August 2, 2019

National Institute of Standards and Technology
ITL - Computer Security Division
Attn: Ron Ross and Victoria Pillitteri
100 Bureau Drive, M/S 8930
Gaithersburg, MD 20899-8930

RE: Response to NIST's Request for Public Comment on SP 800-171B, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets (NIST-2019-0002)

Dr. Ross and Ms. Pillitteri,

Johns Hopkins Applied Physics Laboratory (JHU/APL) formally provides the attached response to NIST SP 800-171B on behalf of the collective members of the Federally Funded Research and Development Centers (FFRDC) InfoSec Collaborative. The FFRDC InfoSec Collaborative was founded in 2010 to share knowledge and collaborate on the unique cybersecurity threats and challenges faced by universities and research and development organizations supporting the DoD and other government agencies. The membership of the Collaborative includes Information Security professionals from FFRDCs and Navy University Affiliated Research Centers to include: JHU/APL, MITRE Corporation, The Aerospace Corporation, Institute for Defense Analysis (IDA), The Charles Stark Draper Laboratory (Draper), MIT Lincoln Laboratory, Jet Propulsion Lab (JPL), Carnegie Mellon Software Engineering Institute (SEI), RAND Corporation, University of Washington Applied Physics Laboratory (UW/APL), Applied Research Laboratories The University of Texas Austin (ARL/UT), University of Hawaii Applied Research Laboratory (UH/ARL), Penn State Applied Research Laboratory (PS/ARL), Center for Naval Analysis (CNA), and Space Dynamics Laboratory. It is important to note that while the Information Security staff who participate in the Collaborative provide this collective response, each organization may independently provide additional responses which may be (a) additional content beyond what the Collaborative team members developed and / or (b) from members within those organizations who are not represented by members of the Collaborative.

The FFRDC Information Security Collaborative is comprised of experts in information technology architecture design, engineering and operations; offensive and defensive cybersecurity; compliance and governance. This expertise crosses classified and unclassified domains. Members meet on a quarterly basis to discuss topics such as strategy, advanced persistent threats, organizational tools and capabilities, lessons learned, next generation architecture designs for emerging technologies, and so on. Occasionally external organizations are invited to attend these meetings to meet with the Collaborative to present Threat Intel (eg, DSS, NCIS, FBI, etc.), regulatory changes (eg, a representative from DoD CIO to discuss NIST 800-171), and vendor solutions (eg, Splunk, Microsoft, Google). The same members of this Collaborative worked together to collaborate on the implementation and challenges associated with DFARS 252.204-7012 and NIST SP 800-171, Rev 1 and Rev 2. As such, the attached responses to NIST 800-171B factor in this expertise and past lessons learned from other regulatory changes.

The FFRDC InfoSec Collaborative recognizes and appreciates the challenges to protect Controlled Unclassified Information (CUI). We commend NIST for intentionally creating a separate document called NIST 800-171B instead of making the enhanced security requirements part of an appendix within NIST 800-171. While NIST SP 800-171B was written specifically to protect a small number of contractors involved in the development or protection of High Valued Assets (HVA) and / or Critical Program Information (CPI). According to NIST's "Request for Comment on Draft NIST SP 800-171B and DoD Cost Estimate" publication, retrieved on July 15, 2019, "estimates ... the number of contractors that develop DoD's most critical capabilities …would affect less than one-half of one per cent of an overall contractor base of over 69,000." We are, however, concerned these requirements will be added more broadly by Contracting Officers who do not understand this applicability. For example, following the September 28, 2018 Navy memorandum "Implementation of Enhanced Security Controls on Select Defense Industrial Base Partner Networks" numerous DoD contractors reported seeing language from this memorandum copied and pasted directly into DD254s. If requirements from NIST SP 800-171B are added to contracts for basic CUI on an enterprise network, the operational and cost impact would be significant.

The FFRDC InfoSec Collaborative urges NIST to:

- re-write or eliminate requirements which are academic in nature with no practical affordable means to implement: 3.1.1.e, 3.13.2.e, 3.13.3e, 3.13.4e.
- re-write / clarify requirements which are nebulous and subjective, without a means to assess proper implementation to include: 3.11.2.e, 3.11.3e, 3.11.6e, 3.13.1e.
- provide opportunity to comment on revisions to NIST SP 800-171B
- require training for DoD Contracting Officers to properly recognize when to apply this language
- continue to underscore the costs to meet these requirements can be significant; government programs will need to plan for those increased costs
- require training for compliance assessing organizations to enable fair and consistent results
- publish a list (classified or unclassified but accessible by members of industry) of programs / contracts deemed Critical Program Information (CPI) or High Value Assets (HVA)
- before final publication, produce an assessment guide similar to NIST 800-171A

Sincerely,

Dawn Greenman
on behalf of the FFRDC InfoSec Collaborative
Deputy Program Manager Cybersecurity
Johns Hopkins Applied Physics Laboratory (JHU/APL)

cc: FFRDC InfoSec Collaborative Members from:

- Applied Research Laboratories at The University of Texas Austin (ARL/UT)
- Carnegie Mellon Software Engineering Institute (SEI)
- Center for Naval Analysis (CNA)
- Institute for Defense Analysis (IDA)
- Jet Propulsion Lab (JPL)
- Johns Hopkins Applied Physics Laboratory (JHU/APL)
- MIT Lincoln Laboratory
- MITRE Corporation
- Penn State Applied Research Laboratory (PS/ARL)
- RAND Corporation
- Space Dynamics Laboratory
- The Aerospace Corporation
- The Charles Stark Draper Laboratory (Draper)
- University of Hawaii Applied Research Laboratory (UH/ARL)
- University of Washington Applied Physics Laboratory (UW/APL)

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
General	All	800-171B as a whole	References	E, G	_All	All	All	In document, provide references which point to the select recommendations providing defense against the APT (provides validity these work to achieve outcome to defend against APT)	**See comment**	
General	All	Recommendations	Recommendation Selection Criteria	E, G, T	_All	All	All	Clarify intent: if two or more requirements have the same effect on an adversary (e.g., both contain the adversary at same stage in kill chain) then is it not logical to require both.	**See comment**	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by:			Dawn Greenman on behalf of FFRDC InfoSec Collaborative					Date Submitted:	8/2/19	
Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
Requirements	All	All	Requirement rationale / risk acceptance	E, G	_All	All	All	No information is provided regarding whether the requirements are complementary or redundant; if two or more requirements have the same effect on an adversary (e.g., both contain the adversary at same stage in kill chain) then is it not logical to require both.	See comment	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
Requirements	All	All	Applicability and requirement rationale / risk acceptance	E, G	_All	All	All	There is no evidence regarding the effectiveness of the requirements against the Advanced Persistent Threat. As such, requiring a Contracting Officer to identify all requirements should be implemented, it is proposed there is a risk based discussion with the organization to determine which of the requirements should be implemented based on a risk based analysis regarding the network configuration and criticality of the HVA / CPI data.	See comment	
General	All	Purpose and applicability	Applicability	E, G	_All	All	All	Clarify and justify the need for 800-171B in general, given that DoD and federal agencies can already specify additional security requirements through existing contractual mechanisms.	See comment	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
General	All	800-171B as a whole	Data Definition of HVA, CPI, CUI, CDI and Training	G	_All	N/A	N/A	Government needs to define what CUI / CDI is and finish the training program so contracting officers know and disclose what data needs to be protected.	See comment	Implement training to Program Officers; Update NARA CUI Registry
General	All	800-171B as a whole	Charge Back for Cybersecurity Costs	G	_All	N/A	N/A	Is there a mechanism to do chargebacks for the cyber costs?	See comment	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
General	All	800-171B as a whole	Requirement / Recommendation Language	E, G, T	_All	N/A	N/A	Write ALL recommendations / controls in condensed version in human legible language. Because they cannot be secure, we want them secure or isolated. Add an "intent" statement. They could also use a statement about the threat you are defending against so we can factor this into our RMF analysis (not the degree of risk but what kind of risk this is to solve). If you were to propose an equally effective control – need to know it is effective against what threat?	See comment	
General	All	800-171B as a whole	Cybersecurity Maturity Model Certification (CMMC) potential collision	G	_All	N/A	N/A	CMMC is coming out soon; please defer this document and the FAR until CMMC is released to avoid confusion.	Avoid implementing such an impactful change with CMMC on the horizon.	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
Cover Page	All	All	APT Behavior and Evidence of Defense	E, G	1	Cover Page	Cover Page	Considering NIST SP 800-171B is a set of recommended ***requirements*** versus guidelines there are limited published agreed upon practices for dealing with an Advanced Persistent Threat (APT) which changes tactics and techniques continuously. There are no citied references which provide evidence the requirements do in fact provide effective defense against this ever changing adversary.	Produce evidence these requirements provide defense against APT, especially given the costs to implement. How will changing adversary techniques be addressed?	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
General	All	800-171B as a whole	Intent: Clarify: "The enhanced recommendations apply only to the components of nonfederal systems that process, store, or transmit CUI contained in a critical program or high value asset or that provide protection for such components."	E, G	6	116	119	Explicitly word document to prevent contracting officers from declaring all of its contractors supporting critical programs or high value assets to meet all requirements for all organizational systems and clarify the costs allowable under the contract. DoD contractors have seen contracting officers copy and paste language from Navy Memo dated Sept 28, 2018 and other documents unnecessarily.	**See comment**	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
General	All	Recommendations	Recommendation Selection Clarification: "The publication contains ***recommendations*** for enhanced security requirements to provide additional protection for Controlled Unclassified Information in nonfederal systems and organizations when such information is part of a critical program or a high value asset."	E, G	6	116	119	Clarify how recommendations are selected. Is a contracting officer to pick and choose from the list of recommendations in NIST 800-171B?	The publication contains ***recommendations to select from for*** enhanced security requirements to provide additional protection for Controlled Unclassified Information in nonfederal systems and organizations when such information is part of a critical program or a high value asset ***based upon XYZ criteria (or as defined in XYZ.***	
General	All	Data Definitions / Verifications	High Value Assets or Critical Program Information	E, G, T	6	116	119	Need single source of programs deemed: High Value Assets or Critical Program Information. Reference provided for High Value Assets which are DHS designations. No reference provided for DoD related Critical Program Information (CPI) designations	Publish and reference a list of applicable critical programs or high value assets to clarify what data and contracts are impacted.	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
General	All	Purpose and applicability	"provide federal agencies with recommended enhanced security requirements for protecting confidentiality of CUI..."	E, G, T	13	244	244	Reference to "federal agencies" is beyond DoD - are all agencies following 800-171 B?	See comment	
General	All	Purpose and applicability	"provide federal agencies with recommended enhanced security requirements for protecting confidentiality of CUI..."	E, G, T	13	244	244	Only confidentiality - then assumption is availability and integrity are not as important	See comment: expand definition to include "confidentiality and availability" if applicable.	
General	All	The Requirements	No footnote definition of "Critical Program Information" as seen with High Value Assets	E, G	13	Footnote 6	Footnote ?	Missing definition of Critical Program Information which is necessary to identify it.	Add footnote referencing definition and treatment of CPI.	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	Family	Control	Discussion	*Type: E - Editorial, G - General T - Technical	Page	Starting Line	Ending Line	Comment (Include rationale for comment)^	Suggested Change^	Recommended Solutions
General	All	Basic Assumptions	CUI Categorization	E, G	16	304	305	**Lines 304-5** state that additional protections may be necessary to protect CUI that may be targeted by an APT because it is part of an HVA or critical program. However, the fundamental assumption of the CUI program is that the “value” of the CUI is assigned by the category of the CUI, as determined by the appropriate federal body. There is not currently a designated CUI category which covers HVAs or critical programs. Therefore, it is not clear why or how the data that purportedly resides on non-federal systems as part of HVAs or critical programs is classified as needing this additional level of protection. Who decides this, and how is the classification level	See comment	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
Basic Assumptions	All	Basic Assumptions	CUI Categorization	E, G	16	320	322	***Lines 320-322*** state that organizations may “implement alternative, but equally effective, security measures to compensate for the inability to satisfy a requirement”, but there is a lack of discussion of risk-based decision making around compensating controls. How would an organization implement compensating controls with sufficient effectiveness, and how would such controls be effectively verified and validated?	See comment	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
Basic Assumptions	All	Basic Assumptions	Managed Service Providers	E, G	16	323	324	***Lines 323-324*** state that managed service providers are one way of satisfying security requirements. However, given the assumption in 800-171 and continuing through 800-171B that organizations maintain full control of their system and network boundaries, depending on the arrangement with the MSP, it would be difficult to fulfill these requirements in a distributed or cloud environment.	See comment	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
Basic Assumptions	All	All	Alternate but Equally Effective	E, G	17	320	320	*"Nonfederal organizations may not have the necessary organizational structure or resources to satisfy every security requirement and may implement alternative, but equally effective, security measures to compensate for the inability to satisfy a requirement"*	Clarify who approves Alternate But Equally Effective security measures. Is this a joint approval? Government and contractor agree? DoD CIO?	
The Requirements	All	Requirements	Footnote - Unsubstantiated reference to NTCTF	E, G	19	375 Footnote	375 Footnote	***Footnote 18, at line 375,*** states that "The enhanced security requirements have been designed to address the threats described in NTCTF" (the NSA technical cyber threat framework). However, this claim is not substantiated anywhere in the document.	Substantiate claim with evidence	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
The Requirements	All	Requirements	Footnote - Unsubstantiated reference to NTCTF	E, G	19	375 Footnote	375 Footnote	**Footnote 18, at line 375** **RE: NTCTF:** DoDcAR/GovCAR, which both use the NTCTF, assumes perfect implementation when assessing the effectiveness of controls against threat actions. Numerous audits and surveys indicate that organizations have a difficult enough time implementing the controls of 800-171, let alone perfectly. Requiring the enhanced controls of 800-171B might induce a false sense of safety or security effectiveness, if organizations and government sponsors are not vigilant about verifying the control implementations.	See comment	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
General	All	The Requirements	Footnote 17: Organizations are cautioned against applying the enhanced security requirements in this appendix to protect all CUI. The application of the requirements is restricted to critical programs and high value assets containing CUI that are likely to be targeted by the APT.	E, G, T	19	Footnote	Footnote	Need all contracting officers trained to understand this does not apply to all CUI data	See comment	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.1.1e	Access Control	Employ dual authorization to execute critical or sensitive system and organizational operations.	Dual authorization, also known as **two-person control,** reduces risk related to insider threat. **Dual authorization requires the approval of two authorized individuals to execute certain commands, actions, or functions.** For example, organizations employ dual authorization to help **ensure that changes** to selected system components (i.e., hardware, software, and firmware) or information **cannot occur unless two qualified individuals approve and implement such changes**. The two individuals possess the skills and expertise to determine if the proposed changes are correct implementations of the approved changes. The individuals are also accountable for the changes. **Organizations also employ dual authorization for the execution of privileged commands.** To reduce the risk of collusion, organizations **consider rotating dual authorization duties** to other individuals.	E, G, T	23	471	482	Clarifiying questions: - Is this requirement stating to do BOTH: --- Change Advisory Board expertise to APPROVE on all changes, and --- Have TWO qualified people IMPLEMENT the change? Appears to be two separate integrity controls. This appears to be beyond a CONFIDENTIALITY control. Define critical or sensitive system and organizational operations and explicitly when this requirement would be used. Provide examples to guide intent. Address outliers. How do you address changes that	See comment This requirement appears academic and nature with no practical affordable means to implement; recommend removing.	Is there a commercial application / tool that could address situations when only one person can make a change? Example: when making a change of an OS, is there a solution where User 1 enters a password for action then User 2 enters password to make the change?

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.1.2e	Access Control	**Restrict access** to systems and system components to only those information resources that are **owned, provisioned, or issued by the organization.**	Non-organizationally owned information resources include systems or system components owned by other organizations and personally owned devices. Non-organizational devices and software present a significant risk to the organization and complicate the organization's ability to employ a "comply-to-connect" policy or implement device attestation techniques to ensure the integrity of the organizational system.	E, G, T	23	483	490	Clarity: Discussion is vague: internet, cloud providers, CDS solutions, or other non-organizationally owned or provisioned networks could be included in this restriction including Government Furnished Equipment (GFE) The closest relevant SP800-53r5 control is AC-20(3) which has a more specific and broader set of exclusions. AC-20(3) is not required under any standard control baseline.	Consider revising to be more specific about scope to say that this is only relevant to 'system' components and not external systems. Should also include a provision for discussing BYOD or partner systems. - Does this prohibit personally owned device access eg from a home PC using Citrix to connect. - Third Party access – how to they have a 3rd party SOC that is not owned provisioned by me. - Does this prohibit cloud use?	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.1.3e	Access Control	Employ **secure information transfer solutions** to **control** information **flows** between security domains on connected systems.	Organizations employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between connected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services; provide a packet-filtering capability based on header information; or provide message-filtering capability based on message content. Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Transferring information between systems in different security domains	E, G, T	23	491	518	This is an extension of requirement from 171. What is the extent of the extension. Make it clear that it relates to this and what does it add to it. "Secure information transfer solutions" appears to really be the requirement – in addition to what is in 171. Start discussion with that. • Provide better definition of security domain • What does email mean in this control? If I *elect* to intentionally send an email to someone is intentional decision enough of a control or do we need more?		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.2.1e	Awareness and Training	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.	One of the most effective ways to detect APT activities and to reduce the effectiveness of those activities is to provide specific awareness training for individuals. A well-trained and security aware workforce provides another organizational safeguard that can be employed as part of a defense-in-depth strategy to protect organizations against malicious code injections via email or the web applications. Threat awareness training includes educating individuals on the various ways APTs can infiltrate into organizations including through websites, emails, advertisement pop-ups, articles, and social engineering. Training can include techniques for recognizing suspicious emails, the use of removable systems in non-secure settings, and the potential targeting of individuals by adversaries outside the workplace. Awareness training is assessed and updated periodically to ensure that the training is relevant	E	25	522	537	Who defines “when there are significant changes to the threat?”	Define who and how "significant changes" are announced which alerts to make then change. What artifacts are required?	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.2.2e	Awareness and Training	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.	Awareness training is most effective when it is complemented by practical exercises tailored to the tactics, techniques, and procedures (TTP) of the threat. Examples of practical exercises include no-notice social engineering attempts to gain unauthorized access, collect information, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links. Rapid feedback is essential to reinforce desired user behavior. Training results, especially failures of personnel in critical roles, can be indicative of a potential serious problem. It is important that senior management are made aware of such situations so that they can take appropriate remediating actions. [SP 800-181] provides guidance on role-based information security training in the workplace.	E	25	538	550	Concerns over this last sentence "It is important that senior management are made aware of such situations so that they can take appropriate remediating actions." Is this relevant? Assumption is Sr Managers are made aware. This is not a confidentiality control. If goal is to educate senior managers perhaps that is a different control: It is important that senior management are made aware of such situations so that they can take appropriate remediating actions.		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.3.0e	Audit and Accountability	N/A	There are no enhanced security requirements for audit and accountability at this time. Basic and derived requirements for audit and accountability are contained in [SP 800-171].	N/A	26	551	554	Develop an assessment guide similar to NIST 800-171A before releasing.	Recommend defining audit requirements for consistency	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.4.1e	Configuration Management	Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.	The establishment and maintenance of an authoritative source and repository includes a system component inventory of approved hardware, software and firmware; approved system baseline configurations and configuration changes; and verified system software and firmware, as well as images and/or scripts. See 3.4.1 and 3.4.3 related to system component inventories, baseline configurations, and configuration change control. The information in the repository is used to demonstrate adherence to or identify deviation from the established configuration baselines and to restore system components from a trusted source. From an automated assessment perspective, the system description provided by the authoritative source is referred to as the desired state. Using automated tools, the desired state is compared to the actual state to check for compliance or deviations.	E, G, T	27	557	572	- Automated comparison and set baseline is costly and a challenge. Clarity: - Does term "system components" include things like Ruby Gem or Python Module? Do you need MS patches cached locally? Is this a source code repository mirror? - Is this just operating systems or enterprise software? - How far down into the system do you go into the hardware and system components? - Is expectation to track firmware updates on all servers, computers and printers which process, store or come into contact with CUI / CDI data? - Define "trusted and authoritative source"		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.4.2e	Configuration Management	Employ automated mechanisms to detect the presence of misconfigured or unauthorized system components and remove the components or place the components in a quarantine or remediation network that allows for patching, re-configuration, or other mitigations.	System components used to process, store, transmit, or protect CUI are monitored and checked against the authoritative source (i.e., hardware and software inventory and associated baseline configurations). From an automated assessment perspective, the system description provided by the authoritative source is referred to as the desired state. Using automated tools, the desired state is compared to the actual state to check for compliance or deviations. System components that are unknown or that deviate from the approved configuration are removed from the system and rebuilt from the trusted configuration baseline established by the authoritative source. Automated security responses can include halting system functions, halting system processing, or issuing alerts or notifications to personnel when there is an unauthorized modification of an organization-defined configuration item.	E, G, T	27	573	588	• Sounds like this is automating the check of 3.4.1 and mitigating. How do you do this with hardware? Is this CMDB checks for hardware component changes? Clarity needed: • Is this control automatically detecting AND removing? - How far down into the system do you go into the hardware and system components? • How far in the weeds going for components • Suggest tools that would address this gap? Does NAC completely address? • Seems to go to almost to a Zero trust model or continuous monitoring and detecting. **Challenges** with systems		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.4.3e	Configuration Management	Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components.	The system component inventory includes system-specific information required for component accountability and to provide support to identify, control, monitor, and verify configuration items in accordance with the authoritative source. Information necessary for effective accountability of system components includes system name; hardware component owners; hardware inventory specifications; software license information; software component owners; version numbers; and for networked components, the machine names and network addresses. Inventory specifications include manufacturer; supplier information; component type; date of receipt; cost; model; serial number; and physical location. Organizations also use automated mechanisms to implement and maintain authoritative (i.e., up-to-date, complete, accurate, and available) baseline configurations for	E, G, T	27	589	604	**Clarity:** - How far down into the system do you go into the hardware and system components? - "Information necessary" and "inventory specifications" – must we record at least these things? - Define "Specifications" / Provide examples - Are we expanding in the requirement for 3.4.1 or just restating it?		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.5.1e	Identification and Authentication	Identify and authenticate systems and system components before establishing a network connection using bidirectional authentication that is cryptographically-based and replay resistant.	Cryptographically-based and replay resistant authentication between systems, components, and devices addresses the risk of unauthorized access from spoofing (i.e., claiming a false identity). The requirement applies to client-server authentication, server-server authentication, and device authentication (including mobile devices). The cryptographic key for authentication transactions is stored in suitably secure storage available to the authenticator application (e.g., keychain storage, Trusted Platform Module (TPM), Trusted Execution Environment (TEE), or secure element). For some architectures (e.g., service-oriented architectures), mandating authentication requirements at every connection point may not be practical and therefore, the authentication requirements may only be applied periodically or at the initial point of network connection.	E, G, T	29	607	620	Interpretation: • Assuming this is when 2 nodes connect talk to each other…. not necessarily when you connect a computer to a network. Example: NAC v2 with PKI, VPN Always On, IPSec Signatures for Domain Controllers Clarification Needed: Confirm this is beyond what is currently done at the NAC network level. Costly, operationally impactful.		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.5.2e	Identification and Authentication	Employ password managers for the generation, rotation, and management of passwords for systems and system components that do not support multifactor authentication or complex account management.	In situations where static passwords or personal identification numbers (PIN) are used (e.g., certain system components do not support multifactor authentication or complex account management such as separate system accounts for each user and logging), enterprise password managers can automatically generate, rotate, manage, and store strong and different passwords for users and device accounts. For example, a router might have one administrator account, but an enterprise typically has multiple network administrators. Thus, access management and accountability are problematic. An enterprise password manager uses techniques such as automated password rotation (in this example, for the router password) to allow a specific user to temporarily gain access to a device by checking out a temporary password and then checking the password back in to end the access.	E, G, T	29	625	640	Clarity Needed: - Current requirement is MFA to gain access to a system. This expands the defintion in 800-171 to MFA for all system components. - Define component? - Does this prohibit use of Single Single Sign On? - Does the password manager have to do the rotation? - Are single use passwords with automatic rotation the expectation or is this just an example? Are these one-time use passwords or passwords rotated on a set basis? What is the actual requirement?		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.5.3e	Identification and Authentication	Employ automated mechanisms to prohibit system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state, or in a trust profile.	Identification and authentication of system components and component configurations can be determined, for example, via a cryptographic hash of the component. This is also known as device attestation and known operating state or trust profile. A trust profile based on factors such as the user, authentication method, device type, and physical location is used to make dynamic decisions on authorizations to data of varying types. If device attestation is the means of identification and authentication, then it is important that patches and updates to the device are handled via a configuration management process such that the patches and updates are done securely and do not disrupt the identification and authentication to other devices. System components that are either unknown or in an unapproved state are placed in a quarantine or remediation network that allows for patching, configuration, or other	E, G, T	29	641	656	Clarification Needed: • Is this NAC, Landesk, SCCM, NAC with posture assessment? - Is this Zero Trust to avoid non-enterprise managed systems or a delegation of 'properly configured state'.		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by:		Dawn Greenman on behalf of FFRDC InfoSec Collaborative						Date Submitted:	8/2/19	
Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.6.1e	Incident Response	Establish and maintain a full-time security operations center capability.	A security operations center (SOC) is the focal point for security operations and computer network defense for an organization. The purpose of the SOC is to defend and monitor an organization's systems and networks (i.e., cyber infrastructure) on an ongoing basis. The SOC is also responsible for detecting, analyzing, and responding to cybersecurity incidents in a timely manner. The SOC is staffed with skilled technical and operational personnel (e.g., security analysts, incident response personnel, systems security engineers); operates 24 hours per day, seven days per week; and implements technical, management, and operational controls (including monitoring, scanning, and forensics tools) to monitor, fuse, correlate, analyze, and respond to threat and security-relevant event data from multiple sources. Sources include perimeter defenses, network devices (e.g., gateways, routers, switches) and	E, G, T	31	659	677	Clarity: • Contradicts 3.1.2 when applying a 3rd party SOC. - If an organization has a SOC which is staffed and operates under a model where staff are rotate an "on-call" after-hours to respond to critical incidents / alerts, is that good enough? Need description of acceptable implementations. - Is this SOC only for the environment where the CPI or HVA data exists vs SOC for entire enterprise? - Depending on implementation requirement, can be very costly.		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.6.2e	Incident Respons e	Establish and maintain a cyber incident response team that can be deployed to any location identified by the organization within 24 hours.	A cyber incident response team (CIRT) is a team of experts that assesses, documents, and responds to cyber incidents so that organizational systems can recover quickly and implement the necessary controls to avoid future incidents. CIRT personnel typically include forensic analysts, malicious code analysts, systems security engineers, and real-time operations personnel. The incident handling capability includes performing rapid forensic preservation of evidence and analysis of and response to intrusions. The team members may or may not be full-time but need to be available to respond in the time period required. The size and specialties of the team are based on known and anticipated threats. The team is typically pre-equipped with the software and hardware (e.g., forensic tools) necessary for rapid identification, quarantine, mitigation, and recovery, and is familiar with how to preserve evidence and maintain	E, G, T	31	678	695	Clarity: - Define "deploy" - can this be a process or technology running? - Must an staff be deployed to a physical location or can incident be addressed remotely. Example - a system image capture over the wire? If a system or harddrive is isolated, can it be "deployed" by being returned to the CIRT via US Mail / Overnight if a smaller incident to clean up rather than send people out? This in lieu of flying people out via an 8 hour flight, example. What is the incident definition criteria that rises to a need to deploy a human to an incident?		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	Family	Control	Discussion	*Type: E - Editorial, G - General T - Technical	Page	Starting Line	Ending Line	Comment (Include rationale for comment)^	Suggested Change^	Recommended Solutions
3.7.0e	Maintenance	N/A	There are no enhanced security requirements for maintenance at this time. Basic and derived requirements for maintenance are contained in [SP 800-171].	N/A	32	697	700	N/A		
3.8.0e	Media Protection	N/A	There are no enhanced security requirements for media protection at this time. Basic and derived requirements for maintenance are contained in [SP 800-171].	N/A	33	701	704	N/A		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	Family	Control	Discussion	*Type: E - Editorial, G - General T - Technical	Page	Starting Line	Ending Line	Comment (Include rationale for comment)^	Suggested Change^	Recommended Solutions
3.9.1e	Personnel Security	Conduct enhanced personnel screening (vetting) for individual trustworthiness and reassess individual trustworthiness on an ongoing basis.	Personnel security is the discipline that provides a trusted workforce based on an evaluation or assessment of conduct, integrity, judgment, loyalty, reliability and stability (e.g., trustworthiness). The extent of the vetting is commensurate with the level of risk that individuals could bring about by their position and access. For individuals accessing federal government facilities and systems, the federal government employs resources, information, and technology in its vetting processes, to ensure a trusted workforce. These vetting processes may be extended all or in part to persons accessing federal information including CUI resident in nonfederal systems and organizations through contractual vehicles or other agreements established between federal agencies and nonfederal organizations. Examples of enhanced personnel screening for security purposes	E, G, T	34	707	722	Clarity: - Define the specifications of the background check? It is intentionally vague? - Define frequency of "on going" - What determines compliance? How do you assess? What artifacts are required? - Is this specifically for staff working on HVA / CPI programs wiith this requirement in contracts or all staff? Concern: - DSS advised not to submit every person an org has for a background check for a clearance. Is this requiring a clearance for this data?		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.9.2e	Personnel Security	Ensure that organizational systems are protected whenever adverse information develops regarding the trustworthiness of individuals with access to CUI.	When adverse information develops which questions an individual's trustworthiness for continued access to systems containing CUI, actions are taken to protect the CUI while the information is resolved, or the individual is terminated or transferred to other duties that do not involve access to CUI.	E, G, T	34	723	730	Clarity: - How will this be assessed? - Who gets to define adverse information? - Is this the same information you would report for someone with a security clearance? (DD FM 398 Personnel Security Questionairre - PSQ)? - If you have an Insider Threat Program for unclassified network does that cover requirement? - Clarify that vetting needs to be elevated above the organizations current baseline.		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	Family	Control	Discussion	*Type: E - Editorial, G - General T - Technical	Page	Starting Line	Ending Line	Comment (Include rationale for comment)^	Suggested Change^	Recommended Solutions
3.10.	Physical Protection	N/A	There are no enhanced security requirements for physical protection at this time. Basic and derived requirements for maintenance are contained in [SP 800-171].	E, G, T	35	731	734	N/A		N/A

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.11.1e	Risk Assessment	Employ threat intelligence to inform the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.	The constantly changing and increased sophistication of adversaries, especially the advanced persistent threat (APT), makes it more likely that adversaries can successfully compromise or breach organizational systems. Accordingly, threat intelligence can be integrated into and inform each step of the risk management process throughout the system development life cycle. This includes defining system security requirements, developing system and security architectures, selecting security solutions, monitoring (including threat hunting) and remediation efforts. [SP 800-30] provides guidance on risk assessments. [SP 800-39] provides guidance on the risk management process. [SP 800-160-1] provides guidance on security architectures and systems security engineering. [SP 800-150] provides guidance on cyber threat information sharing.	E, G, T	36	735	749	Clarity: - From a compliance perspective, how would this be assessed. - Is this control stating this needs to be done for selecting vendors within the supply chain for tools an organization would purchase? If yes, provide examples for how this would be done.		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: Dawn Greenman on behalf of FFRDC InfoSec Collaborative Date Submitted: 8/2/19

Section	Family	Control	Discussion	*Type: E - Editorial, G - General T - Technical	Page	Starting Line	Ending Line	Comment (Include rationale for comment)^	Suggested Change^	Recommended Solutions
3.11.2e	Risk Assessment	Establish and maintain a cyber threat hunting capability to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls.	Threat hunting is an active means of cyber defense in contrast to the traditional protection measures such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandboxes, and Security Information and Event Management (SIEM) technologies and systems. Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. The objective is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses. Indicators of compromise are forensic artifacts from intrusions that are identified on organizational systems at the host or network level, and can include unusual network traffic, unusual file changes, and the presence of malicious code. Threat hunting teams use existing threat intelligence and may create new threat	E, G, T	36	750	771	Clarity: - Can Hunt team be an outsourced option? If yes, please provide as example. - How often do you need to perform threat hunting - What artifacts of evidence do you need to provide to prove threat hunting? Concern: High Cost especially for small business		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: Dawn Greenman on behalf of FFRDC InfoSec Collaborative Date Submitted: 8/2/19

Section	Family	Control	Discussion	*Type: E - Editorial, G - General T - Technical	Page	Starting Line	Ending Line	Comment (Include rationale for comment)^	Suggested Change^	Recommended Solutions
3.11.3e	Risk Assessment	Employ advanced automation and analytics capabilities to predict and identify risks to organizations, systems, or system components.	A properly resourced Security Operations Center (SOC) or Computer Incident Response Team (CIRT) may be overwhelmed by the volume of information generated by the proliferation of security tools and appliances unless it employs advanced automation and analytics to analyze the data. Advanced automation and predictive analytics capabilities are typically supported by artificial intelligence concepts and machine learning. Examples include Automated Workflow Operations, Automated Threat Discovery and Response (which includes broad-based collection, context-based analysis, and adaptive response capabilities), and Machine Assisted Decision tools. Note, however, that sophisticated adversaries may be able to extract information related to analytic parameters and retrain the machine learning to classify malicious activity as benign. Accordingly, machine learning is augmented by human	E, G, T	36	772	786	Clarity: - Does control explicitly require the use of artificial intelligence for compliance? Concern: High Cost		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.11.4e	Risk Assessment	Document or reference in the system security plan the risk basis for security solution selection and identify the system and security architecture, system components, boundary isolation or protection mechanism, and dependencies on external service providers.	System security plans relate security requirements to a set of security controls and solutions. The plans describe how the controls and solutions meet the security requirements, and, when the APT is a concern, includes traceability between threat and risk assessments and selection of a security solution, including discussion of any relevant analyses of alternatives and rationale for key security-relevant architectural and design decisions. This level of detail is important as the threat changes, requiring reassessment of the risk and the basis for previous security decisions. When incorporating external service providers into the system security plan, organizations state the type of service provided (e.g., software as a service, platform as a service), the point and type of connections (including ports and protocols), the nature and type of the information flows to and from the service	E, G, T	37	787	804	Clarity: - Is underlying requirement really RMF? - In discussion, reference to "Service Providers" – sounds like cloud service providers – is that the intent or can it be non-cloud providers? - Is requirement to explain the rationale behind why a security provider or tool is selected? - If a GRC tool is used, does that achieve intent? If, for example you selected an email solution do you need to explain rationale for every purchase.		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.11.5e	Risk Assessment	Assess the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence.	Since sophisticated threats such as the APT are constantly changing, the threat awareness and risk assessment of the organization is dynamic, continuous and informs the actual system operations, the security requirements for the system, and the security solutions employed to meet those requirements. Threat intelligence (i.e., threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes) is infused into risk assessment processes and information security operations of the organization to identify any changes required to address the dynamic threat environment. [SP 800-30] provides guidance on risk assessments, threat assessments, and risk analyses.		37	805	815	None		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.11.6e	Risk Assessment	Assess, respond to, and monitor supply chain risks associated with organizational systems.	Supply chain events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code. These events can have a significant impact on a system and its information and therefore, can also adversely impact organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. The supply chain-related events may be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required. [SP 800-30] provides guidance on risk assessments, threat assessments, and risk analyses. [SP 800-161]	E, G, T	37	816	827	Clarity: - References "**organizational systems**" - is this requirement beyond the systems housing HVA and CPI data defined in contract? - This alludes to cybersecurity or IT being responsible for supply chain risk management. - This may be very difficult. Government needs to provide briefings when there are issues with the supply chain based on intel received. This is not always transparent nor proactive. Purchasing / contracts offices need to be engaged in cybersecurity / intel discussions. - Does a GRC system, used	Define organizational systems.	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.11.7e	Risk Assessment	Develop and update as required, a plan for managing supply chain risks associated with organizational systems.	The growing dependence on products, systems, and services from external providers, along with the nature of the relationships with those providers, present an increasing level of risk to an organization. Threat actions that may increase risk include the insertion or use of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the supply chain. Supply chain risks can be endemic or systemic within a system element or component, a system, an organization, a sector, or the Nation. Managing supply chain risk is a complex, multifaceted undertaking requiring a coordinated effort across an organization building trust relationships and communicating with both internal and external stakeholders. Supply chain risk management (SCRM) activities involve identifying and assessing	E, G, T	38	828	846	Clarity: - Is requirement specific to the HVA / CPI program associated with the contract? - Is the expectation to create a supply chain department focused on this? Is this just a process to address 3.11.6e? Scope and depth both need to be defined. Concern: - High cost (potential) depending on scope and implementation		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.12.1e	Security Assessment	Conduct penetration testing at least annually, leveraging automated scanning tools and ad hoc tests using human experts.	Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is conducted by penetration testing agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application level security. Penetration testing can be used to validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include time, resources, and skills. Organizations may also supplement penetration testing with red team exercises. Red teams attempt to duplicate the actions of adversaries in carrying out attacks against organizations and provide an in-depth analysis of security-related	E, G, T	39	849	874	The last paragraph in the discussion says 'SP 800-53A provides guidance on conducting security assessments'. Paragraph 2 of Chapter 3 says that 'The enhanced requirements in Sections 3.1 through 3.14 are derived from the security controls in SP 800-53'. SP 800-171r2 Draft-IPD Section 2.2 says that 'The derived security requirements, which supplement the basic security requirements, are taken from the security controls in SP 800-53' from a moderate baseline. Further that these are tailored to remove uniquely federal requirements or other non-CUI based controls. However, without a specific mapping to applicable SP 800-53r5		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.13.1e	System and Communications Protection	Employ diverse system components to reduce the extent of malicious code propagation.	Organizations often use homogenous information technology environments to reduce costs and to simplify administration and use. But a homogenous environment can also facilitate the work of the APT, as it allows for common mode failures and the propagation of malicious code across identical system components (i.e., hardware, software, and firmware). In these environments, adversary tactics, techniques, and procedures (TTP) that work on one instantiation of a system component will work equally well on other identical instantiations of the component regardless of how many times such components are replicated or how far away they may be placed in the architecture. Increasing diversity within organizational systems reduces the impact of potential exploitations or compromises of specific technologies. Such diversity protects against common mode failures,	E, G, T	39	877	909	Clarity: - Requirement should state “when possible” or “where technically feasible” in the TITLE of the control. Needs to be based on a risk based decision. Requirement language: "Employee diverse system components..." sounds like a “Must statement” but it is optional or risk based based upon the discussion Discussion references "Orgnizations often use" -- this discussion should speak just to the critical systems impacted by this specific for HVA or CPI. Not for all organizational systems. A request was made to scrap this control. How	Where technically feasible and risk is high, employ diverse system components to reduce the extent of malicious code propagation.	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.13.2e	System and Communications Protection	Disrupt the attack surface of organizational systems and system components through unpredictability, moving target defense, or non-persistence.	Cyber-attacks by adversaries are predicated on the assumption of a certain degree of predictability and consistency regarding the attack surface. The attack surface is the set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, the system, system element, or environment. Changes to the attack surface reduce the predictability of the environment, making it difficult for adversaries to plan and carry out attacks and thus can cause the adversaries to make miscalculations that can either impact the overall effectiveness of the attacks or increase the observability of the attackers. Unpredictability can be achieved by making changes in seemingly random times or circumstances (e.g., by randomly shortening the time when the credentials are valid). Randomness introduces increased levels of	E, G, T	39	910	955	Clarity: - Confirm only required for contracts / networks containing HVA / CPI data. – where is the risk based decision on this. It could be detrimental to your program if not done really well. - How do you audit this? - How do you determine if it is effective. - How do you make this a requirement someone can comply. Discussion Concerns: - Uncertain these are feasible: "changing processing storage locations" language is concerning - concern about practicality.	"moving target" -- requirement should be "if technically feasible" This requirement appears academic in nature with no practical affordable means to implement; recommend removing or defining recommendations for how to achieve.	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.13.3e	System and Communications Protection	Employ technical and procedural means to confuse and mislead adversaries through a combination of misdirection, tainting, or disinformation.	Deception is used to confuse and mislead adversaries regarding the information the adversaries use for decision making; the value and authenticity of the information the adversaries attempt to exfiltrate; or the environment in which the adversaries desire to operate. Such actions can impede the adversary's ability to conduct meaningful reconnaissance of the targeted organization; delay or degrade an adversary's ability to move laterally through a system or from one system to another system; divert the adversary away from systems or system components containing CUI; and increase observability of the adversary to the defender, revealing the presence of the adversary along with its TTPs. Misdirection can be achieved through deception environments (e.g., deception nets) which provide virtual sandboxes into which malicious code can be diverted and adversary TTP can be safely examined. Tainting involves	E, G, T	41	956	975	Clarity: - Are you requiring honeypots? Could use internally to identify internal connection attempts to investigate. - Is this recommendation, if selected, mandating an enterprise program vs program specific requirement for HVA / CPI data? Concern: - High Cost - will need to have people write / create / monitor deceptive content. This is non-trivial and comes with a cost. Risk is doing more harm than good. Example: fake file planted to deceive, legitimate staff access deceptive content and use it for research not knowing	This requirement appears academic in nature with no practical affordable means to implement; recommend removing or defining recommendations for how to achieve.	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.13.4e	System and Communications Protection	Employ physical and logical isolation techniques in the system and security architecture.	Physical and logical isolation techniques applied at the architectural level of the system can limit the unauthorized flow of CUI; reduce the system attack surface; constrain the number of system components that must be highly secure; and impede the movement of an adversary. Physical and logical isolation techniques when implemented with managed interfaces, can isolate CUI into separate security domains where additional protections can be applied. Any communications across the managed interfaces (i.e., across security domains), constitutes remote access, even if the communications stay within the organization. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection	G	42	976	1015	This suggests the lateral movement restrictions of a firewall or other isolation technique.		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	Family	Control	Discussion	*Type: E - Editorial, G - General T - Technical	Page	Starting Line	Ending Line	Comment (Include rationale for comment)^	Suggested Change^	Recommended Solutions
3.14.1.e	System and Information Integrity	Employ roots of trust, formal verification, or cryptographic signatures to verify the integrity and correctness of security critical or essential software.	Verifying the integrity of the organization's security critical or essential software is an important capability as corrupted software is the primary attack vector used by adversaries to undermine or disrupt the proper functioning of organizational systems. There are many ways to verify software integrity and correctness throughout the system development life cycle. Root of trust mechanisms such as secure boot and trusted platform modules verify that only trusted code is executed during boot processes. This capability helps system components protect the integrity of boot firmware in organizational systems by verifying the integrity and authenticity of updates to the firmware prior to applying changes to the system component and preventing unauthorized processes from modifying boot firmware. Formal verification involves proving that a software program satisfies some	E, G, T	44	1020	1044	Clarity: What is essential? (Email?)		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.14.2e	System and Information Integrity	Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.	Monitoring is used to identify unusual or unauthorized activities or conditions related to individual users and system components, for example, unusual internal systems communications traffic; unauthorized exporting of information; signaling to external systems; large file transfers; long-time persistent connections; attempts to access information from unexpected locations; unusual protocols and ports in use; and attempted communications with suspected malicious external addresses. The correlation of physical audit record information and the audit records from systems may assist organizations in identifying examples of anomalous behavior. For example, the correlation of an individual's identity for logical access to certain systems with the additional information that the individual was not present at the	E, G, T	44	1045	1067	Clarify scope – CONFIRM this just systems with the CPI, HVA? The requirements state "organizational" requirements and systems. - Does an Enterprise, Detection, Response (EDR) address this requirement?		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: Dawn Greenman on behalf of FFRDC InfoSec Collaborative Date Submitted: 8/2/19

Section	Family	Control	Discussion	*Type: E - Editorial, G - General T - Technical	Page	Starting Line	Ending Line	Comment (Include rationale for comment)^	Suggested Change^	Recommended Solutions
3.14.3e	System and Information Integrity	Ensure that Internet of Things (IoT), Operational Technologies (OT), and Industrial Internet of Things (IIoT) systems, components, and devices are compliant with the security requirements imposed on organizational systems or are isolated in purpose-specific networks.	Operational Technology (OT) is the hardware, software, and firmware components of a system used to detect or cause changes in physical processes through the direct control and monitoring of physical devices. Examples include distributed control systems (DCS), supervisory control and data acquisition (SCADA) systems, and programmable logic controllers (PLC). The term operational technology is used to highlight the differences between industrial control systems (ICS) that are typically found in manufacturing and power plants and the information technology (IT) systems that typically support traditional data processing applications. The term Internet of Things (IoT) is used to describe the network of devices (e.g., vehicles, medical devices, wearables, and home appliances) that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and	G	45	1068	1103	General Comment: - Create guidance - This is the only requirement where you have an option to exclude something altogether and not make it compliant.		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	Family	Control	Discussion	*Type: E - Editorial, G - General T - Technical	Page	Starting Line	Ending Line	Comment (Include rationale for comment)^	Suggested Change^	Recommended Solutions
3.14.4e	System and Information Integrity	Refresh organizational systems and system components from a known, trusted state at least twice annually.		E, G	45	1104	1136	Concern: - High cost, operationally not feasible; disruptive	Eliminate requirement	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.14.4e	System and Information Integrity	Refresh organizational systems and system components from a known, trusted state at least twice annually.	DISCUSSION This requirement mitigates risk from the APT by reducing the targeting capability of adversaries (i.e., the window of opportunity for the attack). By implementing the concept of non-persistence for selected system components, organizations can provide a known state computing resource for a specific time-period that does not give adversaries sufficient time on target to exploit vulnerabilities in organizational systems and the environments in which those systems operate. Since the APT is a high-end, sophisticated threat regarding capability, intent, and targeting, organizations assume that over an extended period, a percentage of attacks will be successful. Non-persistent system components and system services are activated as required using protected information and are terminated periodically or at the end of sessions. Non-persistence	E, G, T	45	1104	1136	Clarity - Requirement states "organizational systems" - however, clarity this is specific to contracts with this requirement to protect defined HVA / CPI data. If this is an enterprise wide requirement, please provide guidance / best practices based upon the lessons learned / success the government has made in this arena. Challenge: Operationally not feasible; will be very disruptive and costly.		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.14.6e	System and Information Integrity	Use threat indicator information relevant to the information and systems being protected and effective mitigations obtained from external organizations to inform intrusion detection and threat hunting.	The constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), make it essential that threat information relating to specific threat events (e.g., TTP, targets) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, and threat intelligence (i.e., indications and warnings about threats that can occur) be sourced from and shared with trusted organizations. This information can be used by organizational Security Operations Centers (SOC) and incorporated into monitoring capabilities. Threat information sharing includes threat indicators, signatures, and adversary TTP from organizations participating in various threat-sharing consortia, government-commercial cooperatives, and government-government cooperatives (e.g., CERTCC, US-CERT, FIRST, ISAO, DIB CS	E, G, T	45	1152	1168	Clarity: - Vague as to minimum level of external threat intel to be consumed or shared. General: - Need to know what APT is focused on that specific program. Need the intel and appropriate IOCs. Some of the IOCs need to come from the sponsor in an unclassified form.	Use **SPONSOR PROVIDED** threat indicator information relevant to the information and systems being protected and effective mitigations obtained from external organizations to inform intrusion detection and threat hunting.	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
3.14.5e	System and Information Integrity	Conduct periodic reviews of persistent organizational storage locations and purge CUI that is no longer needed consistent with federal records retention policies and disposition schedules.	As programs, projects, and contracts evolve, some CUI may no longer be needed. Periodic and event-related (e.g., at project completion) reviews are conducted to ensure that CUI that is no longer required is securely removed from persistent storage. Retaining information for longer than it is needed makes the information a potential target for advanced adversaries searching for critical program or high value asset information to exfiltrate. For system-related information, unnecessary retention of such information provides advanced adversaries information that can assist in their reconnaissance and lateral movement through organizational systems. Alternatively, information which must be retained but is not required for current activities is removed from online storage and stored off-line in a secure location to eliminate the possibility of individuals gaining unauthorized access to the information through a	E, G, T	46	1137	1151	Clarity: - Requires contract language or information from sponsor to dictate the retention periods. - Clarify applicable only to relevant contract for HVA / CPI data. - Concern for FFRDCs and Research Organizations. Research consistently build from and is derived from prior learnings. This creates a longer longitudinal arc for CUI data. Given the organizational requirement, this would need to be deconflicted in an audit. While this could be done by discussing organizational standards, it would need to be carefully worded for exceptions that		

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
General	All	Introduction and Purpose and applicability	Applicability	E, G	12-13	198	250	***Line 198*** indicates the importance of protecting sensitive data on non-federal systems, while ***line 224*** states that CUI "may be contained in a critical program or high value asset", with references to OMB M-19-03 and OCIO HVA. Both of these documents refer only to data residing on federal information systems. ***Lines 244-250*** further specify that the scope of the document pertains to CUI on non-federal information systems. Additionally, ***lines 248-250*** specify the third condition for applicability of these requirements: when "no specific safeguarding requirements" are required by law, regulation, or policy. However, since the terms "HVA" and "critical	See comment	

FFRDC InfoSec Collaborative Comments on NIST SP 800-171B and Edits Requested

Submitted by: **Dawn Greenman on behalf of FFRDC InfoSec Collaborative** **Date Submitted:** **8/2/19**

Section	**Family**	**Control**	**Discussion**	***Type: E - Editorial, G - General T - Technical**	Page	Starting Line	Ending Line	**Comment (Include rationale for comment)^**	**Suggested Change^**	**Recommended Solutions**
General	All and 3.1.1e	Defintions / Appendix	Definitions: Critical, Sensitive System, Sensitive Operations, Organizational Operations, Organizational Systems, System Components	E, G, T	19 37 66	388 471 801 1201	388 471 801 1201	Provide clear definition of critical or sensitive system AND organizational operations	See comment	
Requiremnts	All	Requirements	The Requirements and Applicability: "The requirements apply only to the components of nonfederal systems that process, store, or transmit CUI contained in a critical program or high value assets that provide protection for such components"	E, G	22 (and 19)	463 371	466 372	Contractors have already seen Contracting Officers / Program Managers declare all CUI has critical.	Add clarity and detailed description of what such Programs or Assets entail and / or cost imposed upon DoD Programs if they apply such designations (e.g., they have to cover all or X% of the cost to contractors satisfy the requirements)	
Appendix	All	Organizational Systems impacted	No defintion of "organizational systems" in the appendix.	E, G, T	59 60	Appendix	Appendix	Definition of Organization System is critical. If this is an "enterprise network" this has a significant cost and operational impact as opposed to a network segment containing this data.	Define "organizational systems" HOWEVER **drop** reference to an entire organization system if related to an enterprise network due to cost and operational impacts.	