#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
1	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		2	226			171B is crafted under the premise that this 'specific' CUI is not more harmful (same as least moderate as 171). The differentiator between 171 and 171B is likelihood of APT attack and specifically not higher impact level. As 171B states, this need is not certain, but based upon contract requirements. After all, it is a risk management decision as to the practical tradeoff between cost application of 171B and gain for a specific program/mission.	From: (APT). The APT is an … To: (APT). Hence while not necessarily a source for greater harm than other CUI, CUI contained in critical program or high value assets may require additional protection against APT attack. The APT is an …
2	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		3	250			Suggest worhtwhile to early on relay what will be reinforced later that confidentiality and integrity are inter-dependent, and achieving the former is not possible without also achieving aspects of the later.	Append: With that objective it is noted that protecting the integrity and availability of means used to achieve this confidentiality protection is also within scope. Additionally, while outside the explicit purpose of this publication, users should be aware that the ATP may seek to harm organizations, individuals, or the Nation by compromising the integrity of CUI upon which missions depend; for example, mission software categorized as CUI.
3	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		3	253			Suggest recognize the explicitly stated document purpose while noting the other things the requirements achieve.	From: Additionally, the enhanced security requirements To: Additionally, while outside the explicit scope of this document, the enhanced security requirements

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
4	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		5	303			Within the context of 171B, it is this CUI that is of interest. Also, secondarily, added text to focus on critical/high and to lay ground work for realization that, despite 32 CFR 2002, some CUI is actually low impact.	From: CUI is no less than To: CUI that is part of a critical program or high value asset is no less
5	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		5	303		Footnote 11	While the footnote has true information with respect to federal IS, this information is non-operational for non-federal systems, the scope of this document. And hence to the intended users of 171B, non-helpful. Also, SP 800-53 does not 'require', but rather provide guidance for control selection. And SP 800-53 is not mandated for non-federal systems, just as FIPS 200 is not.	Delete footnote 11 (The moderate impact value defined in [FIPS 199] may become part of a moderate impact system in [FIPS 200], which requires the use of the moderate baseline in [SP 800-53] as the starting point for tailoring actions.)
6	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		5	309			Stress that it is not change in impact level that 171B is addresssing, but change in likelihood of APT attack.	From: and high value assets targeted by To: and high value assets not primarily because such CUI represents a greater path for harm, but because such CUI is more likely to be targeted by

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
7	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		6	322			Suggest that 'alterative, but equally effective' does in fact satisfy! In fact, it may be a "better" way to achieve the protection intent in a specific organizational/mission context. Bottom line: Suggest it is most helpful to stress "meet the goal" with how not really that important if the goal is met. And suggest it is most hurtful to suggest that meeting the goal is not satisfying the requirement.	From: security measures to compensate for the inability to satisfy a requirement; and To: security measures to satisfy the intent of the requirement; and
8	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		6	329			Related to existing text box in Chapter 3 that correctly states the applicability of the extended requirements. And notes that government does not have to require all of the extended requirements.	From: or designated high value asset. To:or designated high value asset and as mandated by a federal agency in a contract, grant, or other agreement.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
9	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		6	330			To actually "address" as in effectively limit the risk would require literally an order of magnitude increase in cyber defense capability over than needed to comply with 171 as written. And to effectively limit this risk, more than function must be specified; name, trustworthiness of function that is lacking from 171B. Functionality in 171B is difficult to achieve and adding essential trustworthiness moves to goal post even further. Bottom line: It is not clear that 171B is intended to relay a maturity level that even major DIB member are not currently achieving. And if it is that is problematic from level of expectation and what is missing to actually have such maturity.	From: designed to address To: desinged to help address
10	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		6	334			Stating upfront what is made explicit in the introductory text of the mapping appendix.	Append: The mapping to SP 800-53 controls is provided for informational purposes; noting that the related SP 800-53 controls do not provide additional requirements over and above the requirement text in this document.
11	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		6	338			171B is not intended to be prescriptive of mechanisms, but only descriptive.	From: mechanisms and procedures used to implement To: mechanisms and procedures that can be used to implement

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
12	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		6	339			Suggesting text to reinforce the purpose of Discussion section.	From: discussion section is not To: discussion section is informational only and not
13	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		7	359			States: "The contingency planning, system and services acquisition, and planning requirements are not included" Yet note that this is another reason why 171B helps address ATP rather than addresses APT. For example, elements of the CP family (e.g., effective contingency operations), as well as the SA family (e.g., supply chain protections) and PL family (e.g., security architecture) are important elements of effectively addressing the full spectrum APT.	No change suggested, comment reinforces 'helps address" as the better phrase over 'addresses'.
14	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		8	372			Relates to later text in this chapter that relays the government might require only some of the enhanced requirements, not necessarily all.	From: and therefore, requires enhanced protection. To: and therefore, as mandated by a federal agency in a contract, grant, or other agreement requires enhanced protection
15	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		8	372		Footnote 17	Footnote deleted because (1) unnecessary -point is stated in main body of this paragraph and (2) inconsistent text - foot note relates to protecting the critical program and high value assets, but 171B is protecting CUI contained in such and wherever the CUI may be.	Delete footnote 17 (Organizations are cautioned against applying the enhanced security requirements in this appendix to protect all CUI. The application of the requirements is restricted to critical programs and high value assets containing CUI that are likely to be targeted by the APT.)

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
16	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		8	375			It is incorrect to say they only apply to components that … or that provide protection because any component that represents an attack path (e.g., via trust relationships) must be addressed. The changed wording allows for limiting application according to purpose without attempting to define all instances.	From: The enhanced requirements apply only to the components of To: The enhanced requirements must be applied as necessary to protect CUI contained in a critical program or high value assets. The organization may limit application across its enterprise as long as the needed protection is achieved; for example, apply only to the components
17	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		8	376			Provide the other key element in list of examles of what that must be considered in deciding where to apply 171B	From: provide protection for such components. To: provide protection for such components, or that provide an attack path to such components (e.g., due to trust relationships between system components).
18	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		9	411			Not clear how 'being resilient' can be just outsourced as a service. Suggest delete Rationale; As stated unclear how this is a service and other bullets appears to adequately present examples to explain the concept of out sourcing.	Delete "Cyber resiliency"
19	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		10	414			States: "provide the foundation for" Existing text that supports earlier comments related to 'helps address' as opposed to 'addresses'.	No change suggested, comment reinforces 'helps address" as the better phrase over 'addresses'.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
20	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		10	420			Defensive cyber operations is a key, if not THE key, element. The change is intended to explicitly include DCO via the point of 'out maneuvering' the adversary.	From: countermeasures to confuse, To: countermeasures to out maneuver, confuse,
21	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		11	462			Change reinforces the information above that government can require some and not all.	From: when mandated To: as mandated
22	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		12	471			Here and elsewhere: 1. Require that it be made explicit as to what is to be done 2. Recognize that there is no 'one size fits all' for what dual authorization must be employed. Especially at the level of specificity of the 171 family of documents. 3. As current written, noting that absolutes are typically not feasible, requirements become in effect – doing something, anything achieves the requirement as stated. Better to have in the requirement the need to make explicit what is to be done. Then that explicit information will be in the SSP for the government to review.	From: execute critical To: execute explicitly identified critical
23	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		12	478			Ensure discussion is written as informational.	From: The two individuals To: The In that example, the two individuals

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
24	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		12	480			Ensure discussion is written as informational.	From: approved changes. The individuals are accountable for the changes. Organizations also employ dual To: approved change, and the individuals would also be accountable for the changes. Another example is employing dual
25	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		12	484			Organizations will sometimes need to employ non-organizational assets at times (e.g., sponsor or supporting organization)	Append: or otherwise explicitly authorized with consideration of the risk involved.
26	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		12	491			See comment for line 471	From: control information flows To: control explicitly identified information flows
27	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		12	505			Ensure discussion is written as informational.	From: Organizations mandate specific architectural solutions when required to enforce logical or physical separation between systems in different security domains. Enforcement includes; prohibiting To: Organizations consider mandating specific architectural solutions when required to enforce logical or physical separation between systems in different security domains. Enforcement includes; for example, prohibiting

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
28	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		13	515			True, but more likely to confuse than assist DIB companies with protection of unclassified information. Protection of interface with a classified system is NOT the intent of the 171 series. Such protection would be covered by guidance to DIB from classified information security program.	Delete: " There are 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."
29	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		14	524			Added so that this good idea does not appear out of the blue in discussion where requirements are not to be levied.	From: at least annually based or when To: at least annually based upon assessment of effectiveness or when
30	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		16	568			Not part of the requirement. And covered by 3.4.2e	Delete: "Using automated tools, the desired state is compared to the actual state to check for compliance or deviations."
31	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		16	573			The discussion provides for other alternatives. So moved this to list of alternatives in the discussion and added 'respond' to the requirement. (see comment on line 584)	From: 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. To: detect and respond to the presence of misconfigured or unauthorized system components.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
32	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		16	584			See comment for line 573	From: an include halting system functions To: an include remove the components; place the components in a quarantine or remediation network that allows for patching, re-configuration, or other mitigations; halting system functions
33	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		16	586			3.4.2e discussion is written with the presumption that 3.4.1e has been achieved.	Append: This control assumes 3.4.1e.
34	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		17	600			Ensure discussion is written as informational.	From: Organizations also use automated To: Organizations could also use automated

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
35	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		17	603			Add new requirement. Rationale: CM in accordnance with a CM plan is a key element of a mature CM process and would seem to be an important, foundational elemet for achieving the abiltiy to address the APT. (NOTE: Max row hight limit prevents displaying entirety of the suggested change, need to open cell).	Append new requirement: 3.4.4e Implement a configuration management program operated in accordance with an approved, documented, and maintained configuration management plan. DISCUSSION Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual systems. Such plans define processes and procedures for how configuration management is used to support system development life cycle activities. Configuration management plans are typically developed during the development and acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes, how to update configuration settings and baselines, how to maintain system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
36	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		18	607			See comment for line 471	From: establishing a explicitly connection or types of using To: establishing explicitly identified network connections or types of connections using
37	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		18	618			Editorial suggestion to help ensure discussion is written as informational.	From: authentication requirements may only be applied To: authentication requirements might only be applied
38	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		18	621			To avoid requirement appearing first in the discussion.	From: rotation, and management To: rotation, protection, and management
39	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		18	641			Suggest move to SI or CM. Rationale, while this requirement includes "authenticated", IA is not where 53 'authenticates' configurations. That is either SI (e.g., SI-4) or CM (e.g., CM-8). Bottom line: In 53 the IA family is not where configurations are 'authenticated'. (Also see comment for line 642)	Move 3.5.2e to SI or CM.
40	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner			642			Change 3.5.3e to reflect authentication of configuration as device authentication is covered by 3.5.1e. (also see comment for line 641)	From: are known, authenticated, in a properly To: are authenticated to be in a properly

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
41	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		18	644			See comment for line 642 Also this is covered by 3.4.2e	From: Identification and authentication of system components and component configurations can be To: Authentication of component configurations can be
42	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		19	653			Ensure discussion is written as informational. Also this is covered by 3.4.2e	From: unapproved state are placed in To: unapproved state can be placed in
43	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		20	683			Ensure discussion is written as informational.	From: typically include forensic analysts, To: typically include; for example, forensic analysts,
44	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		20	692			CIRT appears to be an example of potential third-party support.	Append: "Additionally, an organization may employ third-party organizations to provide the CIRT capability."
45	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		23	707			See comment for line 471	From: Conduct exenhanced To: Conduct explicitly identified enhanced

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
46	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		23	713	718		Not sure what is intended here with regard to current practices as opposed to something that might happen in the future. I am not aware of any DOD processes similar to DHS contractor suitability that are applied to DIB for access to CUI. DoD personnel screening processes appear to be classified, not CUI focused. How much is expectation and how much is could-be-but-don't-know? If more the latter, then suggest delete. If former, then some examples would seem helpful.	Suggest delete "For individuals … nonfederal organizations." OR Provide examples (that I cannto because not aware of what they would be)
47	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		23	727			Editorial suggestion	From: while the information is resolved To: while the adverse information is resolved
48	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		25	735			Granted, like 53 families this is just a title of a section of requirements in 171 and 171B –yet: 3.11.1e, .2e, 3e, 4e, 6e (most), and 7e are not RA, but rather part of risk mitigation using results of RA in concert with RM decisions.	Suggest consider that rather than significantly overlord the term risk *assessment* with risk response actions, move risk responses to other sections such as IR, SC, and SI.
49	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		25	768			Threat hunting appears to be a capability that might be achieved via third-party support.	Append: An organization may choose to employ third-party providers in achieving this capability.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
50	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		25	772			SOC, as the discussion text relays, deals with threats, not risks (degree organizations, individuals, or the Nation are threaten and typically a combination of likelihood and impact). SOC does not make risk calcuations, as that is the perview of other organizational elements.	From: identify risks to organizations, systems, or system components To: identify threats to organizations, systems, or system components
51	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		26	787			Ultimately the goal is to have risk management inculcated into the system cybersecurity requirements fed into the plan generation process. The plan takes this input and represents the set of 'solutions' that 'best' achieves those requirements. And the plan includes reasons to believe that it does, will fact achieve the requirements. A bottom line: The 171B requirements are much too imprecise to define a capability achieved against any attacker, let alone ATP. Hence compliance with 171B results in indeterminate risk. And hence if risk is to be assessed, and a determination of acceptable risk made and acted upon, that must take place outside of 171B compliance. PS: This is an area where more work will be required over time.	From: security plan the risk basis for security solutionTo: security plan the risk basisa convincing rationale for security solution To: security plan a convincing rationale for security solution

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
52	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		26	791	796		See comment for line 787. Also plan content does not have to include; for example, discussion of AoAs. The plan might include that and such discussion might be helpful, but is not definitional for the content of a good rationale.	Replace with: System security plans relate risk management needs and a set of security requirements to a set of security controls and solutions. The plans provide the rationale for the controls and solutions achieving the security requirements and the risk management need, and, when the APT is a concern, includes specific rationale for ATP-related security requirements being achieved and related risk adequately mitigated. The level of detail provided should be sufficient to enable understanding of whether the plan should be modified in response to changes in threat, operational environment, security control effectiveness, or organizational risk management decisions.
53	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		26	805	806		Assessing solutions is covered by security assessment (as used in 171 and 171B). 3.11.5e is about applying that security assessment in assessment of risk. Issue is risk through the system to organizations, individuals, an and the Nation, not risk to the IS.	From: 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. To: Assess at least annually anticipated risk to t the organization based on current and accumulated threat intelligence and results of security assessment of the effectiveness of security solutions.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
54	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		26	808			The capabilities of "APT" are not constantly changing; and have been pretty consistent for many years. Specific attack paths and TTPs change, yet not as this phrase would indicate. Rather what is really dynamic is the organization's understanding of threat and the organization's assessed risk.	From: Since sophisticated threats such as the APT are constantly changing, the threat awareness and To: The threat awareness and
55	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		26	816			Suggest that a document SCRM plan is essential elment of a foundation for effectively addressing the ATP and therefore is better expressed as part of 3.11.6e instead of a separate 3.11.7e. See comment on lines 828-845	Append: in accordance with a documented organizational supply chain risk management plan

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
56	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		26	817			Add to discussion to reflect addition suggested in comment to line 816. Moved from 3.11.7.e discussion (see comment on lines 828-845)	Append After: The growing dependence on products, systems, and services from external providers, along with the nature of the relationships with those providers, present an increasing level of risk to an organization. Threat actions that may increase risk include the insertion or use of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the supply chain. Supply chain risks can be endemic or systemic within a system element or component, a system, an organization, a sector, or the Nation.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
57	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		27	827			Add to discussion to reflect addition suggested in comment to line 816. Moved from 3.11.7.e discussion (see comment on lines 828-845)	Append after: Managing supply chain risk is a complex, multifaceted undertaking requiring a coordinated effort across an organization building trust relationships and communicating with both internal and external stakeholders. Supply chain risk management (SCRM) activities involve identifying and assessing risks, determining appropriate mitigating actions, developing SCRM plans to document selected mitigating actions, and monitoring performance against plans. SCRM plans address requirements for developing trustworthy secure and resilient system components and systems, including the application of the security design principles implemented as part of life cycle-based systems security engineering processes.
58	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		27	828	845		Incorporated into 3.11.6e as 6e should be done in accordance with 7e and suggest incorporation is better alternative to separate requirements.	Delete and incorporate into 3.11.6e
59	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		28	849			As the discussion relays, pen testing and red teaming are not the same and the discussion mentions both, not just pen testing.	From: Conduct penetration testing at least annually, To: Conduct penetration testing/red teaming at least annually,

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
60	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		28	870			Applies to both pen testing and red teaming	From: The penetration testing team may be To: The penetration testing or red team may be
61	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		28	872			From the SP 800-53A guidance and suggest an important element for effectiveness of this requirement. Otherwise the implementation becomnes just another on-going penetrate and patch exercise that will not be effective against the APT.	Append: Organizations should consider penetration testing/red teaming from perspective of measuring the cybersecurity of the organization as opposed to a primary focus on finding vulnerabilities.
62	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		29	877			See comment for line 471 Also without something more, the requirement is fully achieved by any diversity that accomplishes any reduction. Similar comment for other, similar suggestions.	From: employ diverse system components to reduce the extent of malicious code propagation To: employ identified diverse system components to reduce the extent of malicious code propagation as explicitly deemed necessary for that part of risk mitigation this capability is to provide.
63	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		29	906			Suggest make explicit the balance that must be considered	Append: Organizations should seek to balance cybersecurity value obtained against APT with negative impact on the organizational cybersecurity capabilities resulting from increased complexity and operational effort associated with added diversity.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
64	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		29	910	911		See comment on line 877	From: Disrupt the attack surface of organizational systems and system components through unpredictability, moving target defense, or non-persistence. To: Disrupt the attack surface of organizational systems and system components through identified unpredictability, moving target defense, and/or non-persistence as explicitly deemed necessary for that part of risk mitigation this capability is to provide.
65	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		30	940			Ensure discussion is written as informational.	From: organizations update their management To: organizations can update their management
66	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		30	952			Suggest make explicit the balance that must be considered	Append: Organizations should seek to balance cybersecurity value obtained against APT with negative impact on the organizational cybersecurity capabilities resulting from increased complexity and operational effort associated with added such attack surface disruption.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
67	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		30	956	957		See comment on line 877	From: Employ technical and procedural means to confuse and mislead adversaries through a combination of misdirection, tainting, or disinformation. To: Employ identified technical and procedural means to confuse and mislead adversaries through a combination of misdirection, tainting, or disinformation as explicitly deemed necessary for that part of risk mitigation this capability is to provide.
68	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		31	976			See comment on line 877	From: Employ physical and logical isolation techniques in the system and security architecture. To: Employ identified physical and logical isolation techniques in the system and security architecture as explicitly deemed necessary for that part of risk mitigation this capability is to provide.
69	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		31	1013			Suggest make explicit the balance that must be considered	Append: Organization should explicitly consider the trustworthiness of the isolation techniques in architecting for sufficient risk migration, noting; for example, that logical isolation relies on information technology that would be a high value target because of the function being performed yet with its own set of vulnerabilities.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
70	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		33	1020	1021		Correctness and integrity are different things, not a list of similar. Verifying integrity is VERY different from verifying correctness. Point is to verify integrity and discussion indicate some of the "many way to verify" (as stated in the discussion). Added 3.14.7e for verification of correctness - See comment on line 1167	From: Employ roots of trust, formal verification, or cryptographic signatures to verify the integrity and correctness of security critical or essential software. To: Verify the integrity of security critical or essential software.
71	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		33	1031	1037		Deletion moved to discussion for new correctness requirement. See comment on lines 1020-1021	Delete: Formal verification involves proving that a software program satisfies some formal property or set of properties. The nature of such formal verification is generally time consuming and not employed for most commercial operating systems and applications. Therefore, it would likely only be applied to some very limited uses such as verifying cryptographic protocols. However, in cases where software exists with formal verification of its security properties, such software provides more assurance and trustworthiness and is preferred over similar software that has not been formally verified.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
72	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		34	1068	1070		No different than for any IT. Suggest that the point is that IoT, OT, and IIoT are not overlooked with regard to meeting the requirements of 171B and protection of CUI.	From: 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. To: Ensure that Internet of Things (IoT), Operational Technology (OT), and Industrial Internet of Things (IIoT) systems, components, and devices are included in organizational risk management and addressed in cybersecurity planning and implementation.
73	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		34	1104	1105		I suspect that twice annually is not justifiable as in general either sufficient or necessary. Not sufficient because a much more rapid rate may be required to impact the APT. Not necessary perhaps due to effectiveness of other means being employed. Rather make the organization come to an explicit risk management decision documented in their SSP that the government can then review.	From: Refresh organizational systems and system components from a known, trusted state at least twice annually. To: Refresh organizational systems and system components from a known, trusted state at an identified frequency deemed necessary for that part of risk mitigation this capability is to provide.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
74	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		35	1147			Ensure discussion is written as informational.	From: current activities is removed from To: current activities can be removed from
75	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		35	1156	1157		As indicated earlier, the capability for advance ATP is largely unchanged for many years, and not 'constantly changing. Specific attack paths and to a lesser degree TTPs change, but the general characteristics of threats sources at the high end have been pretty consistent over time. Within DIB by nation state actors seeking to harm our nation, the changes reflect shifts of priority among warfighting areas (e.g., submarine, hyper-velocity missile …). And not substantive changes in nation state capabilities. Bottom line: Such text as constantly changing seems to overlook what remains about the same and causing a focus on vulnerability of the moment changes that we cannot afford to allow to drive our thinking on how to address the APT.	From: The constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), make it essential that threat information relating to To: Threat information relating to

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
76	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		36	1167			Verification of integrity and or correctness are two VERY different things and hence two different requirements. See comment on lines 1020-1021	Append new requirement: 3.14.7e Verify the correctness of security critical or essential software prior to execution. DISCUSSION For example, formal verification involves proving that a software program satisfies some formal property or set of properties. The nature of such formal verification is generally time consuming and not employed for most commercial operating systems and applications. Therefore, it would likely only be applied to some very limited uses such as verifying cryptographic protocols. However, in cases where software exists with formal verification of its security properties, such software provides more assurance and trustworthiness and is preferred over similar software that has not been formally verified.
77	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		66	1222			PM-31 appears to directly map tio 3.11.7e. Note that there is no associated control in Rev 4, PM-31 is from Rev 5	From: SR-2 Supply Chain Risk Management Plan To: PM-31 Supply Chain Risk Management Plan
78	Johns Hopkins Applied Physics Laboratory (JHU/APL)	Gary Stoneburner		67	1224			SA-12(11) appears to directly map to 3.21.1e	From: SR 6(1) Supplier Reviews Penetration Testing and Analysia To: SA-12(11) Supply Chain Risk Management | Penetration Testing and Analysis