by the National Industrial Security Program (NISP) and the Committee on National Security Systems (CNSS).

Acquisition & Regulatory Process

- Assessing controls for a nonfederal profile without a risk-based nonfederal profile tailored to threat and operations is problematic. The draft describes the controls and implementations as “intended to be implemented comprehensively however services/programs can select and/or exempt certain enhanced security requirements”. Acquisition processes that allow for cybersecurity protections to be unilaterally divergent service by service, company by company, contract by contract, and specified differently across DOD programs and requiring activities appears to be inconsistent with common and proven risk management frameworks and implementations. However, with the development of the DOD’s new Cybersecurity Maturity Model Certification (CMMC) effort, the risk-tailored aspect of 800-171B may be described within the CMMC levels of maturity that contain 800-171B controls.

- Clear requirements and contractor and multi-tier subcontractor implementation specifics are needed to understand the acquisition and business process intended for contactors, suppliers, vendors, and service providers in the areas of operational performance, risk, compliance, and allowable costs. Per DOD briefings, the CMMC is expected to have five tiers of assessed maturity and include the NIST 800 series of publications that will enable third-parties to audit contractors to assess cybersecurity compliance. Under the CMMC, the level of cybersecurity required by a procuring activity (to include 800-171 and 800-171B) will be indicated on all contract solicitations starting in mid-2020.

- Acquisition processes and procedures across federal and nonfederal stakeholders is currently disjointed across departments and agencies further complicating collaborative communication, training, and awareness. The acquisition process will be further complicated by the yet to be defined concept of “critical programs,” a key determinant of 800-171B application. This, when combined with the existing struggles of procuring activities to identify CUI and the lack of updated agency CUI guidance as contemplated by the NARA rule, will lead to further uncertainty in the industrial base, particularly for small business operations, manufacturing facilities, and commercial products.

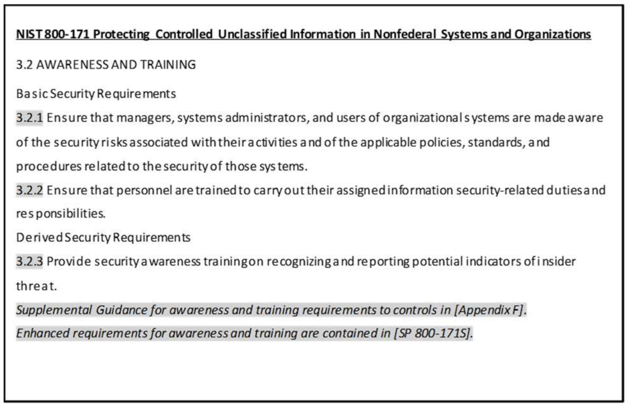
- AIA also is aware that multiple DOD components in the last year have been imposing or seeking to impose their own enhanced safeguards designed at protecting against the APT. Now that NIST has published the draft of 800-171B, these agencies should be strongly encouraged to use the unified standards for all DOD contracts applying to critical programs instead of their own requirements. It is critical for industry to have uniformity, predictability, as well as a meaningful opportunity for review and comment before any new requirements are imposed on contractors and their supply chains.

Supply Chain: Government(s), Owners, Operators, Suppliers, Vendors, and Service Providers

- Small companies will most likely be unable to satisfy the enhanced controls and will find difficulty identifying authorized service providers with small volume licensing models thereby impacting specialized deliverables. The 800-171B requirements as written are infeasible to execute by and across the tiered supply chain. AIA supply chain companies are reporting 75% of the enhanced controls will have a high impact and the remaining 25% are considered high to moderate.

- The draft 800-171B contemplates that determinations as to the applicability of enhanced controls will be made at a program level. This raises concerns with respect to flow-down. For example, if a third-tier supplier only has an export-controlled drawing of its small component, the application of the enhanced controls seems unnecessary and wasteful. AIA recommends considering additional guidance regarding flow-down, particularly as it may be less important depending on the extent of a lower tier supplier's access to CUI.

- AIA members recommend. the 800-171B publication be renamed to 800-171E to reference the requirements as "Enhanced" and designated supplemental with minor formatting refinements. The sequential numbering of the enhanced security requirements should be changed to reflect a distinctive supplemental schema associated with the control family distinguishable from the individual objective of the numbered NIST 800-171 requirement. An example is provided below showing that under control family 3.2, the enhanced controls would continue the number schema and be further identified with the addition of an 'E' at the end.



NIST 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

3.2 AWARENESS AND TRAINING

Basic Security Requirements

3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

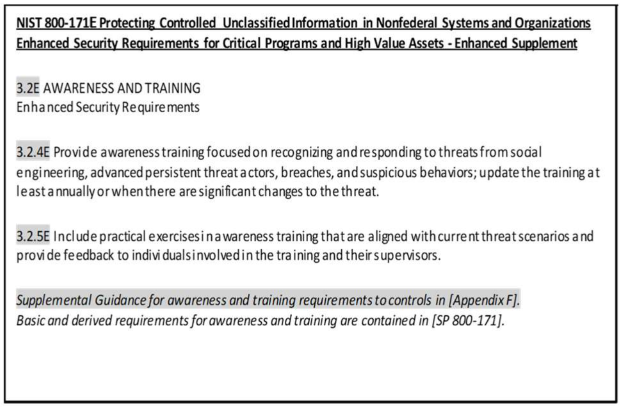
3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

Derived Security Requirements

3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Supplemental Guidance for awareness and training requirements to controls in [Appendix F].

Enhanced requirements for awareness and training are contained in [SP 800-171S].



NIST 800-171E Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
Enhanced Security Requirements for Critical Programs and High Value Assets - Enhanced Supplement

3.2E AWARENESS AND TRAINING
Enhanced Security Requirements

3.2.4E Provide awareness training focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training at least annually or when there are significant changes to the threat.

3.2.5E Include practical exercises in awareness training that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.

Supplemental Guidance for awareness and training requirements to controls in [Appendix F].
Basic and derived requirements for awareness and training are contained in [SP 800-171].

As a broader topic, and one that will ultimately involve NIST and other federal offices, AIA would like to understand the acquisition procedures, communications, and training as well as the risk criteria, control prioritization, and probable decision-making process aligned with the procuring activities' execution of 800-171B. To this end, due to the complexity and cost associated with 800-171B, there should be a phase-in period provided similar to the approach DOD ultimately took with implementation of the 800-171 controls. Additionally, new requirements should not be imposed immediately upon publication of 800-171B.

AIA and its member companies are committed to initiatives that secure information from cyber threats and we continually work to encourage collaboration between industry and government on cybersecurity matters to include innovation, agility, and flexibility across all businesses and government entities supporting national and international missions.

Thank you for the opportunity to provide these comments and concerns. Specific 800-171B control comments can be found in the accompanying comment template designated by line numbers.

Sincerely,

Jason Timm
Assistant Vice President, National Security Policy

^ Required Field
*Type: E - Editorial, G - General T - Technical

Please submit responses to:
sec-cert@nist.gov by Aug 2, 2019

Comment Template for
Initial Public Draft NIST SP 800-171B

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
1	AIA	J. Timm	E & G	Cover	NA **Rename NIST 800-171B to NIST 800-171E**	NA **Rename NIST 800-171B to NIST 800-171E**	Publication/Text Box	Clarity	**Rename NIST 800-171B to NIST 800-171E** Recommend the 33 controls for each 3.x.x followed by sequential numbering as per the current specification of Basic Security Requirements and Derived Security Requirements. Criteria for supplementing the basic and derived should be added to include the definitions for critical program
2	AIA	J. Timm	G	i	28	29	Authority	800-171B has mappings to unpublished 800-53 requirements, undefined terms (eg critical program), and 30 guidance references.	Develop and maintain a site with NIST strategy and estimated timelines for 800 series publications in order to ensure mappings align and are available. Add the site link in addition to the list of available publications
3	AIA	J. Timm	E & G	ii	63	65	Abstract	The designation of critical program is undefined and the use of "or" enlists one or the other of the cases.	Clarification of "*The enhanced requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components when the designated CUI is contained in a critical program or high value asset.* "

All public comments received will be posted at https://csrc.nist.gov/projects/protecting-cui/public-comments and https://www.regulations.gov docket number NIST-2019-0002 without change or redaction

Comment Template for
Initial Public Draft NIST SP 800-171B

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
4	AIA	J. Timm	E & G	ii	70	74	Keywords	Add keywords of significance	Add Critical Program, High Value Asset, and NIST Special Publication 800-171
5	AIA	J. Timm	T	iv	111	114	Notes to Reviewers	The designation of critical program is undefined	Clarification of *"The enhanced security requirements are not required for any particular category or article of CUI, rather are focused on designated high value assets or critical programs that contain CUI."*
6	AIA	J. Timm	E & G	iv	116	119	Notes to Reviewers	The designation of critical program is undefined and the use of "or" enlists one or the other of the cases.	Clarification of "*The enhanced requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components when the designated CUI is contained in a critical program or high value asset.* "
7	AIA	J. Timm	G	iv	120	123	Notes to Reviewers	NIST should be mandated to follow an adjudication process to include abritration for control implementation methods	Add a security control adjudication process. Add schedules, timeline estimates, and general strategy for cybersecurity related special publications to allow nonfederal entities to plan and estimate as a result of NIST controls being specified thru contractual requirements; consider the contractual process as to abritration upon cybersecurity controls related to Govt audits and specified maturity levels .

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
8	AIA	J. Timm	E & G	1	191	210	ALL CHAPTERS; all footnotes, references, and glossary	For continuity and clarity definitions, references, and footnotes should include the authoritative source for all federal agencies and checked for latest version and numbering. With the pending NARA FAR CUI and the DFARS 252.204-7012 the NIST 800-171 publication is a specification for requirements in nonfederal contractual terms.	Use definitions with uniformity; consider contractual federal sources (e.g. information systems [xx CFR § xxx.xxx], in footnote, and/or Glossary)
9	AIA	J. Timm		6	339	340	2.2 ORGANIZATION OF ENHANCED SECURITY REQUIREMENTS	Clarity	Move the discussion section to an Appendix in order to enforce the intent of the text *"The discussion section is not intended to extend the scope of the requirements."*
10	AIA	J. Timm	T	12	471	472	3.1 ACCESS CONTROL 3.1.1e	Expands beyond confidentiality and APT. Concern with delay in executing critical privileged actions, such as issuing patches	Delete 3.1.1e
11	AIA	J. Timm	T	12	474	482	3.1 ACCESS CONTROL 3.1.1e DISCUSSION	Add more examples and/or scenarios for the operational state for two person rule	Delete 3.1.1e or edit to specify - *Employ dual authorization or control processes for organizational critical or sensitive system operations*
12	AIA	J. Timm	T	12	483	484	3.1 ACCESS CONTROL 3.1.2e	Scenarios related to collaboration solutions, mobile devices, cloud services, etc	Edit 3.1.2e for clarity to specify - *Restrict access to systems and system components to only those information resources that are owned, provisioned, issued, or evaluated and approved by the organization* .
13	AIA	J. Timm	T	12	485	490	3.1 ACCESS CONTROL 3.1.2e DISCUSSION	Scenarios related to collaboration solutions, mobile devices, cloud services, etc	Edit for clarity Move the discussion section to an Appendix

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
14	AIA	J. Timm	T	12	491	492	3.1 ACCESS CONTROL 3.1.3e	Scenarios related to Cross company collaboration and engineering; Partnerships and Subcontractors	Edit 3.1.3e for clarity to specify - *Employ information transfer solutions to control information flows on connected systems.*
15	AIA	J. Timm	T	12 & 13	493	518	3.1 ACCESS CONTROL 3.1.3e DISCUSSION	Scenarios related to Cross company collaboration and engineering; Partnerships and Subcontractors	Edit for clarity Move the discussion section to an Appendix
16	AIA	J. Timm	T	14	522	524	3.2 AWARENESS AND TRAINING3.2.1e	Similar to 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. and 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Delete 3.2.1e
17	AIA	J. Timm	T	14	525	537	3.2 AWARENESS AND TRAINING 3.2.1e DISCUSSION	Similar to 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. and 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Delete
18	AIA	J. Timm	T	14	538	539	3.2 AWARENESS AND TRAINING 3.2.2e	Similar to 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. and 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Delete 3.2.2e Move the discussion section to an Appendix
19	AIA	J. Timm	T	14	540	549	3.2 AWARENESS AND TRAINING 3.2.2e DISCUSSION	Similar to 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. and 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Delete

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
20	AIA	J. Timm	T	16	557	558	3.4 CONFIGURATION MANAGEMENT 3.4.1e	Similiar to 800-171 Revision 2 Security Requirements 3.4.1 and 3.4.3? 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems.	Delete 3.4.1e
21	AIA	J. Timm	T	16	559	572	3.4 CONFIGURATION MANAGEMENT 3.4.1e DISCUSSION	Similiar to 800-171 Revision 2 Security Requirements 3.4.1 and 3.4.3? 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems.	Delete
22	AIA	J. Timm	T	16	573	575	3.4 CONFIGURATION MANAGEMENT 3.4.2e	Risk analysis on configurations; e.g., automated processes aren't always compatible with network architecture, manual processes can be more flexible and thus effective than automated ones, etc.	Edit 3.4.2e for clarity to specify - 3.4.2e Employ automated mechanisms and/or organizational processes to detect the presence of misconfigured or unauthorized system components and implement procedures that allow for patching, re-configuration, and/or other mitigations.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
23	AIA	J. Timm	T	16	576	588	3.4 CONFIGURATION MANAGEMENT 3.4.2e DISCUSSION	Risk analysis on configurations	Edit for clarity Move the discussion section to an Appendix
24	AIA	J. Timm	T	16	589	590	3.4 CONFIGURATION MANAGEMENT 3.4.3e	Similiar to 800-171 Revision 2 Security Requirements 3.4.1 and 3.4.3? 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems.	Edit 3.4.3e for clarity to specify - 3.4.3e Employ discovery and management tools and/or organizational processes to maintain an inventory of system components.
25	AIA	J. Timm	T	16 & 17	591	603	3.4 CONFIGURATION MANAGEMENT 3.4.3e DISCUSSION	Similiar to 800-171 Revision 2 Security Requirements 3.4.1 and 3.4.3? 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems.	Edit for clarity Move the discussion section to an Appendix Rename Discussion sections to Supplemental Guidance sections.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
26	AIA	J. Timm	T	18	607	609	3.5 IDENTIFICATION AND AUTHENTICATION 3.5.1e	Similar to 800-171 Revision 2 Security Requirements 3.5.1 and 3.5.2? 3.5.1 Identify system users, processes acting on behalf of users, and devices 3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	Delete 3.5.1e
27	AIA	J. Timm	T	18	610	620	3.5 IDENTIFICATION AND AUTHENTICATION 3.5.1e DISCUSSION	Similar to 800-171 Revision 2 Security Requirements 3.5.1 and 3.5.2? 3.5.1 Identify system users, processes acting on behalf of users, and devices 3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	Delete
28	AIA	J. Timm	T	18	621	623	3.5 IDENTIFICATION AND AUTHENTICATION 3.5.2e	Similar to 800-171 Revision 2 Security Requirements 3.5.1 and 3.5.2? 3.5.1 Identify system users, processes acting on behalf of users, and devices 3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	Delete 3.5.2e
29	AIA	J. Timm	T	18	624	640	3.5 IDENTIFICATION AND AUTHENTICATION 3.5.2e DISCUSSION	Similar to 800-171 Revision 2 Security Requirements 3.5.1 and 3.5.2? 3.5.1 Identify system users, processes acting on behalf of users, and devices 3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	Delete

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
30	AIA	J. Timm	T	18	641	643	3.5 IDENTIFICATION AND AUTHENTICATION 3.5.3e	Similar to the NIST 800-171 Revision 2 requirements in the 3.14 SYSTEM AND INFORMATION INTEGRITY Family.	Delete 3.5.3e
31	AIA	J. Timm	T	18 & 19	644	655	3.5 IDENTIFICATION AND AUTHENTICATION 3.5.3e DISCUSSION	Similar to the NIST 800-171 Revision 2 requirements in the 3.14 SYSTEM AND INFORMATION INTEGRITY Family.	Delete
32	AIA	J. Timm	T	20	659	659	3.6 INCIDENT RESPONSE 3.6.1e	Technical criteria for full-time or situational awareness.	Delete or Edit 3.6.1e for clarity to specify - Establish and maintain situational awareness capabilities managed by a organizationally defined security operations center
33	AIA	J. Timm	T	20	660	677	3.6 INCIDENT RESPONSE 3.6.1e DISCUSSION	Technical criteria for full-time or situational awareness.	Delete
34	AIA	J. Timm	T	20	678	679	3.6 INCIDENT RESPONSE 3.6.2e	Does the specification support physical on site or available to respond within 24 hours.	Edit 3.6.2e for clarity to specify - 3.6.2e Establish and maintain a cyber incident response team that can handle incidents identified by the organization within 24 hours.
35	AIA	J. Timm	T	20	680	695	3.6 INCIDENT RESPONSE 3.6.2e DISCUSSION	Recommend additional scenarios be added.	Edit for clarity Move the discussion section to an Appendix
36	AIA	J. Timm	T	23	707	708	3.9 PERSONNEL SECURITY 3.9.1e	Similar to NIST 800-171 Revision 2 requirement Add periodic re-evaluation to 3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.	Delete or Edit 3.9.1e for clarity to specify - 3.9.1e Establish and maintain an organizationally defined personnel screening (vetting) process for trustworthiness, reassessment, and adverse reporting of individuals with access to critical program(s) or high value asset(s).
37	AIA	J. Timm	T	23	709	722	3.9 PERSONNEL SECURITY 3.9.1e DISCUSSION	Similar to NIST 800-171 Revision 2 requirement Add periodic re-evaluation to 3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.	Delete or Edit for clarity Move the discussion section to an Appendix

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
38	AIA	J. Timm	T	23	723	724	3.9 PERSONNEL SECURITY 3.9.2e	Criteria not specified for adverse information Add adverse reporting to 3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.	Delete with Edit to 3.9.1e for clarity to specify - 3.9.1e Establish and maintain an organizationally defined personnel screening (vetting) process for trustworthiness, reassessment, and adverse reporting of individuals with access to critical program(s) or high value asset(s).
39	AIA	J. Timm	T	23	725	729	3.9 PERSONNEL SECURITY 3.9.2e DISCUSSION	Criteria not specified for adverse information Add adverse reporting to 3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.	Delete or Edit for clarity Move the discussion section to an Appendix
40	AIA	J. Timm	T	25	737	739	3.11 RISK ASSESSMENT 3.11.1e	Add scenarios related to the threat intelligence and threat hunting criteria	Edit 3.11.1e for clarity to specify - 3.11.1e Employ threat intelligence to inform the risk asssessment for the development of system and security architectures, selection of security controls, and monitoring for remediation
41	AIA	J. Timm	T	25	740	749	3.11 RISK ASSESSMENT 3.11.1e DISCUSSION	Add scenarios related to the threat intelligence and threat hunting criteria	Edit for clarity Move the discussion section to an Appendix
42	AIA	J. Timm	T	25	750	751	3.11 RISK ASSESSMENT 3.11.2e	The cyber threat hunting reference is more specific to the Incident Response (IR) family of NIST 800-171B	For clarity move requirement 3.11.2e to the Incident Response Family
43	AIA	J. Timm	T	25	752	771	3.11 RISK ASSESSMENT 3.11.2e DISCUSSION	The cyber threat hunting reference is more specific to the Incident Response (IR) family of NIST 800-171B	Edit for clarity and move to the Incident Response IR Family Move the discussion section to an Appendix

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
44	AIA	J. Timm	T	25	772	773	3.11 RISK ASSESSMENT 3.11.3e	Add scenarios on advanced automation and predictive analytics criteria. The automation and analytics references are more specific to the Incident Response (IR) family of NIST 800-171B	For clarity move requirement 3.11.3e to the Incident Response Family
45	AIA	J. Timm	T	25 & 26	774	786	3.11 RISK ASSESSMENT 3.11.3e DISCUSSION	Add scenarios on advanced automation and predictive analytics criteria. The automation and analytics references are more specific to the Incident Response (IR) family of NIST 800-171B	Edit for clarity and move to the Incident Response IR Family Move the discussion section to an Appendix
46	AIA	J. Timm	T	26	787	789	3.11 RISK ASSESSMENT 3.11.4e	System Security Plan requirement in NIST 800-171 Revision 2 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	Delete 3.11.4e
47	AIA	J. Timm	T	26	790	804	3.11 RISK ASSESSMENT 3.11.4e DISCUSSION	Redundant to System Security Plan requirement in NIST 800-171 Revision 2 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	Delete

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
48	AIA	J. Timm	T	26	805	806	3.11 RISK ASSESSMENT 3.11.5e	Similar to 3.11.1e as to assessment without the time specification	Delete 3.11.5e and Edit 3.11.1e for clarity to specify annually - 3.11.1e Employ threat intelligence to inform the risk asssessment for the development of system and security architectures, selection of security controls, and monitoring for remediation annually
49	AIA	J. Timm	T	26	807	815	3.11 RISK ASSESSMENT 3.11.5e DISCUSSION	Similar to 3.11.1e as to assessment without the time specification	Delete
50	AIA	J. Timm	T	26	816	816	3.11 RISK ASSESSMENT 3.11.6e	Redundant to System Security Plan requirement in NIST 800-171 Revision 2 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	Delete 3.11.6e or clarify to specify - 3.11.6e Assess supply chain risks to inform risk asssessment for applicable organizational systems
51	AIA	J. Timm					3.11 RISK ASSESSMENT 3.11.6e DISCUSSION	Redundant to System Security Plan requirement in NIST 800-171 Revision 2 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	Delete

Comment Template for
Initial Public Draft NIST SP 800-171B

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
52	AIA	J. Timm	T	27	828	829	3.11 RISK ASSESSMENT 3.11.7e	Redundant to System Security Plan requirement in NIST 800-171 Revision 2 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	Delete 3.11.7e
53	AIA	J. Timm	T	27	830	845	3.11 RISK ASSESSMENT 3.11.7e DISCUSSION	Redundant to System Security Plan requirement in NIST 800-171 Revision 2 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	Delete
54	AIA	J. Timm	T	28	849	850	3.12 SECURITY ASSESSMENT 3.12.1e	Add scenarios for penetration testing by moving the techniques (e.g. scanning tools, ad hoc tests, human experts) to the discussion section	Edit 3.12.1e for clarity to specify - 3.12.1e Conduct organizationally defined penetration testing simulating network and system attacks threat intel at least annually for critical programs or high value assets.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
55	AIA	J. Timm	T	28	851	873	3.12 SECURITY ASSESSMENT 3.12.1e DISCUSSION	Add scenarios for penetration testing by moving the techniques (e.g. scanning tools, ad hoc tests, human experts) to the discussion section	Recommend review to align the requirement with the discussion by adding scenarios on penetration testing to include but not limited to 3rd party services and the associated requirements for penetration testing services. Move the discussion section to an Appendix
56	AIA	J. Timm	T	29	877	877	3.13 SYSTEM AND COMMUNITCATION PROTECTION 3.13.1e	Review the benefits and risks of diverse systems and APT Review malicious code propagation techniques for inclusion as a risk factor in control families 3.11 Risk Assessment or 3.14 System and Information Integrity	Delete 3.13.1e
57	AIA	J. Timm	T	29	878	909	3.13 SYSTEM AND COMMUNITCATION	Review the benefits and risks of diverse systems and APT	Delete
58	AIA	J. Timm	T	29	910	911	3.13 SYSTEM AND COMMUNITCATION PROTECTION 3.13.2e	Review the control for specification	Delete 3.13.2e Review techniques in relationship to the risk analysis of attack surfaces of organizational systems thru control families 3.11 Risk Assessment
59	AIA	J. Timm	T	29 & 30	912	955	3.13 SYSTEM AND COMMUNITCATION	Review the control for specification	Delete

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
60	AIA	J. Timm	T	30	956	957	3.13 SYSTEM AND COMMUNITCATION PROTECTION 3.13.3e	Review the control for specification. High risk to manufacturing and operational environments by contractors and subcontractors	Delete 3.13.3e
61	AIA	J. Timm	T	30 & 31	958	975	3.13 SYSTEM AND COMMUNITCATION PROTECTION 3.13.3e DISCUSSION	Review the control for specification. High risk to manufacturing and operational environments by contractors and subcontractors	Delete
62	AIA	J. Timm	T	31	976	976	3.13 SYSTEM AND COMMUNITCATION PROTECTION 3.13.4e	Add scenarios related to isolation criteria for individual contracts.	Delete, Review isolation techniques for inclusion as a risk mitigation in control family 3.11 Risk Assessment, or Edit 3.13.4e for clarity to specify - 3.13.4e Employ organizational defined physical or logical isolation in the system architecture
63	AIA	J. Timm	T	31	977	1015	3.13 SYSTEM AND COMMUNITCATION PROTECTION 3.13.4e DISCUSSION	Add scenarios related to isolation criteria for individual contracts. Data segregation or network segmentation will be required on a individual contract basis	Delete

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
64	AIA	J. Timm	T	33	1020	1021	3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.1e	Add scenarios related to integrity criteria and security critical or essential software.	Review integrity techniques for inclusion as a risk mitigation in control family 3.11 Risk Assessment or Edit 3.14.1e for clarity to specify - 3.14.1e Define procedures for integrity verification on software organizationally defined as security critical or essential.
65	AIA	J. Timm	T	33	1022	1044	3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.1e DISCUSSION	Add scenarios related to integrity criteria and security critical or essential software.	Provide context regarding guidance of FIPS 140-2, FIPS 180-4, FIPS 202, FIPS 186-4, SP 800-147, and NIST TRUST Move the discussion section to an Appendix
66	AIA	J. Timm	T	33	1045	1046	3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.2e	Relocate to the appropriate control families based on monitoring not integrity	Delete 3.14.2e or Edit 3.6.1e for clarity to specify - Establish and maintain situational awareness capabilities managed by a organizationally defined security operations center
67	AIA	J. Timm	T	33 & 34	1047	1067	3.14 SYSTEM AND INFORMATION INTEGRITY 3.41.2e DISCUSSION	Relocate to the appropriate control families based on monitoring not integrity	Delete
68	AIA	J. Timm	T	34	1068	1070	3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.3e	Risks associated with the controls should be assessed with capabilities across operational environments.	Edit 3.14.3e for clarity to specify segregation over isolation - Ensure that Internet of Things (IoT), Operational Technology (OT), and Industrial Internet of Things (IIoT) systems, components, and devices are compliant with the security requirements imposed on organizational systems or are segregated in purpose-specific networks.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
69	AIA	J. Timm	T	34	1071		3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.3e DISCUSSION	Risks associated with the controls should be assessed with capabilities across operational environments.	Recommend review to align the requirement with the discussion by adding scenarios on segretation. Move the discussion section to an Appendix
70	AIA	J. Timm	T	34	1104	1105	3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.4e	Risks associated with the controls should be assessed with capabilities across operational environments.	Delete 3.14.4e Review techniques in relationship to the risk analysis of attack surfaces of organizational systems thru control families 3.11 Risk Assessment
71	AIA	J. Timm	T	34 & 35	1106	1136	3.14 SYSTEM AND INFORMATION INTEGRITY	Reimaging information is specific as to twice annually .	Delete
72	AIA	J. Timm	T	35	1137	1138	3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.5e	Review control family 3.8 for media protection and CUI	Delete 3.14.5e and review NIST 800-171 for potential edits for clarity to specify - 3.8.3 Sanitize or destroy system media containing CUI before disposal, release for reuse, and purge.
73	AIA	J. Timm	T	35	1139	1151	3.14 SYSTEM AND INFORMATION INTEGRITY	Review control family 3.8 for media protection and CUI	Delete
74	AIA	J. Timm	T	35	1152	1154	3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.6e	Similar to Incident Response and Security Operations Center specified in the Incident Response (IR) family of NIST 800-171B	Edit for clarity and move 3.14.6e to the Incident Response IR Family Similiarities to 3.11.1e for potential consolidation - 3.11.1e Employ threat intelligence to inform the risk asssessment for the development of system and security architectures, selection of security controls, and monitoring for remediation
75	AIA	J. Timm	T	35 & 36	1155	1167	3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.6e DISCUSSION	Discussion references threat intelligence and Security Operations Centers (SOC)	Edit for clarity and move to the Incident Response IR Family. Move the discussion section to an Appendix