National Defense Information Security and Analysis Center
1050 Connecticut Ave NW #500, Washington, DC 20036
www.ndisac.org | (202) 888-2724 | info@ndisac.org

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

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

Ladies and Gentlemen,

Thank you for the opportunity to comment on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171B. Given the scope of the specified actions we believe NIST SP 800-171B creates significant impacts on our Member Companies and across the Defense Industrial Base (DIB) sector. In that context, the ND-ISAC engaged cybersecurity subject matter experts (SMEs) from our Member Companies to decompose 800-171B requirements and evaluate the technical efficacy of specified actions within their corporate enterprise networks. Through this structured, iterative, and exhaustive process our Member Companies also identified risks and impacts that implicate significant costs to business operations. Please find the results of those efforts documented in the prescribed comment matrix and enhanced controls review sheet, attached.

We also invite your attention to the following areas of highest impact that our SMEs identified and encourage your favorable consideration to developing revised language in these areas of concern:

- Designation of critical programs and high value assets is essential to determine which nonfederal systems may be in scope and therefore require concept, design, and/or modification to meet NIST 800-171B enhanced security requirements.

- The requirement to implement and operate a 24x7 Security Operations Center (SOC) has significant cost and resource tradeoffs, and may afford a competitive advantage to companies with already established capabilities. Additionally, the shifting of limited SOC resources to focus on 800-171B applicable network segments vs the entire enterprise attack surface paradoxically increases risk to non-800-171B covered systems.

National Defense Information Security and Analysis Center
1050 Connecticut Ave NW #500, Washington, DC 20036
www.ndisac.org | (202) 888-2724 | info@ndisac.org

- Techniques for decoys, concealment, misdirection, and tainting are unique in objective and at considerable cost require extraordinary rules, controls, and attention to prevent risk and liability. Experience among our SMEs suggests these complex solutions, if deployed, are customarily specified and directed by Programs thru contracts and for national security systems. Further, the language for enhanced security requirements based on threat intelligence with risk analysis and assessment, specifies requirements (e.g. bi-annual refresh, diverse system components, two-person rule), which minimally impact APT threats and attack scenarios, which those requirements are intended to deter.

Thank you for the opportunity to submit these comments to accompany the completed NIST comment matrix corresponding by line numbers to NIST 800-171B (Attachment 1), and also accompanied by our enhanced controls sheet with Impact Levels (Attachment 2).

The ~100 Member Companies of ND-ISAC are committed to contributing to the improved cybersecurity and resilience of the Defense Industrial Base. In that regard, we look forward to collaborating with NIST and the Department of Defense to develop approaches that are supportive of the objectives of the Department of Defense and national security but, at the same time and to our mutual benefit, recognize and sustain business efficiencies.

STEVEN D. SHIRLEY
Executive Director

Attachments:
1. Comment Matrix
2. Enhanced Control Sheet

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
1	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	Cover	NA **Change the designation from NIST 800-171B to reflect Supplement or Enhanced**	NA **Change the designation from NIST 800-171B to reflect Supplement or Enhanced**	Publication /Text Box	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. NIST should initiate analysis with the FAR Council as to applicability to federal acquisitions and NIST Chapter 3 Requirements with instructions and resources for contracting training and awareness. The supplemental text box should be removed from the cover page. The text is not indicated in the same detail within the publication.	**Change the designation from NIST 800-171B to reflect Supplement or Enhanced 800-171S or 800-171E** Recommend renumbering the 33 controls in NIST 800-171 Enhanced under the heading for each 3.x.x as "Enhanced Security Requirements" 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 and high value asset.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
2	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	G	i	28	29	Authority	For nonfederal owners/operators the NIST 800-171 series are specified in contractual terms. Timing of revisions with specific intervals for business planning purposes are required as the requirements regard finance, levels of effort, education and awareness, and physical assets. Currently there isn't a timeline available for NIST 800-171A, NIST 800-53 Rev 5 2nd Draft Spring 2019 Final Summer 2019, & NIST 800-171 Rev 3 Draft Fall/Winter 2019. The timing and correlation of requirements are critical and should have a known life cycle process to include the interdependencies. This initial draft was slated for Feb 2019 and slipped to June 2019 and was accompanied with two additional drafts while paralleled with NISTIR 8183 Cybersecurity Framework Manufacturing Profile, in total over 1000 pages to review in 30 days, extended to 45 days for industry in comparison to 120 days for Government. This initial draft of 800-171B has mappings to unpublished 800-53 requirements, undefined terms (e.g. critical program), and 30 guidance references.	Develop and maintain a site with NIST strategy and estimated timelines for 800 series publications. Add the site link in addition to the list of available publications

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
3	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	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.* "
4	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	ii	66	68	Abstract	The text is not indicated in the same detail within the publication. 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. NIST should initiate analysis with the FAR Council as to applicability to federal acquisitions and NIST Chapter 3 Requirements in a single document with instructions and resources for contracting training and awareness.	Recommend renumbering the 33 controls to NIST 800-171 under the heading for each 3.x.x as "Enhanced Security Requirements" 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 and high value asset.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
5	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	ii	70	74	Keywords	Add keywords of significance	Add Critical Program, High Value Asset, and NIST Special Publication 800-171
6	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	iv	84	93	Notes to Reviewers	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	Criteria for supplementing the basic, derived, and enhanced security requirements should be added for analysis to include the definitions for critical program and high value asset. Risk based frameworks are instrumental in determining effective, manageable, and operational controls to deliver valued safeguards and countermeasures in diverse and dynamic global environments.
7	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	iv	94	100	Notes to Reviewers	Text highlights security requirement 3.14.3e when other requirements are not deemed for reference to reviewers; appears unnecessary context for reviewers with the text being repeated in Chapter One, Page 2	Delete lines 94-100

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
8	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	iv	101	110	Notes to Reviewers	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	Penetration Resistant environments for unclassified information are limited based on purpose, function, and capability. Risk based frameworks are instrumental in determining effective, manageable, and operational controls to deliver valued safeguards and countermeasures in diverse and dynamic global environments.
9	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	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."*

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
10	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	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.* "
11	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	G	iv	120	123	Notes to Reviewers	NIST should be mandated to follow an adjudication process to include arbitration	Add adjudication process to include timeline and strategy for special publications inserted as contractual requirements to nonfederal entities; contractual process steps such as arbitration and audit should be considered by NIST and federal agencies as applicable to nonfederal owners and operators.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
12	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	G & T	vi	Text Box	Text Box	CUI ENHANCED SECURITY REQUIREMENTS	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	Delete Text Box
13	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	vii	152	Text Box	FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	Allow nonfederal owners and operators to use NIST CSF and to identify organizational risk mappings

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
14	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	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)
15	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	2	220	223	CHAPTER ONE; INTRODUCTION	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	NARA federal CUI regulation should consider cybersecurity or risk management framework to include requirements, processes and procedures. Current activities and products from NARA appear to be paralleled with NISPOM
16	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	2	224	224	CHAPTER ONE; INTRODUCTION	Definition for critical program is absent	Criteria for supplementing the basic and derived should be added to include the definitions for critical program and high value asset.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
17	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	2	226	233	CHAPTER ONE; INTRODUCTION	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	Recommend clarity for the categorization of critical program, high value asset, CUI, confidentiality, integrity, and APT in association to threats and attack scenarios
18	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	2	236	240	CHAPTER ONE; INTRODUCTION	Risks associated with the controls should be assessed with capabilities across operational environments.	Recommend Internet of Things (IoT), Operational Technology (OT), and Industrial Internet of Things (IIoT) systems, components, and devices to not be categorized as a new class of systems; reference appears to be discussion and recommend include as needed for supplemental guidance

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
19	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	2	240	242	CHAPTER ONE; INTRODUCTION	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	Recommend clarity for the categorization of critical program, high value asset, CUI, confidentiality, integrity, and APT in association to threats and attack scenarios
20	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	2	245	245	1.1 PURPOSE AND APPLICABILITY	The footnote for enhanced security requirements is broad in terms of nonfederal systems and contractual vehicles.	Recommend review and rewrite for clarity. Update Appendix B GLOSSARY
21	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	3	253	253	1.1 PURPOSE AND APPLICABILITY	Definition for critical program is absent	Criteria for supplementing the basic, derived, and enhanced security requirements should be added for analysis to include the definitions for critical program and high value asset.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
22	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	3	254	256	1.1 PURPOSE AND APPLICABILITY	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	Recommend clarity for the categorization of critical program, high value asset, CUI, confidentiality, integrity, and APT in association to threats and attack scenarios
23	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	3	256	259	1.1 PURPOSE AND APPLICABILITY	Clarification with "*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.* " The text is not indicated in the same detail within the publication. 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. NIST should initiate analysis with the FAR Council as to applicability to federal acquisitions and NIST Chapter 3 Requirements in a single document with instructions and resources for contracting training and awareness.	Criteria for supplementing the basic, derived, and enhanced security requirements should be added for analysis to include the definitions for critical program and high value asset.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
24	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	3	272	276	1.2 TARGET AUDIENCE	The text is not indicated in the same detail within the publication. 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.	NIST should initiate analysis with the FAR Council as to applicability to federal acquisitions and NIST Chapter 3 Requirements for only specifying requirements without discussion or supplemental guidance. Instructions and resources for contracting training and awareness are required and referenced thru potentially an appendix

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
25	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	4	282	283	1.3 ORGANIZATION OF THIS PUBLICATION	The text is not indicated in the same detail within the publication. 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.	NIST should initiate analysis with the FAR Council as to applicability to federal acquisitions and NIST Chapter 3 Requirements for only specifying requirements without discussion or supplemental guidance. Instructions and resources for contracting training and awareness are required and referenced thru potentially an appendix

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
26	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	4	284	287	1.3 ORGANIZATION OF THIS PUBLICATION	The text is not indicated in the same detail within the publication. 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.	Edit for clarity to - Supporting appendices provide additional information and supplemental guidance related to the protection of CUI in nonfederal systems categorized by a critical program or high value asset including: general references; definitions and terms; acronyms; mapping tables relating the enhanced security requirements [SP 800-171E] to the security controls in [SP 800-53].
27	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	G	5	298	302	2.1 BASIC ASSUMPTIONS	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	Recommend rewrite on risk management in contracts to the current environment having a lack of consistency with regards to NIST special publications and operational environments for nonfederal entities

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
28	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	5	303	303	2.1 BASIC ASSUMPTIONS	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	Recommend clarity for the categorization of critical program, high value asset, CUI, confidentiality, integrity, and APT in association to threats and attack scenarios
29	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	G	5	304	305	2.1 BASIC ASSUMPTIONS	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	Recommend clarity for the categorization of critical program, high value asset, CUI, confidentiality, integrity, and APT in association to threats and attack scenarios

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
30	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	G & T	5	306	309	2.1 BASIC ASSUMPTIONS	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	Recommend clarity for the categorization of critical program, high value asset, CUI, confidentiality, integrity, and APT in association to threats and attack scenarios
31	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	5	308	309	2.1 BASIC ASSUMPTIONS	Definition for critical program is absent	Criteria for supplementing the basic, derived, and enhanced security requirements should be added for analysis to include the definitions for critical program and high value asset.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
32	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	5	309	311	2.1 BASIC ASSUMPTIONS	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	Recommend clarity for the categorization of critical program, high value asset, CUI, confidentiality, integrity, and APT in association to threats and attack scenarios
33	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	5	314	316	2.1 BASIC ASSUMPTIONS	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	Recommend clarity for the categorization of critical program, high value asset, CUI, confidentiality, integrity, and APT in association to threats and attack scenarios

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
34	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	5	317	319	2.1 BASIC ASSUMPTIONS	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	Recommend clarity for the categorization of critical program, high value asset, CUI, confidentiality, integrity, and APT in association to threats and attack scenarios
35	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	6	320	322	2.1 BASIC ASSUMPTIONS	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	Recommend clarity for the criteria associated with equally effective to compensate for the inability to satisfy an enhanced security requirement

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
36	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	6	323	324	2.1 BASIC ASSUMPTIONS	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	Recommend clarity for the criteria associated with potential security solutions directly or using external service providers to satisfy enhanced security requirements Risks are inherent with third parties
37	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	6	326	326	2.2 ORGANIZATION OF ENHANCED SECURITY REQUIREMENTS	Reference and applicability of NIST 800-171A is unclear	Recommend clarity to specify - In addition to the basic and derived security requirements described in [SP 800-171] and [SP 800-171A]
38	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	6	327	329	2.2 ORGANIZATION OF ENHANCED SECURITY REQUIREMENTS	Definition for critical program is absent	Criteria for supplementing the basic, derived, and enhanced security requirements should be added for analysis to include the definitions for critical program and high value asset.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
39	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	6	330	332	2.2 ORGANIZATION OF ENHANCED SECURITY REQUIREMENTS	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	Recommend clarity for the categorization of critical program, high value asset, CUI, confidentiality, integrity, and APT in association to threats and attack scenarios

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
40	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	6	335	336	2.2 ORGANIZATION OF ENHANCED SECURITY REQUIREMENTS	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. NIST should initiate analysis with the FAR Council as to applicability to federal acquisitions and NIST Chapter 3 Requirements with instructions and resources for contracting training and awareness. The text is not indicated in the same detail within the publication.	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."* Rename Discussion sections to Supplemental Guidance sections. Recommend renumbering the 33 controls in NIST 800-171 Enhanced under the heading for each 3.x.x as "Enhanced Security Requirements" 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 and high value asset

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
41	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	6	339	340	2.2 ORGANIZATION OF ENHANCED SECURITY REQUIREMENTS	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. NIST should initiate analysis with the FAR Council as to applicability to federal acquisitions and NIST Chapter 3 Requirements with instructions and resources for contracting training and awareness. The text is not indicated in the same detail within the publication.	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."* Rename Discussion sections to Supplemental Guidance sections. Recommend renumbering the 33 controls in NIST 800-171 Enhanced under the heading for each 3.x.x as "Enhanced Security Requirements" 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 and high value asset

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
42	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	7	359	361	2.2 ORGANIZATION OF ENHANCED SECURITY REQUIREMENTS	Federal and nonfederal organizations face similar cyber threats, organizations are unique within varied environments and should have the latitude to address these threats uniquely with a common risk and threat-based framework. Agencies can leverage the Cybersecurity Framework to complement their current information security programs therefore nonfederal entities should be permitted a risk and threat based approach for information systems and programs.	Recommend clarity for the categorization of critical program, high value asset, CUI, confidentiality, integrity, and APT in association to threats and attack scenarios Tailoring is not risk aligned

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
43	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E, G, & T	8 thru 11	367	389	Chapter 3 THE REQUIREMENTS	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. NIST should initiate analysis with the FAR Council as to applicability to federal acquisitions and NIST Chapter 3 Requirements with instructions and resources for contracting training and awareness. The text is not indicated in the same detail within the publication.	Recommend moving the text associated with Chapter 3 THE REQUIREMENTS to Chapter 2 THE FUNDAMENTALS Section 2.2 ORGANIZATION OF ENHANCED SECURITY REQUIREMENTS as a continuation of the subject. Review the comments above on Chapter 2 to rewrite the text in Chapter 3. Chapter 3 THE REQUIREMENTS should start with page 12. 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."* Rename Discussion sections to Supplemental Guidance sections. Recommend renumbering the 33 controls in NIST 800-171 Enhanced under the heading for each 3.x.x as "Enhanced Security Requirements" 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 and high value asset

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
44	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	12 thru 36	469	1168	Chapter 3 THE REQUIREMENTS	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. NIST should initiate analysis with the FAR Council as to applicability to federal acquisitions and NIST Chapter 3 Requirements with instructions and resources for contracting training and awareness. The supplemental text box should be removed from the cover page. The text is not indicated in the same detail within the publication.	**Change the designation from NIST 800-171B to reflect Supplement or Enhanced 800-171S or 800-171E** Recommend renumbering the 33 controls in NIST 800-171 Enhanced under the heading for each 3.x.x as "Enhanced Security Requirements" followed by sequential numbering as per the current specification of Basic Security Requirements and Derived Security Requirements. Criteria for supplementing the basic, derived, and enhanced security requirements should be added for analysis to include the definitions for critical program and high value asset.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
45	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	12	471	472	3.1 ACCESS CONTROL 3.1.1e	Physical and nuclear security systems require specific two-person criteria. Expands beyond confidentiality and APT. Recommend deletion for CP/HVA CUI context since low risk and cybersecurity value when applying existing NIST 800-171 requirements such as insider threat, user privileges, and monitoring. Nonfederal operations have dynamic information and control capabilities.	Delete 3.1.1e or edit to specify - 3.1.23E *Employ dual authorization or control processes for organizational critical or sensitive system operations*
46	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	12	474	482	3.1 ACCESS CONTROL 3.1.1e DISCUSSION	Add more examples: such as promoting code from test to production, privilege user case where as a user - authorized by two individuals to have privilege in the first place is no further authorization required to implement a change.	Delete or Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. Rename Discussion sections to Supplemental Guidance sections.
47	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	12	483	484	3.1 ACCESS CONTROL 3.1.2e	Clarifying statement on the difference between this requirement and NIST 800-171 Revision 2 Security Requirement 3.1.18 scenarios related to GFE, collaboration solutions, mobile devices, cloud services, etc.	Edit 3.1.2e for clarity to specify - 3.1.24E *Restrict access to systems and system components to only those information resources that are owned, provisioned, issued, or evaluated and approved by the organization* .

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
48	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	12	485	490	3.1 ACCESS CONTROL 3.1.2e DISCUSSION	Clarifying statement on the difference between this requirement and NIST 8--171 Revision 2 Security Requirement 3.1.18; scenarios related to GFE, collaboration solutions, mobile devices, cloud services, etc.	Edit for clarity Rename Discussion sections to Supplemental Guidance sections. Move the discussion section to an Appendix in order to enforce the intent of the text.
49	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	12	491	492	3.1 ACCESS CONTROL 3.1.3e	Cross company collaboration, engineering. Normal cross domain item. Usually don't have formal tools that we have on a classified side. Only have DLP DRM. If it is somehow regulated, keep records on transfers. That should be sufficient with the controls. One part of the business to another part. Or it could be partner or team partner. Subcontractor would be some kind of "handshake" of transferring files, need policy of what can or cannot be done.	Edit 3.1.3e for clarity to specify - 3.1.25E *Employ information transfer solutions to control information flows on connected systems.*

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
50	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	12 & 13	493	518	3.1 ACCESS CONTROL 3.1.3e DISCUSSION	Recommend more information on SC-46 cross domain - unpublished. Cross Domain Solution A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains. Domain [CNSSI 4009] An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See Security Domain. security domain A domain that implements a security policy and is administered by a single authority. DOD Instruction 8540.01 Cross Domain (CD) Policy DoD ISs with a CDS as a component (e.g., an enclave) or a CDS as a separate IS (e.g., an enterprise CD service) must be authorized to operate by the authorizing official (AO) "Cross domain solutions approved by the United Cross Domain Services Management Office [UCDSMO] and secure information transfer solutions that have similar properties but are without formal UCDSMO approval." - access by DOD CAC only so how will the materials be provided to contractors and subcontractors?	Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. 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^
51	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	14	522	524	3.2 AWARENESS AND TRAINING3.2.1e	Recommend more info related to AT-2 (4), (6), & (7) - unpublished. How does this differentiate from 800-171 Revision 2 Security Requirement 3.2.2? Add APT to 3.2.3. 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat. Add identifier as to threat for context between unclassified and classified threat information.	Delete 3.2.1e; move and update NIST 800-171 Revision 2, 3.2.4

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
52	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	14	525	537	3.2 AWARENESS AND TRAINING 3.2.1e DISCUSSION	Recommend more info related to AT-2 (4), (6), & (7) - unpublished. Review discussion from NIST 800-171 Revision 2 for Security Requirements 3.2.2 & 3.2.3 Add identifier as to threat for context between unclassified and classified threat information.	Delete DISCUSSION or Move the discussion section to an Appendix in order to enforce the intent of the text. Rename Discussion sections to Supplemental Guidance sections. Provide context regarding guidance of NIST 800-50 with the 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." Review discussion from NIST 800-171 Revision 2 for Security Requirements 3.2.2 & 3.2.3

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
53	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	14	538	539	3.2 AWARENESS AND TRAINING 3.2.2e	Recommend more info related to AT-2 (8) - unpublished. How does this differentiate from 800-171 Revision 2 Security Requirement 3.2.2? Add APT to 3.2.3. 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat. Add identifier as to threat for context between unclassified and classified threat information.	Delete 3.2.2e; move and update NIST 800-171 Revision 2 3.2.5

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
54	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	14	540	549	3.2 AWARENESS AND TRAINING 3.2.2e DISCUSSION	Recommend more info related to AT-2 (8) - unpublished. How does this differentiate from 800-171 Revision 2 Security Requirement 3.2.2? Add APT to 3.2.3. 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat. Add identifier as to threat for context between unclassified and classified threat information.	Delete DISCUSSION or Move the discussion section to an Appendix in order to enforce the intent of the text. Rename Discussion sections to Supplemental Guidance sections. Provide context regarding guidance of NIST 800-181 with the 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." Review discussion from NIST 800-171 Revision 2 for Security Requirements 3.2.2 & 3.2.3

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
55	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	16	557	558	3.4 CONFIGURATION MANAGEMENT 3.4.1e	Definitions are absent for authoritative source and trusted source. Is management intended contract by contract? How does this differentiate from 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. What is the correlation to 3.11.6e? 3.11.6e Assess, respond to, and monitor supply chain risks associated with organizational systems.	Delete 3.4.1e; move and update NIST 800-171 Revision 2 existing security requirements 3.4.10

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
56	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	16	559	572	3.4 CONFIGURATION MANAGEMENT 3.4.1e DISCUSSION	How does this differentiate from 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. What is the correlation to 3.11.6e? 3.11.6e Assess, respond to, and monitor supply chain risks associated with organizational systems.	Delete DISCUSSION or Move the discussion section to an Appendix in order to enforce the intent of the text. Rename Discussion sections to Supplemental Guidance sections. Provide context regarding guidance of NIST 800-128 & IR 8011 with the 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." Review discussion from NIST 800-171 Revision 2 for Security Requirements 3.2.2 & 3.2.3

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
57	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	16	573	575	3.4 CONFIGURATION MANAGEMENT 3.4.2e	Criteria absent for automated mechanisms and misconfigured. Recommend more information related to mapping CM-3(8) - unpublished. Processes should include risk assessment to organizational processes and procedures regarding configuration actions.	Edit 3.4.2e for clarity to specify - 3.4.11E 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^
58	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	16	576	588	3.4 CONFIGURATION MANAGEMENT 3.4.2e DISCUSSION	Processes should include risk assessment to organizational processes and procedures regarding configuration actions. How does this differentiate from 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 in order to enforce the intent of the text. Provide context regarding guidance of IR 8011 with the 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." 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^
59	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	16	589	590	3.4 CONFIGURATION MANAGEMENT 3.4.3e	Criteria absent for automated discovery, complete, accurate, and readily available. How does this differentiate from 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 - 3.4.12E Employ discovery and management tools and/or organizational processes to maintain an inventory of system components.
60	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	16 & 17	591	603	3.4 CONFIGURATION MANAGEMENT 3.4.3e DISCUSSION	Broad categorization by definition of system components for inventory specifications. Criteria absent for automated discovery, complete, accurate, and readily available. How does this differentiate from 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 in order to enforce the intent of the text. 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^
61	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	18	607	609	3.5 IDENTIFICATION AND AUTHENTICATION 3.5.1e	Unclear as to the risk and residual value for a wired attack and APT. Clarify connection	Delete 3.5.1e or edit for clarity; move and update NIST 800-171 Revision 2 existing requirements 3.5.1 and 3.5.2 or 3.5.12E
62	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	18	610	620	3.5 IDENTIFICATION AND AUTHENTICATION 3.5.1e DISCUSSION	Add additional scenarios to include 802.1x; Linux & Mac environments; implication to certificate based with the SP 800-63-3 reference; deployment specification for clients and servers, containers, platforms.	Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. Provide context regarding guidance of SP 800-63-3 with the 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." 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^
63	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	18	621	623	3.5 IDENTIFICATION AND AUTHENTICATION 3.5.2e	Requirement is specifying a solution and should identify multi factor authentication and complex account management. Clarity as to specifications counter to single sign on, SAML, and federated access. contrary to one time in the path guidance. Recommend more information related to mapping IA-5(18) - unpublished.	Delete 3.5.2e or edit for clarity; move and update NIST 800-171 Revision 2 existing requirements 3.5.1 and 3.5.2 or 3.5.13E
64	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	18	624	640	3.5 IDENTIFICATION AND AUTHENTICATION 3.5.2e DISCUSSION	Clarity for trust models and practical implementations as to applied periodically or at the initial point of network connection, identify the scenarios and resultant criteria.	Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. Rename Discussion sections to Supplemental Guidance sections.
65	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	18	641	643	3.5 IDENTIFICATION AND AUTHENTICATION 3.5.3e	The specification is on device attestation with added requirements as to a trust profile & network access control. The statements related to patching, configuration management, and automation support align to the 3.14 SYSTEM AND INFORMATION INTEGRITY Family.	Delete 3.5.3e or edit for clarity; move and update NIST 800-171 Revision 2 existing requirements 3.14.4 thru 3.14.7 or 3.5.14E

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
66	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	18 & 19	644	655	3.5 IDENTIFICATION AND AUTHENTICATION 3.5.3e DISCUSSION	Add additional information related to the trust model and implementation scenarios.	Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. Provide context regarding guidance of IR 8011 with the 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." 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^
67	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	20	659	659	3.6 INCIDENT RESPONSE 3.6.1e	Recommend more information related to mapping IR-4(14) - unpublished. Provide both physical and technical criteria for organizationally defined security operations such as monitoring, alerting, and on call response equivalent to term full-time or situational awareness.	Delete or Edit 3.6.4E for clarity to specify - Establish and maintain situational awareness capabilities managed by a organizationally defined security operations center. Edit for clarity to allow for wide-ranging capabilities from large contractors (e.g. Follow the Sun SOCs, dynamic sensing, enterprise models) to small to medium companies (e.g. 3rd Party Services, Open Source Tools, and logging/monitoring configurations).

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
68	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	20	660	677	3.6 INCIDENT RESPONSE 3.6.1e DISCUSSION	Definitions and criteria not specified for incident handling information center. Add scenarios for 24x7 autonomous monitoring with a 24x7 response capability. Edit the statement on SOC capability guidance to - Organizations may implement a dedicated SOC or may employ third-party organizations to provide commensurate capability	Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. Provide context regarding guidance of SP 800-61, 800-86, 800-101, 800-150, and 800-184 with the 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." 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^
69	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	20	678	679	3.6 INCIDENT RESPONSE 3.6.2e	Recommend more information related to mapping IR-4(11) - unpublished. Does the specification support physical on site or available to respond within 24 hours.	Edit 3.6.2e for clarity to specify - 3.6.5E Establish and maintain a cyber incident response team that can handle incidents identified by the organization within 24 hours.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
70	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	20	680	695	3.6 INCIDENT RESPONSE 3.6.2e DISCUSSION	Provide both physical and technical criteria for capabilities organizationally defined for incident response support. Recommend additional scenarios be added.	Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. Provide context regarding guidance of SP 800-61, 800-86, 800-101, 800-150, and 800-184 with the 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." 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^
71	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	23	707	708	3.9 PERSONNEL SECURITY 3.9.1e	Definitions and criteria not specified for terms - enhanced, vetting, and ongoing basis. Add periodic re-evaluation to NIST 800-171 3.9.1	Delete or Edit 3.9.1e for clarity to specify - 3.9.3E 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).
72	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	23	709	722	3.9 PERSONNEL SECURITY 3.9.1e DISCUSSION	Provide additional scenarios similar to the text as "additional background checks". Provide information related to the vetting criteria (access to unclassified in comparison to classified systems); DOD granting clearances based on role in comparison to "need to know". Define terms of CUI or the applicability of access to critical program or high value asset	Delete or Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. 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^
73	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	23	723	724	3.9 PERSONNEL SECURITY 3.9.2e	Duplicative as to trustworthiness and NIST 800-53 mappings on Personnel & Developer Screening. Criteria not specified for adverse information	Delete with Edit to 3.9.1e for clarity to specify - 3.9.3E 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).
74	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	23	725	729	3.9 PERSONNEL SECURITY 3.9.2e DISCUSSION	Provide information related to the adverse information criteria (access to unclassified in comparison to classified systems) Define terms of CUI or the applicability of access to critical program or high value asset	Delete or Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. 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^
75	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	25	737	739	3.11 RISK ASSESSMENT 3.11.1e	Recommend more information related to mapping RA-3(3) - unpublished. Provide information related to the threat intelligence and threat hunting criteria Edit requirement to align with the Risk Assessment family, the threat awareness and intelligence references are more specific to Incident Response and Security Operations Center specified in the Incident Response (IR) family of NIST 800-171B	Edit 3.11.1e for clarity to specify - 3.11.4E Employ threat intelligence to inform the risk assessment for the development of system and security architectures, selection of security controls, and monitoring for remediation
76	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	25	740	749	3.11 RISK ASSESSMENT 3.11.1e DISCUSSION	Provide scenarios related to the threat intelligence and threat hunting criteria Discussion is focused on risk assessment, the threat awareness and intelligence references are more specific to Incident Response and Security Operations Center specified in the Incident Response (IR) family of NIST 800-171B	Edit for clarity Provide context regarding guidance of SP 800-30, 800-39, 800-160-1, and 800-150, with clear reference to risk assessment and "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." 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^
77	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	25	750	751	3.11 RISK ASSESSMENT 3.11.2e	Recommend more information related to mapping RA-10 - unpublished. The cyber threat hunting reference is more specific to Incident Response and Security Operations Center specified in the Incident Response (IR) family of NIST 800-171B	For clarity move requirement 3.11.2e to the Incident Response Family to specify - 3.6.6E 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.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
78	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	25	752	771	3.11 RISK ASSESSMENT 3.11.2e DISCUSSION	Provide scenarios related to the threat hunting criteria The cyber threat hunting reference is more specific to Incident Response and Security Operations Center specified in the Incident Response (IR) family of NIST 800-171B	Edit for clarity and move to the Incident Response IR Family Provide context regarding guidance of SP 800-30, 800-160-2, and 800-150, with clear reference to security operations and "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." 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^
79	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	25	772	773	3.11 RISK ASSESSMENT 3.11.3e	Recommend more information related to mapping RA-3(4) - unpublished. Provide information related to advanced automation and predictive analytics criteria. The automation and analytics references are more specific to Incident Response and Security Operations Center specified in the Incident Response (IR) family of NIST 800-171B	For clarity move requirement 3.11.3e to the Incident Response Family to specify - 3.6.7E Employ automation and analytics capabilities to identify and predict threats to organizations, systems, or system components.
80	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	25 & 26	774	786	3.11 RISK ASSESSMENT 3.11.3e DISCUSSION	The automation and analytics references are more specific to Incident Response and Security Operations Center specified in the Incident Response (IR) family of NIST 800-171B	Edit for clarity and move to the Incident Response IR Family Remove guidance of SP 800-30 associated with risk assessments and risk analysis. Rename Discussion sections to Supplemental Guidance sections.
81	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	26	787	789	3.11 RISK ASSESSMENT 3.11.4e	Redundant to System Security Plan requirement in NIST 800-171 3.12.4 Adding risk determinations and the specified level of detail is reflected in requirements related to the 3.12 Security Assessment family in NIST 800-171. Automation and dynamic environments are considered beneficial and operational in comparison to risks and static documentation.	Delete 3.11.4e

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
82	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	26	790	804	3.11 RISK ASSESSMENT 3.11.4e DISCUSSION	Adding risk determinations and the specified level of detail is reflected in requirements related to the 3.12 Security Assessment family in NIST 800-171. Automation and dynamic environments are considered beneficial and operational in comparison to risks and static documentation	Move discussion to 3.12.4 in NIST 800-171 Rename Discussion sections to Supplemental Guidance sections.
83	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	26	805	806	3.11 RISK ASSESSMENT 3.11.5e	Recommend more information related to mapping RA-3(3) - unpublished. Similar to 3.11.1e as to assessment without the time specification	Delete 3.11.5e and Edit 3.11.4E for clarity to specify annually - 3.11.4E Employ threat intelligence to inform the risk assessment for the development of system and security architectures, selection of security controls, and monitoring for remediation annually

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
84	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	26	807	815	3.11 RISK ASSESSMENT 3.11.5e DISCUSSION	Discussion on assessment without the time specification	Move discussion of 3.11.4E Provide context regarding guidance of SP 800-30 with clear reference to security operations and "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." Rename Discussion sections to Supplemental Guidance sections. Add text for timing - "is infused annually into the risk assessment processes and information security operations of the organization to identify any changes required to address the dynamic threat environment."

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
85	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	26	816	816	3.11 RISK ASSESSMENT 3.11.6e	Redundant to System Security Plan requirement in NIST 800-171 3.12.4 Adding risk determinations and the specified level of detail is reflected in requirements related to the 3.12 Security Assessment family in NIST 800-171. Requirement does not include a specification for a information technology control. SCRM clauses are specified contractually by Government and Agencies thru FAR (e.g. DFARS, HSAR). DFARS 252.204-7012 includes subcontract flow down for NIST 800-171. Unclear the association with the terms for CUI as to categorization as a critical program or high value asset	Delete 3.11.6e or clarify to specify - 3.11.5E Assess supply chain risks to inform risk assessment for applicable organizational systems

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
86	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director					3.11 RISK ASSESSMENT 3.11.6e DISCUSSION	SCRM clauses are specified contractually by Government and Agencies thru FAR (e.g. DFARS, HSAR). DFARS 252.204-7012 includes subcontract flow down for NIST 800-171.	Recommend review to align the requirement with the discussion by adding scenarios on supply chain risks mitigations Provide context regarding guidance of SP 800-30 and 800-161 with "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." 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^
87	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	27	828	829	3.11 RISK ASSESSMENT 3.11.7e	Recommend more information related to mapping SR-2 - unpublished. Redundant to System Security Plan requirement in NIST 800-171 3.12.4 and specifications thru the Contract Data Requirements List (CDRL). Adding risk determinations and the specified level of detail is reflected in requirements related to the 3.12 Security Assessment family in NIST 800-171. SCRM clauses are specified contractually by Government and Agencies thru FAR (e.g. DFARS, HSAR). DFARS 252.204-7012 includes subcontract flow down for NIST 800-171. Unclear the association with the terms for CUI as to categorization as a critical program or high value asset	Delete 3.11.7e

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
88	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	27	830	845	3.11 RISK ASSESSMENT 3.11.7e DISCUSSION	Redundant to System Security Plan requirement in NIST 800-171 3.12.4 and specifications thru the Contract Data Requirements List (CDRL). Adding risk determinations and the specified level of detail is reflected in requirements related to the 3.12 Security Assessment family in NIST 800-171. SCRM clauses are specified contractually by Government and Agencies thru FAR (e.g. DFARS, HSAR). DFARS 252.204-7012 includes subcontract flow down for NIST 800-171.	Recommend review to align the requirement with the discussion by adding scenarios on supply chain risk mitigations. Provide context regarding guidance of SP 800-161 with "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." 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^
89	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	28	849	850	3.12 SECURITY ASSESSMENT 3.12.1e	Recommend more information related to mapping SR-6(1) - unpublished. Review 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 - 3.12.5E 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^
90	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	28	851	873	3.12 SECURITY ASSESSMENT 3.12.1e DISCUSSION	Add types and techniques to include scenarios for levels and mission types in order to understand scope and criteria for assessing service and value.	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. Provide context regarding guidance of SP 800-53A with "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." 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^
91	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	29	877	877	3.13 SYSTEM AND COMMUNICATION PROTECTION 3.13.1e	Recommend more information related to mapping SA-17(9) and SC-47 - unpublished. Review the benefits of diverse systems, APT, and risk as operating systems and chipsets constrain the general implication of precision in heterogeneity. Criteria specification in regards to audit and assessments. Considerations for the scope to critical programs and high value assets should be an input to the risk analysis.	Delete 3.13.1e 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

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
92	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	29	878	909	3.13 SYSTEM AND COMMUNICATION PROTECTION 3.13.1e DISCUSSION	Employing diverse system components introduces risk at a higher level in consideration of support related to specifications and capabilities thru experience and training. Managing updates and system configurations across several diverse components should be identified as a risk input. Concerns as to the variety of third party products and services, economies of scale, and cross integration of complex manufacturing operating environments.	Deletion 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 Provide context regarding guidance of SP 800-160-1, 800-160-2, and 800-161 with "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." 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^
93	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	29	910	911	3.13 SYSTEM AND COMMUNICATION PROTECTION 3.13.2e	Non-persistence implementations are unique in objective and complex solutions are regularly specified by programs thru contractual terms. NIST has no liability protections in the event non-persistence techniques generate operational issues. Risks associated with the controls cannot be described without specificity and should be assessed on key capabilities across operational environments.	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

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
94	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	29 & 30	912	955	3.13 SYSTEM AND COMMUNICATION PROTECTION 3.13.2e DISCUSSION	Complex and substantial processes, coordination and maintenance with minimal regard to operational capabilities and thresholds	Deletion Review non-persistence techniques for inclusion as a risk factor in control families 3.11 Risk Assessment Provide context regarding guidance of SP 800-160-1 and 800-160-2 with "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." 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^
95	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	30	956	957	3.13 SYSTEM AND COMMUNICATION PROTECTION 3.13.3e	**Reviewers deem as a CRITICAL Comment:** Techniques for decoys, concealment, misdirection, and tainting are unique in objective and complex solutions are customarily specified by programs thru contractual terms. On the other hand, a general recommendation by NIST confers no liability protections in the event non-persistence techniques generate operational issues. For unclassified information, Government entities are required to share information that may associate with the deception key. Risks associated with the controls cannot be described without specificity and should be assessed with key capabilities across operational environments and the probability of success against APT.	Delete 3.13.3e - Critical: High Impacts to Critical Infrastructure Sectors to include Air, Defense, and Manufacturing.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
96	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	30 & 31	958	975	3.13 SYSTEM AND COMMUNICATION PROTECTION 3.13.3e DISCUSSION	Risks associated with the controls cannot be described without specificity and should be assessed with key capabilities across operational environments and success against APT.	Deletion Provide context regarding guidance of SP 800-160-2 with "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." 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^
97	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	31	976	976	3.13 SYSTEM AND COMMUNICATION PROTECTION 3.13.4e	Provide information related to isolation criteria. Are requirements excluded by requiring activities if internet isolation is specified?	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 - 3.13.17E Employ organizational defined physical or logical isolation in the system architecture

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
98	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	31	977	1015	3.13 SYSTEM AND COMMUNICATION PROTECTION 3.13.4e DISCUSSION	Add scenarios for specifications by/across requiring activities, programs, and/or contracts. Review terms as to criteria and/or definition (e.g. highly secure).	Deletion Provide context regarding guidance of SP 800-160-1 with "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." 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^
99	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	33	1020	1021	3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.1e	Provide information related to integrity criteria and security critical or essential software with applicability to an asset categorized as a critical program or high value asset.	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 - 3.14.8E Define procedures for integrity verification on software organizationally defined as security critical or essential.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
100	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	33	1022	1044	3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.1e DISCUSSION	Selectively needed	Provide context regarding guidance of FIPS 140-2, FIPS 180-4, FIPS 202, FIPS 186-4, SP 800-147, and NIST TRUST with "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." Rename Discussion sections to Supplemental Guidance sections.
101	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	33	1045	1046	3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.2e	Review requirements in Control Families 3.3, 3.9, 3.12, & 3.14 in both NIST 800-171 and for 171B for duplication, potential consolidation, or focus to continuous monitoring with accountability in Control Family 3.3 and 3.6 regarding SOC.	Delete 3.14.2e or Edit 3.6.4E for clarity to specify - Establish and maintain situational awareness capabilities managed by a organizationally defined security operations center

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
102	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	33 & 34	1047	1067	3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.2e DISCUSSION	Relocate to the appropriate control families based on monitoring not integrity	Delete and append to minimally 3.3.5 and 3.6.1e discussions Move the discussion section to an Appendix in order to enforce the intent of the text. Provide context regarding guidance of SP 800-61, 800-83, 800-92, 800-94, and 800-137 with the 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." 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^
103	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	34	1068	1070	3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.3e	Recommend more information related to mapping SC-49 - unpublished. Isolation isn't inherent to types of OT operationally. Risks associated with the controls should be assessed with capabilities across operational environments.	Edit 3.14.3e for clarity to specify segregation over isolation - 3.14.9E 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^
104	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	34	1071		3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.3e DISCUSSION	Add information related to IIoT and NIST special publication(s) on and related to Industrial Control Systems in nonfederal systems for water, electricity, and manufacturing	Move the discussion section to an Appendix in order to enforce the intent of the text. Provide context regarding guidance of SP 800-160-1 and the addition of 800-82 with the 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." 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^
105	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	34	1104	1105	3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.4e	Recommend more information related to mapping SI-14(2) and SI-14(3) - unpublished. Non-persistence implementations are unique in objective and complex solutions generate operational issues. Risks associated with the controls should be assessed with capabilities across operational environments. Review the information within the control family 3.4 as to configuration and 3.13.2e on non-persistence in order to consolidate and focus objective	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
106	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	34 & 35	1106	1136	3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.4e DISCUSSION	Reimaging information is specific as to twice annually and identifies components without an assessment on system impacts and operational issues. Capabilities for automation, software services, and dynamic environments provide measurable benefits over reimaging.	Delete Move the discussion section to an Appendix in order to enforce the intent of the text. 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^
107	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	35	1137	1138	3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.5e	Recommend more information related to mapping SI-14(2) - unpublished. Review identification of CUI and 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." Update the sanitization definition in the glossary to exclude term "classified" 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. Move the discussion section to an Appendix in order to enforce the intent of the text. Rename Discussion sections to Supplemental Guidance sections.
108	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	35	1139	1151	3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.5e DISCUSSION	Review control family 3.8 for media protection and CUI	Delete and move to the Media Protection Family in NIST 800-171

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
109	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	T	35	1152	1154	3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.6e	The automation and analytics references are more specific 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 3.11.4E Employ threat intelligence to inform the risk assessment for the development of system and security architectures, selection of security controls, and monitoring for remediation

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
110	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	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 Add and provide context regarding guidance of SP 800-150 with the 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." 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^
111	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	37-42	NA	NA	Appendix A - REFERENCES	Missing or inconsistencies with references	Add NIST 800-171A UCDSMO may not be available to contractors and subcontractors FOIA96 not referenced in text FISMA requires brackets as needed [FISMA] within text Footnote 27 has implications as of date of contract OMB A-130 requires brackets as needed [OMB-A-130] within text FIPS 140-3 not referenced in text Change reference [IR 8011] to [IR 8011-1] Add reference for CUI Registry Recommend references after Glossary in order of appendices since the Glossary includes references. References may be more helpful to also include in order instead of groupings - creates ease to find if unfamiliar with type of reference

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
112	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E, G, & T	43-51	NA	NA	Appendix B - GLOSSARY	Missing or inconsistencies with glossary terms and definitions; check if acronyms need definition text	Update all definitions with key authoritative document Keywords from Page ii are missing from the glossary Remove acronyms from glossary word(s) Review document for missing terms and definitions to include but not limited to: Missing Adversary Hunting Missing Adverse Impact Missing Basic Requirement Missing Component Missing Contract Missing Covered Contractor Information System Missing Covered Defense Information Missing Critical Program Missing Cyber Survivability or Survivability Missing Damage Limiting Operations Missing Deception Missing Defense-in-Depth Missing Derived Requirement Missing Enhanced Requirement Missing Enhanced Security Requirement Missing External Service Provider Missing Family(ies) Missing Grant Missing High Value Asset Missing Impact Value Missing Industrial Internet of Things Missing Managed Detection and Response Services Provider Missing Managed Services Missing Managed Security Services Provider Missing Moderate Missing Operations Missing Penetration Resistant Architecture Missing Regulation Missing Requirement Missing Security Architecture Missing Services (IT, Platform, Software) Missing System Architecture Missing Security Operations Center Missing Tactics, Techniques, and Procedures Missing Threat Assessment Missing Vulnerability Assessment Missing Threat Hunting

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
113	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	52 & 53	NA	NA	Appendix C - ACRONYMS	Missing or inconsistencies with abbreviations	Review document to include glossary and references for missing acronyms to include but not limited to: Missing CSF Missing EO Missing GAO Missing HVA Missing USC
114	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E, G, & T	54	NA	NA	Appendix D - MAPPING TABLES	Inconsistency with footnote	Footnote 28 has implications as of date of contract
115	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	54 - 70	NA	NA	Appendix D - MAPPING TABLES	Check mapping for SI-4(24) System Monitoring *Automated Means for Sharing Threat Intelligence*	SI-4(24) System Monitoring *Indicators of Compromise*
116	National Defense Information Security and Analysis Center (ND-ISAC)	Steven D. Shirley, Executive Director	E & G	54 - 70	NA	NA	Appendix D - MAPPING TABLES	Check mapping for unpublished references Check mapping for duplicative mapping with NIST 800-171 Rev 2 and provide explanation in the discussion/supplemental guidance	Unpublished mappings and duplication provided within the comments above by the specific requirement

SP 800-171B (DRAFT) PROTECTING CUI IN NONFEDERAL SYSTEMS AND ORGANIZATIONS
Enhanced Security Requirements for Critical Programs and High Value Assets

TABLE D-1: MAPPING ACCESS CONTROL REQUIREMENTS TO CONTROLS

			Indicators/Impacts						Recommendation	Discussion Recommendations
SECURITY REQUIREMENTS	**NIST SP 800-53** ***Relevant Security Controls***		Function (Cyber Value/Tactic)	Users	Operations (HW, SW)	Admins	Cost	Supply Chain		
3.1.1e Employ dual authorization to execute critical or sensitive system and organizational operations.	AC-3(2)	Access Enforcement *Dual Authorization*	Low	Moderate	High	High	High	High	Delete 3.1.1e or edit to specify - 3.1.23E Employ dual authorization or control processes for organizational critical or sensitive system operations	Delete or Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. Rename Discussion sections to Supplemental Guidance sections.
	AU-9(5)	Protection of Audit Information *Dual Authorization*								
	CM-5(4)	Access Restrictions for Change *Dual Authorization*								
	CP-9(7)	System Backup *Dual Authorization*								
	MP-6(7)	Media Sanitization *Dual Authorization*								
3.1.2e Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.	AC-20(3)	Use of External Systems *Non-Organizationally Owned Systems—Restricted Use*	High	Moderate	Moderate	Low	High	High	Edit 3.1.2e for clarity to specify - 3.1.24E Restrict access to systems and system components to only those information resources that are owned, provisioned, issued, or evaluated and approved by the organization.	Edit for clarity Rename Discussion sections to Supplemental Guidance sections. Move the discussion section to an Appendix in order to enforce the intent of the text.
3.1.3e Employ secure information transfer solutions to control information flows between security domains on connected systems.	AC-4	Information Flow Enforcement	High	High	High	High	High	High	Edit 3.1.3e for clarity to specify - 3.1.25E Employ information transfer solutions to control information flows on connected systems.	Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. Rename Discussion sections to Supplemental Guidance sections.
	AC-4(1)	Information Flow Enforcement *Object Security Attributes*								
	AC-4(6)	Information Flow Enforcement *Metadata*								
	AC-4(8)	Information Flow Enforcement *Security Policy Filters*								
	AC-4(12)	Information Flow Enforcement *Data Type Identifiers*								
	AC-4(13)	Information Flow Enforcement *Decomposition into Policy-Relevant Subcomponents*								
	AC-4(15)	Information Flow Enforcement *Detection of Unsanctioned Information*								
	AC-4(20)	Information Flow Enforcement *Approved Solutions*								
	SC-46	Cross Domain Policy Enforcement								
3.2.1e 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.	AT-2	Awareness Training	High	Moderate	Moderate	Low	Moderate	High	Delete 3.2.1e; move and update NIST 800-171 Revision 2, 3.2.4	Delete DISCUSSION or Move the discussion section to an Appendix in order to enforce the intent of the text. Rename Discussion sections to Supplemental Guidance sections. Provide context regarding guidance of NIST 800-50 with the 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." Review discussion from NIST 800-171 Revision 2 for Security Requirements 3.2.2 & 3.2.3
	AT-2(3)	Awareness Training *Social Engineering and Mining*								
	AT-2(4)	Awareness Training *Suspicious Communications and Anomalous System Behavior*								
	AT-2(6)	Awareness Training *Advanced Persistent Threat*								
	AT-2(7)	Awareness Training *Cyber Threat Environment*								
3.2.2e 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.	AT-2(1)	Awareness Training *Practical Exercises*	High	Moderate	Moderate	Low	Moderate	High	Delete 3.2.2e; move and update NIST 800-171 Revision 2 3.2.5	Delete DISCUSSION or Move the discussion section to an Appendix in order to enforce the intent of the text. Rename Discussion sections to Supplemental Guidance sections. Provide context regarding guidance of NIST 800-181 with the 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." Review discussion from NIST 800-171 Revision 2 for Security Requirements 3.2.2 & 3.2.3
	AT-2(8)	Awareness Training *Training Feedback*								
3.4.1e Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.	CM-2	Baseline Configuration	Moderate	Moderate	High	Moderate	High	High	Delete 3.4.1e; move and update NIST 800-171 Revision 2 existing security requirements 3.4.10	Delete DISCUSSION or Move the discussion section to an Appendix in order to enforce the intent of the text. Rename Discussion sections to Supplemental Guidance sections. Provide context regarding guidance of NIST 800-128 & IR 8011 with the 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." Review discussion from NIST 800-171 Revision 2 for Security Requirements 3.2.2 & 3.2.3
	CM-3	Configuration Change Control								
	CM-8	System Component Inventory								
	SI-14(1)	Non-Persistence *Refresh from Trusted Sources*								
3.4.2e 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.	CM-2	Baseline Configuration	Moderate	Moderate	High	Moderate	High	High	Edit 3.4.2e for clarity to specify - 3.4.11E 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.	Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. Provide context regarding guidance of IR 8011 with the 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." Rename Discussion sections to Supplemental Guidance sections.
	CM-3	Configuration Change Control								
	CM-3(5)	Configuration Change Control *Automated Security Response*								
	CM-3(8)	Configuration Change Control *Prevent or Restrict Configuration Changes*								
3.4.3e Employ automated discovery and management tools to maintain an up-to- date, complete, accurate, and readily available inventory of system components.	CM-2(2)	Baseline Configuration *Automation Support for Accuracy and Currency*							**Edit 3.4.3e for clarity to specify - 3.4.12E Employ discovery and management tools and/or organizational processes to maintain an inventory of system components.**	Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. Rename Discussion sections to Supplemental Guidance sections.

	CM-8(2)	System Component Inventory *Automated Maintenance*	Moderate	Low	Moderate	Moderate	High	High		
3.5.1e Identify and authenticate systems and system components before establishing a network connection using bidirectional authentication that is cryptographically-based and replay resistant.	IA-3	Device Identification and Authentication	Moderate	Low	High	High	High	High	Delete 3.5.1e or edit for clarity; move and update NIST 800-171 Revision 2 existing requirements 3.5.1 and 3.5.2 or 3.5.12E	Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. Provide context regarding guidance of SP 800-63-3 with the 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." Rename Discussion sections to Supplemental Guidance sections.
	IA-3(1)	Device Identification and Authentication *Cryptographic Bidirectional Authentication*								
	IA-2(8)	Identification and Authentication (Organizational Users) *Access to Accounts — Replay Resistant*								
3.5.2e 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.	IA-5(18)	Authenticator Management *Password Managers*	High	Moderate	Moderate	High	High	High	Delete 3.5.2e or edit for clarity; move and update NIST 800-171 Revision 2 existing requirements 3.5.1 and 3.5.2 or 3.5.13E	Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. Rename Discussion sections to Supplemental Guidance sections.
3.5.3e 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.	CM-8(3)	System Component Inventory *Automated Unauthorized Component Detection*	Moderate	Low	High	High	High	High	Delete 3.5.3e or edit for clarity; move and update NIST 800-171 Revision 2 existing requirements 3.14.4 thru 3.14.7 or 3.5.14E	Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. Provide context regarding guidance of IR 8011 with the 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." Rename Discussion sections to Supplemental Guidance sections.
	IA-3(4)	Device Authentication and Authentication *Device Attestation*								
	SI-4(22)	System Monitoring *Unauthorized Network Services*								
3.6.1e Establish and maintain a full-time security operations center capability.	IR-4(14)	Incident Handling *Security Operations Center*	Moderate	Low	High	Low	High	High	Delete or Edit 3.6.4E for clarity to specify - Establish and maintain situational awareness capabilities managed by a organizationally defined security operations center	Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. Provide context regarding guidance of SP 800-61, 800-86, 800-101, 800-150, and 800-184 with the 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." Rename Discussion sections to Supplemental Guidance sections. Edit for clarity to allow for wide-ranging capabilities from large contractors (e.g. Follow the Sun SOCs, dynamic sensing, enterprise models) to small to medium companies (e.g. 3rd Party Services, Open Source Tools, and logging/monitoring configurations).
3.6.2e Establish and maintain a cyber incident response team that can be deployed to any location identified by the organization within 24 hours.	IR-4(11)	Incident Handling *Cyber Incident Response Team*	Low	Low	Moderate	Low	High	High	Edit 3.6.2e for clarity to specify - 3.6.5E Establish and maintain a cyber incident response team that can handle incidents identified by the organization within 24 hours.	Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. Provide context regarding guidance of SP 800-61, 800-86, 800-101, 800-150, and 800-184 with the 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." Rename Discussion sections to Supplemental Guidance sections.
	IR-7	Incident Response Assistance								
3.9.1e Conduct enhanced personnel screening (vetting) for individual trustworthiness and reassess individual trustworthiness on an ongoing basis.	PS-3	Personnel Screening	Low	Low	Low	Low	Moderate	Moderate	Delete or Edit 3.9.1e for clarity to specify - 3.9.3E 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).	Delete or Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. Rename Discussion sections to Supplemental Guidance sections.
	SA-21	Developer Screening								
3.9.2e Ensure that organizational systems are protected whenever adverse information develops regarding the trustworthiness of individuals with access to CUI.	PS-3	Personnel Screening	Low	Low	Low	Low	Moderate	Moderate	Delete with Edit to 3.9.1e for clarity to specify - 3.9.3E 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).	Delete or Edit for clarity Move the discussion section to an Appendix in order to enforce the intent of the text. Rename Discussion sections to Supplemental Guidance sections.
	SA-21	Developer Screening								
3.11.1e Employ threat intelligence to inform the development of the system and security architectures, selection of security controls, monitoring, threat hunting, and response and recovery activities.	PM-16	Threat Awareness Program	High	Low	Moderate	Low	Low	High	Edit 3.11.1e for clarity to specify - 3.11.4E Employ threat intelligence to inform the risk assessment for the development of system and security architectures, selection of security controls, and monitoring for remediation	Edit for clarity Provide context regarding guidance of SP 800-30, 800-39, 800-160-1, and 800-150, with clear reference to risk assessment and "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." Rename Discussion sections to Supplemental Guidance sections.
	PM-16(1)	Threat Awareness Program *Automated Means for Sharing Threat Intelligence*								
	RA-3(3)	Risk Assessment *Dynamic Threat Analysis*								
3.11.2e 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.	RA-10	Threat Hunting	High	Low	Low	Low	High	High	For clarity move requirement 3.11.2e to the Incident Response Family to specify - 3.6.6E 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.	Edit for clarity and move to the Incident Response IR Family Provide context regarding guidance of SP 800-30, 800-160-2, and 800-150, with clear reference to security operations and "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." Rename Discussion sections to Supplemental Guidance sections.
	SI-4(24)	System Monitoring *Indicators of Compromise*								

3.11.3e Employ advanced automation and analytics capabilities to predict and identify risks to organizations, systems, or system components.	RA-3(4)	Risk Assessment *Predictive Cyber Analytics*	Moderate	Moderate	Moderate	High	High	High	For clarity move requirement 3.11.3e to the Incident Response Family to specify - 3.6.7E Employ automation and analytics capabilities to identify and predict threats to organizations, systems, or system components.	Edit for clarity and move to the Incident Response IR Family Remove guidance of SP 800-30 associated with risk assessments and risk analysis. Rename Discussion sections to Supplemental Guidance sections.
	SI-4(24)	System Monitoring *Indicators of Compromise*								
3.11.4e Document 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 mechanisms, and dependencies on external service providers.	PL-2	System Security and Privacy Plans	Low	Low	Moderate	Moderate	Moderate	Moderate	Delete 3.11.4e	Move discussion to 3.12.4 in NIST 800-171 Rename Discussion sections to Supplemental Guidance sections.
3.11.5e 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.	RA-3	Risk Assessment	Low	Low	Low	Low	Low	Moderate	Delete 3.11.5e and Edit 3.11.4E for clarity to specify annually - 3.11.4E Employ threat intelligence to inform the risk assessment for the development of system and security architectures, selection of security controls, and monitoring for remediation annually	Move discussion of 3.11.4E Provide context regarding guidance of SP 800-30 with clear reference to security operations and "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." Rename Discussion sections to Supplemental Guidance sections. Add text for timing - "is infused annually into the risk assessment processes and information security operations of the organization to identify any changes required to address the dynamic threat environment."
	RA-3(3)	Risk Assessment *Dynamic Threat Awareness*								
3.11.6e Assess, respond to, and monitor supply chain risks associated with organizational systems.	RA-3	Risk Assessment	High	Low	Moderate	High	Moderate	Moderate	Delete 3.11.6e or clarify to specify - 3.11.5E Assess supply chain risks to inform risk assessment for applicable organizational systems	Recommend review to align the requirement with the discussion by adding scenarios on supply chain risks mitigations Provide context regarding guidance of SP 800-30 and 800-161 with "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." Rename Discussion sections to Supplemental Guidance sections.
	RA-3(1)	Risk Assessment *Supply Chain Risk Assessment*								
3.11.7e Develop and update as required, a plan for managing supply chain risks associated with organizational systems.	SR-2	Supply Chain Risk Management Plan	Moderate	Low	Moderate	Moderate	Moderate	Moderate	Delete 3.11.7e	Recommend review to align the requirement with the discussion by adding scenarios on supply chain risk mitigations. Provide context regarding guidance of SP 800-161 with "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." Rename Discussion sections to Supplemental Guidance sections.
3.12.1e Conduct penetration testing at least annually, leveraging automated scanning tools and ad hoc tests using human experts.	CA-8	Penetration Testing	High	Low	Moderate	Low	Moderate	High	Edit 3.12.1e for clarity to specify - 3.12.5E Conduct organizationally defined penetration testing simulating network and system attacks threat intel at least annually for critical programs or high value assets.	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. Provide context regarding guidance of SP 800-53A with "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." Rename Discussion sections to Supplemental Guidance sections.
	SR-6(1)	Supplier Reviews *Penetration Testing and Analysis*								
3.13.1e Employ diverse system components to reduce the extent of malicious code propagation.	PL-8	Security and Privacy Architectures	Low	Low	High	High	High	High	Delete 3.13.1e 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	Deletion 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 Provide context regarding guidance of SP 800-160-1, 800-160-2, and 800-161 with "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." Rename Discussion sections to Supplemental Guidance sections.
	SA-17(9)	Developer Security Architecture and Design *Design Diversity*								
	SC-27	Platform-Independent Applications								
	SC-29	Heterogeneity								
	SC-29(1)	Heterogeneity *Virtualization Techniques*								
	SC-47	Communications Path Diversity								
3.13.2e Disrupt the attack surface of organizational systems and system components through unpredictability, moving target defense, or non-persistence.	SC-30(2)	Concealment and Misdirection *Randomness*	Low	High	High	High	High	High	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	Deletion Review non-persistence techniques for inclusion as a risk factor in control families 3.11 Risk Assessment Provide context regarding guidance of SP 800-160-1 and 800-160-2 with "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." Rename Discussion sections to Supplemental Guidance sections.
	SC-30(3)	Concealment and Misdirection *Change Processing and Storage Locations*								
	SI-14	Non-Persistence								
3.13.3e Employ technical and procedural means through a combination of misdirection, tainting, or disinformation to confuse and mislead adversaries.	SC-8(4)	Transmission Confidentiality and Integrity *Conceal or Randomize Communications*	Low	High	High	High	High	High	Delete 3.13.3e - Critical: High Impacts to Critical Infrastructure Sectors to include Air, Defense, and Manufacturing.	Deletion Provide context regarding guidance of SP 800-160-2 with "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." Rename Discussion sections to Supplemental Guidance sections.
	SC-26	Decoys								
	SC-30	Concealment and Misdirection								
	SC-30(2)	Concealment and Misdirection *Randomness*								
	SI-20	Tainting								
3.13.4e Employ physical and logical isolation techniques in the system and security architecture.	SC-7	Boundary Protection	Moderate	High	High	High	High	High	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 - 3.13.17E Employ organizational defined physical or logical isolation in the system architecture	Deletion Provide context regarding guidance of SP 800-160-1 with "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." Rename Discussion sections to Supplemental Guidance sections.
	SC-7(13)	Boundary Protection *Isolation of Security Tools, Mechanisms, and Support Components*								
	SC-7(21)	Boundary Protection *Isolation of System Components*								
	SC-7(22)	Boundary Protection *Separate Subnets for Connecting to Different Security Domains*								
	SC-25	Thin Nodes								
3.14.1e Employ roots of trust, formal verification, or cryptographic signatures to verify the integrity and correctness of security critical or essential software.	SI-7(6)	Software, Firmware, and Information Integrity *Cryptographic Protection*	Moderate	Low	Moderate	Moderate	Moderate	Moderate	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 - 3.14.8E Define procedures for integrity verification on software organizationally defined as security critical or essential.	Provide context regarding guidance of FIPS 140-2, FIPS 180-4, FIPS 202, FIPS 186-4, SP 800-147, and NIST TRUST with "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." Rename Discussion sections to Supplemental Guidance sections.
	SI-7(9)	Software, Firmware, and Information Integrity *Verify Boot Process*								
	SI-7(10)	Software, Firmware, and Information Integrity *Protection of Boot Firmware*								
	SI-7(10)	Software, Firmware, and Information Integrity *Integrity Verification*								

	SA-17	Developer Security Architecture and Design								
3.14.2e Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.	AU-6(6)	Audit Record Review, Analysis, and Reporting	Low	Low	Moderate	Low	Moderate	Moderate	Delete 3.14.2e or Edit 3.6.4E for clarity to specify - Establish and maintain situational awareness capabilities managed by a organizationally defined security operations center	Delete and append to minimally 3.3.5 and 3.6.1e discussions Move the discussion section to an Appendix in order to enforce the intent of the text. Provide context regarding guidance of SP 800-61, 800-83, 800-92, 800-94, and 800-137 with the 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." Rename Discussion sections to Supplemental Guidance sections.
	SI-4(4)	System Monitoring *Inbound and Outbound Communications Traffic*								
	SI-4(7)	System Monitoring *Automated Response to Susaicious Events*								
	SI-4(11)	System Monitoring *Analyze Communications Traffic Anomalies*								
	SI-4(13)	System Monitoring *Analyze Traffic and Event Patterns*								
	SI-4(18)	System Monitoring *Analyze Traffic and Covert Exfiltration*								
	SI-4(19)	System Monitoring *Risk for individuals*								
	SI-4(20)	System Monitoring *Privileged Users*								
3.14.3e 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 isolated in purpose- specific networks.	AC-3	Access Enforcement	High	Low	Low	Moderate	Moderate	High	Edit 3.14.3e for clarity to specify segregation over isolation - 3.14.9E 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.	Move the discussion section to an Appendix in order to enforce the intent of the text. Provide context regarding guidance of SP 800-160-1 and the addition of 800-82 with the 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." Rename Discussion sections to Supplemental Guidance sections.
	AC-4	Information Flow Enforcement								
	SA-8	Security and Privacy Engineering Principles								
	SC-2	Separation of System and User Functionality								
	SC-3	Security Function Isolation								
	SC-49	Hardware-Enforced Separation and Policy Enforcement								
3.14.4e Refresh organizational systems and system components from a known, trusted state at least twice annually.	SI-14	Non-Persistence	Low	High	High	High	High	High	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	Delete Move the discussion section to an Appendix in order to enforce the intent of the text. Rename Discussion sections to Supplemental Guidance sections.
	SI-14(1)	Non-Persistence *Refresh from Trusted Sources*								
	SI-14(2)	Non-Persistence *Non-Persistent Information*								
	SI-14(3)	Non-Persistence *Non-Persistent Connectivity*								
3.14.5e 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.	SC-28(2)	Protection of Information at Rest *Off-Line Storage*	Low	Low	Moderate	Low	Moderate	High	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. Move the discussion section to an Appendix in order to enforce the intent of the text. Rename Discussion sections to Supplemental Guidance sections.	Delete and move to the Media Protection Family in NIST 800-171
	SI-14(2)	Non-Persistence *Non-Persistent Information*								
3.14.6e 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.	PM-16(1)	Threat Awareness Program *Automated Means for Sharing Threat Intelligence*	Low	Low	Moderate	Low	Low	High	Edit for clarity and move 3.14.6e to the Incident Response IR Family 3.11.4E Employ threat intelligence to inform the risk assessment for the development of system and security architectures, selection of security controls, and monitoring for remediation	Edit for clarity and move to the Incident Response IR Family Add and provide context regarding guidance of SP 800-150 with the 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." Rename Discussion sections to Supplemental Guidance sections.
	SI-4(24)	System Monitoring *Automated Means for Sharing Threat Intelligence*								
	SI-5	Security Alerts, Advisories, and Directives								

Column1
High
Moderate
Low