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

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

Please submit responses to:
sec-cert@nist.gov by July 19, 2019

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		G	vii	152		0	Currently, companies are relying heavily on the DoD's FAQ for 800-171, but this will not be "official" going forward. Contractors need a way to get clarity on specific requirements, in a way that can be frequently updated and re-evaluated without having to modify the original text. Also, many of the Discussion sections in the -171B draft are already too long, and an FAQ allows for more useful info to be added while keeping the -171B text to a minimum.	Create a NIST-managed FAQ for 800-171 and 800-171B.

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

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	3	251	256	1.1	The sentences beginning with "The enhanced…" and "Additionally, the…" appear to be at odds. The first sentence indicates that all requirements apply "only to components…in a critical program or high value asset." But the latter sentence speaks to broader topics like "penetration resistant architecture", "damage limiting operations", and "designing for cyber resiliency" that go beyond the scope indicated in the prior sentence. If the latter requirements are truly aimed at a larger scope, the first sentence needs to be modified to indicate that some of the requirements have different scopes. Any decision made here should also apply to the blue information box on page 11, line 461.	Clarify sentence based on intended scopes.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		G	6	337	339	2.2	The guidance provided for controls is not always clear on implementation. Consider providing information such as in 800-171A or the "DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented" document, labeling each control with possible methods of implementation such as hardware, software, IT configuration, policy/process, etc.	Add implementation guidance keywords to each requirement to address how it is expected to be implemented.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		G	6	345		2.2	The “discussion” section follows 800-53’s model, but is often too verbose. Consider moving the discussion sections to an appendix, and breaking up each discussion section into 3 discrete sub-parts: - Key Concept: Include definitions of key terms, further explanation of what the control needs to accomplish to meet the requirement, etc. - Justification: Explanation of why the control is needed (e.g. what threat/risk the control is intended to address). If the only reason is “reduce risk of insider threat”, the text is vague and redundant (it should be assumed that all these controls are there to address insider threat). Consider removing this information from EVERY existing and future 800-53 and 800-171 control and adding it to a supplemental document, as it would create the basis for	Move "Discussion" sections to Appendix and break up into definitions, justifications, and examples. Do this in 800-171 as well. Consider taking all justifications out of 800-171 and 800-171B and creating a new supllementary document to serve as a risk register for all of the controls.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		G	6	345		2.2	Discussion sections need to accomplish 2 specific objectives: provide clarity on the intent & scope of the control, and provide guidance on how the control can be achieved. Many of the -171B Discussion sections provide information that is peripheral to these objectives (e.g. provide an explanation of why the control is needed). The language for each Discussion section should be evaluated to determine if it helps address either of these objectives, and modified based on the evaluation.	Limit Discussion sections to 1) clarify & scope information, and 2) guidance on how to implement the control.
	MITRE (InfoSec)		G	7	355		2.2	Use a different numbering scheme that does not create confusion with current -171 controls. For -171B requirements that do not link back to an 800-171 requirement, use something like “3.1.a”, “3.1.b”, etc., with the first numbers matching up with the section of 800-171.	Use a different numbering scheme based on the -171 section being linked to.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		G	7	355		2.2	If the 171B requirement is an explicit expansion of an existing 171 requirement (e.g. more detail about implementation): - make it clear in the numbering scheme that this is an expansion/enhancement of the base control. For example, dual authorization (currently 3.1.1e) is an extension of 3.1.4's separation of duties, so call it "3.1.4.a" or "3.1.4.e1"). - make it clear in the discussion section what the difference is between the original requirement and the expanded details. -- Example: 3.2.1e is an expansion of 3.2.1 (or 3.2.3). The base control is "provide training to people" and this expansion dictates additional kinds of training that must be included to meet the control.	Explicitly link 800-171B controls to 800-171 controls if the new control expands on the original.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		G	7	355		2.2	If 2 controls are similar but have slight variances in scope or objective, the Discussion sections should explicitly reference the other control and note how they are different. - Example: 3.4.2e and 3.5.3e both speak to assessing system components and taking action, but one is aimed at systems residing indefinitely on the network, while the other refers to systems that are joining a network or initiating a connection to another system. 3.4.1e could also be included, as it is designed to be the repository of approved configurations that 3.4.2e and 3.5.3e use to make assessments.	Where an 800-171 and another -171 or -171B control have similarities, explicitly link the controls and describe how the new control differs from the original control.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	8	371		3	DoD does not use "High Value Asset" terminology, they use "Critical Program Information" (CPI). It needs to be clear how these controls are expected to be implemented. Experience indicates that trying to define these requirements in contracts is not effective; either too much stuff gets pulled into scope, or each work order must include explicit information (which is hard for contractors with multiple contracts to parse).	Confirm that terminology is synchronized across the government before attempting to apply it to contractor systems. If it can't be, provide guidance on how it should be interpreted by gov sponsors and contractors.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
			E		379	382	3	The studies referenced in line 379 should be identified and cited as a footnote or Appendix reference. Many of the controls in 800-171B are written as conceptual practices, without specific implementation guidance or evidence of successful implementations. Having access to these studies could provide additional guidance on how organizations can achieve the objectives, and reasonable steps that could be taken to implement them.	Include citation to "studies" referenced in line 379.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		G	9	404		3	Many inquiries have come to us indicating that a fully single, fully-air-gapped system should be able to avoid some portion of the controls. Given that external service providers are now mentioned as a viable alternative, can air-gapping be mentioned as well? Air-gapping is hinted at in some of the controls as an alternative (e.g. IoT), but it would help to have a better, high-level description of whether air-gapping systems is a viable alternative to implementing some or all of the other -171 and -171B controls.	Identify whether air-gapping is a viable alternative (similar to external security providers) to not implementing certain controls.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		G	11	459		3	The concept of limiting scope, as described here, is insufficient. EVERY control in 800-171 and 800-171B needs to be evaluated for scope, and scope should be described in every requirement (or a table in the Appendix). Examples could include: - HVA CUI system only - HVA CUI system and all networking systems protecting the information - All systems with CUI - All systems on the “compliant” network - All systems on the enterprise network - A specific program or function (e.g. having a security team create a honeypot function, or having a process in HR to do background checks). - All employees (e.g. training).	Apply specific scope language to EVERY requirement in 800-171 and 800-171B

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
			G	11	459		3	One of the concepts going along with 800-171B is that contractors would be able to bill the government to implement many of these controls. But per the problem with scope statements for the controls, it's not evident how a contractor would bill many of these controls to the government. Things like 24/7 SOC and subterfuge would be hard to nail down to a sponsor, especially for contractors that work with multiple government sponsors. -171B writers need to consider how each control would be billed to the government.	Evaluate requirements for direct sponsor billing implications.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		G	11	463	464	3	The statement "the requirements apply only to the components of nonfederal systems that process, store, or transmit CUI..." is sensible, but does not align with how many of the controls are written. Many controls in -171 and -171B have nothing to do with systems, and only make sense when applied on a larger scale, but no additional scope language is provided beyond what is written here. Without additional guidance, organizations implementing these requirements are left with the assumption that the requirements only need to be applied in the context of HVA systems. Note that the language here should be kept consistent with that on page 3, line 251. This comment is repeated below for many of the controls where the scope of the control could easily be interpreted to be much	Apply specific scope language to EVERY requirement in 800-171, in particular to those requirements that are not system-oriented (e.g. training). For those requirements that are beyond the scope of HVA, consider holding these off until the next rev of 800-171.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		E	12	471	471	3.1.1e	This would require re-architecting existing workflows, and even re-architecting systems. In the requirement and the discussion, make it clear that “authorization to execute” can be done via sequential processes (e.g. Level 1 mgr signs off, then Level 2 mgr signs off), and does not have to be technically enforced by a system. At a minimum, include clarification that this does not have to be "2 people at the same time" as in missile systems.	Add “processes with” to make the statement “Employ processes with dual authorization…”
	MITRE (InfoSec)		E	12	478	480	3.1.1e	Not needed as these are addressed by other controls.	In the discussion section, remove sentences starting with “The two individuals…” and “The individuals are…”.
	MITRE (InfoSec)		E	12	483		3.1.2e	As written, this would exclude any kind of cloud implementations or vendor appliances, which are standard for many hardware and storage solutions.	Rewrite for clarity: “Restrict direct access to organization networks and systems from any information resource that is not owned, provisioned, or issued by the organization.”

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	12	483		3.1.2e	It is not clear if the language prohibits a non-organizationally-owned device from accessing organizational systems via a managed intermediary like Citrix (i.e. VPN access to an organizationally-controlled VM).	Please clarify.
	MITRE (InfoSec)		E	12	491		3.1.3e	Link this guidance to 800-171 3.1.3 “control the flow”. Explicitly state in the discussion section that this provides enhanced requirements for that control.	Link to 800-171 3.1.3.
	MITRE (InfoSec)		T	12	491		3.1.3e	This requirement appears to be a subset of, if not identical to, 3.13.4e. The Discussion section needs to elaborate on how these requirements are different.	Distinguish between this and 3.13.4e.
	MITRE (InfoSec)		E	12	491		3.1.3e	Where terms have definitions in the Appendix, include a link or footnote to indicate that the term is defined.	Include reference to "security domains" definition in Appendix.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	12	494		3.1.3e	The Discussion section needs to provide examples of different "security domains". We believe this refers to areas where different government agencies' data is mixed (e.g. nuclear and DoD), but the way it is described here could be interpreted very narrowly (Army Project 1 and Army Project 2).	Refine guidance to clarify what different security domains are.
	MITRE (InfoSec)		T	12	491		3.1.3e	This control appears to apply to things like email and SharePoint files, where there are not "domains" (information is segregated by access controls, not flow control mechanisms). This requirement would appear to prohibit those types of solutions, which would affect some valid business models (cataloging research across government domains).	Clarify how "domains" would be applied to systems like email and SharePoint, or explicitly state that storage systems are exempt.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		E	13	516		3.1.3e	The UCDSMO sites do not appear to be accessible. Not sure if this is temporary, or as a result of not having a valid DoD/government login. Any options like this that are DoD-centered should be avoided if possible. 800-171 is intended to be used for all government contractors, not just DoD contractors.	Remove or correct reference to UCDSMO.
	MITRE (InfoSec)		E	14	526		3.2.1e	The discussion section of this control should provide explicit linkage to 800-171 3.2.1 or 3.2.3.	Link to 800-171 3.2.1 or 3.2.3.
	MITRE (InfoSec)		T	14	526		3.2.1e	The control or the Discussion section should clarify that the additional training is only for individuals managing HVA systems.	Please confirm that scope of this control is only for training indivuals supporting HVA systems (see page 11).
	MITRE (InfoSec)		E	14	541		3.2.2e	The discussion section of this control should provide explicit linkage to 800-171 3.2.1, as it provides extended requirements for 3.2.1.	Link to 800-171 3.2.1.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	14	541		3.2.2e	The control or the Discussion section should clarify that the training exercises are only for individuals managing HVA systems.	Please confirm that scope of this control is only for training exercises for indivuals supporting HVA systems.
	MITRE (InfoSec)		T	16	557		3.4.1e	The control or the Discussion should clarify that the repository is just for operating systems and OS components on HVA systems.	Please confirm that scope of this control is only for maintaining an authoritative source of configurations for systems containing HVA.
	MITRE (InfoSec)		E	16	560		3.4.1e	Is this an enhanced version of least functionality (3.4.6), whitelisting (3.4.8), or controlling user-installed software (3.4.9) from 800-171? If so, it should be explicitly noted here. The Discussion section already mentions 3.4.1 and 3.4.4, which is helpful.	Add link to 800-171 controls (if relevant).
	MITRE (InfoSec)		E	16	564	569	3.4.1e	Remove the sentences referring to why the repository is used, as this becomes clear in the next control (3.4.2e).	Remove the Discussion text from "The information in the repository…" through "…check for compliance or deviations".
	MITRE (InfoSec)		E	16	564		3.4.1e	Add link to 3.4.2e, as these controls are inherently linked.	Add link to 3.4.2e.
	MITRE (InfoSec)		E	16	574	574	3.4.2e	Start new sentence with "Remove the components…"	Separate requirement into 2 sentences.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		E	16	577		3.4.2e	The Discussion section should clarify that this control is intended for systems that reside on the network indefinitely, as opposed to 800-171B 3.5.3e, which is intended to be applied as the system/component is joining the network.	Add link and distinction from 3.5.3e.
	MITRE (InfoSec)		T	16	577		3.4.2e	The scope of this control should be clarified. Based on the guidance on page 11, this control would only apply to systems containing HVA.	Please confirm that scope of this control is only for detecting misconfiged/unauthorized systems containing HVA.
	MITRE (InfoSec)		E	16	592		3.4.3e	This requirement appears to be expanding on 800-171 3.4.1 by adding automation, accuracy, timeliness, and availability to the inventory requirement. It should be explicitly stated that these are enhancements to that control.	Link to 800-171 3.4.1.
	MITRE (InfoSec)		T	16	592		3.4.3e	The scope of this control should be clarified. Based on the guidance on page 11, this control would only apply to systems containing HVA.	Please confirm that scope of this control is only to inventory systems containing HVA.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		E	18	616	619	3.5.1e	Remove sentence starting with "For some architectures…" as a built-in exception to the control is not appropriate (would be ideally put into a FAQ).	Remove sentence starting with "For some architectures…"
	MITRE (InfoSec)		T	18	621	623	3.5.2e	Are password managers not required if the system supports multifactor auth or complex account management?	Clarify intent.
	MITRE (InfoSec)		T	18	621		3.5.2e	"Password manager" is not defined. Can we use a password manager that is on somebody's phone? Does it have to accomplish generation, rotation, and management to be compliant?	Clarify intent.
	MITRE (InfoSec)		E	18	634	639	3.5.2e	Remove sentences at the end of the Discussion section as these are not relevant to understanding how to implement the requirement.	Remove sentences from "Personnel turnover…" to "security module)."

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	18	641	643	3.5.3e	Does this requirement apply only to connecting to systems with HVA? The control is written in such a way that it could be implied that any system connecting to the organizational network, but that scope exceeds the HVA scope identified on page 11.	Please confirm that scope of this control is only for system components connecting to systems containing HVA.
	MITRE (InfoSec)		E	18	641		3.5.3e	This control should reference 3.4.2e, as this is a variation of that control.	Add link to 3.4.2e.
	MITRE (InfoSec)		E	20	659		3.6.1e	Line 666 indicates the SOC needs to be 24/7, so this detail should be explicitly stated in the requirement itself.	Change "full-time" to "24/7".
	MITRE (InfoSec)		G	20	659		3.6.1e	For this control, like many others in -171B, it is not clear how contractors would bill the implementation of the control back to the government.	Clarify how contractors would bill a gov sponsor for this activity.
	MITRE (InfoSec)		T	20	659		3.6.1e	The scope of this control should be clarified. Based on the guidance on page 11, this control would only apply to a SOC overseeing enclaves and systems that contain HVA.	Clarify scope to only address SOC's oversight of HVA.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		E	20	678	679	3.6.2e	The goal of this requirement is to address cyber incidents, so deployment to “any location” is usually irrelevant. The critical factor is being able to address any sort of cyber incident within 24 hours, and the language should reflect this.	Change “deployed to any location” to “deployed to address any cyber incident”

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		E	23	707	708	3.9.1e	"Trustworthiness" is not a valid objective for personnel screening. There is no way to objectively assess trustworthiness. The requirement should be scaled back to just reviewing behavior/conduct periodically. At most, the Discussion section should reference activities that might be flags that would result in further evaluation, monitoring, etc. Also, non-federal institutions may be subject to limits on vetting by national, state, and local laws. The language should acknowledge that those laws should dictate what/when/how screening can and should be performed. The existing language borders on privacy issues.	Rewrite for clarity: "Restrict direct access to organization networks and systems from any information resource that is not owned, provisioned, or issued by the organization."
	MITRE (InfoSec)		T	23	707	708	3.9.1e	Clarify if this is only for people with access to HVA systems.	Please confirm that scope of this control is only for systems containing HVA.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	23	710		3.9.1e	The Discussion section provides no guidance on what sort of behaviors or findings would constitute red flags.	Clarify expectations.
	MITRE (InfoSec)		E	23	710		3.9.1e	This control is closely tied to 3.9.2e and 3.14.2e. Description should reference this.	Link to 3.9.2e and 3.14.2e.
	MITRE (InfoSec)		T	23	723		3.9.2e	“Trustworthiness” is not a valid objective for personnel screening. There is no way to objectively assess trustworthiness. The requirement should be scaled back to just reviewing behavior/conduct periodically. At most, the Discussion section should reference activities that might be flags that would result in	Rewrite to: “Ensure that potential issues related to employee conduct and behavior are addressed such that organizational systems are protected.”
	MITRE (InfoSec)		T	23	726		3.9.2e	The Discussion section should address things like additional monitoring, mental health assistance, mentoring, role changes, and other pro-active measures to address issues related to an individual’s conduct and behavior.	Modify guidance to provide appropriate recommended actions for conduct/behavior issues.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		E	23	726		3.9.2e	This control is closely tied to 3.9.1e. Description should reference this.	Link to 3.9.1e.
	MITRE (InfoSec)		E	25	737		3.11.1e	This requirement should focus on using threat intelligence to develop security requirements, which would then inform these activities. If the intent is to use more advanced attack models, see below.	Change to "Employ threat intelligence to inform the creation of security requirements. Use requirements to: develop systems and architecture, select security solutions, and inform monitoring, threat hunting, and response and recovery activities."
	MITRE (InfoSec)		E	25	737		3.11.1e	If the intent is to encourage companies to use potential adversary attack models to inform various activities, the language should be clarified.	Rewrite to: “Employ adversary tactics and techniques beyond traditional indicators of compromise (IoCs) or signatures of malicious activity to inform the development of: system and security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.”

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	25	737		3.11.1e	It is not clear how compliance with this control (as written) could be assessed. Do new solutions, architectures, etc., have to demonstrate evidence that threat information was used in the decision? Does a system have to be created to track evidence that threat information was used? How do you document proof that threat information was used to inform development? How does a contractor show that threat information was used effectively?	Please clarify.
	MITRE (InfoSec)		T	25	737		3.11.1e	It is unclear whether this control would actually achieve risk reduction. Threat intelligence does not necessarily translate into product development/selection.	Consider removing this control from the first version of -171B.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		E	26	781	785	3.11.3e	This requirement focuses on the solution to the problem, not on the problem that needs to be solved. The language should be more open-ended to facilitate future solutions that may address the same issue in a better way than existing capabilities.	Rewrite to: “Employ a means to analyze available sources of information to predict and identify the risks presented by APT.”
	MITRE (InfoSec)		E	26	781	785	3.11.3e	Content is not relevant to the implementation of the control.	Remove the sentences from “Note, however,…” through “…are not able to conceal their activity.”
	MITRE (InfoSec)		E	26	787	789	3.11.4e	Run-on sentence, start second sentence with "Identify the system…"	Separate requirement into 2 sentences.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		E	26	789		3.11.4e	The final portion of this requirement, "dependencies on external service providers", should be a separate requirement. With DFARS external service providers are not handled via 800-171, but instead are subject to FedRAMP requirements. This is the first inference in 800-171 that external service providers are going to be part of -171 requirements, which is an important distinction.	Remove "dependencies on external service providers" and move this to a separate requirement. From the Discussion section, remove "When incorporating external… to "…by the service provider" to the Discussion section for the new requirement.
	MITRE (InfoSec)		T	26			3.11.4e	It is not clear how the "risk basis for security solution selection" would be described. Many products are selected based on cost or other non-security factors, or selected by executive decision where the decision criteria is not documented. In order to implement this requirement, more guidance is needed on what, exactly, needs to be documented.	Clarify requirement.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		E	26	791		3.11.4e	This requirement is a direct expansion to 800-171 3.12.4. It should be linked in the description.	Link to 3.12.4.
	MITRE (InfoSec)		T	26	791		3.11.4e	The language should explicitly limit the scope of the requirement to only systems with HVA, so it is not misinterpreted.	Please confirm that scope of this control is only for systems containing HVA.
	MITRE (InfoSec)		E	26	805		3.11.5e	It makes more sense to assess the "capabilities" of security solutions to address anticipated risk than the "effectiveness" of security solutions.	Change "effectiveness" to "capabilities".
	MITRE (InfoSec)		T	26	805		3.11.5e	The term "security solution" is not defined in the Appendix.	Define "security solution".

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	26	818	820	3.11.6e	There is insufficient guidance provided on how to assess and monitor supply chain risk. 800-161 refers to 800-53 controls that do not necessarily apply to 800-171 contracts. Mechanisms to assess, document, and monitor risks are not defined in the context of -171, and it is not clear if third party providers exist to assist with this task. NIST needs to provide additional guidance on how to flow requirements down and identify means of assessments for primes.	Additional guidance needed.
	MITRE (InfoSec)		E	27	828	829	3.11.7e	A plan/program must also be implemented in order to be successful. Also recommend changing "plan" to "program" to indicate and on-going effort to achieve a particular strategy.	Sentence should begin “Develop, implement, and regularly update a process for managing supply chain risks…”

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	27	831	845	3.11.7e	There is insufficient guidance provided on how to assess and monitor supply chain risk. 800-161 refers to 800-53 controls that do not necessarily apply to 800-171 contracts. Mechanisms to assess, document, and monitor risks are not defined in the context of -171, and it is not clear if third party providers exist to assist with this task. NIST needs to provide additional guidance on how to flow requirements down and identify means of assessments for primes.	Additional guidance needed on how risk is assessed and calculated.
	MITRE (InfoSec)		E	28	858	872	3.12.1e	Extra descriptive language is not needed for this Discussion section.	Delete all language starting with “Such constraints include…” to "…in its assessment."
	MITRE (InfoSec)		T	29	877		3.13.1e	This is not written as a requirement that can be definitively implemented or assessed. What evidence can be provided to determine if the control is implemented?	Remove this control from the initial version of -171B to gather additional guidance on how the requirement could be implemented. If control is not removed, please define how this would be implemented/assessed.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	29	877		3.13.1e	It is not clear that this would provide actual risk reduction. What metric would provide evidence that this control is working effectively?	Please clarify how the control could be demonstrated to be working effectively.
	MITRE (InfoSec)		T	29	879	893	3.13.1e	It is not clear what scope this control is intended to cover. If a single system with just an OS has HVA, how would the control be implemented? The control only makes sense if implemented across an enterprise, but that is in direct contrast to the scope guidance provided on page 11.	Please confirm that scope of this control is only for systems containing HVA.
	MITRE (InfoSec)		T	29	879	893	3.13.1e	Although 800-171B is intended to enable billing sponsors for implementating the controls, it is not clear how this control could be billed back to a sponsor.	Provide guidance on how cost of this control could be appropriately billed to a sponsor.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	29	910		3.13.2e	This is not written as a requirement that can be definitively implemented or assessed. What evidence can be provided to determine if the control is implemented?	Remove this control from the initial version of -171B to gather additional guidance on how the requirement could be implemented. If left in the list, label it as "not selected" as other 800-53 controls have been.
	MITRE (InfoSec)		T	29	910		3.13.2e	It is not clear that this would provide actual risk reduction. What metric would provide evidence that this control is working effectively? What industry examples demonstrate effective implementation of this control?	Please clarify how the control could be demonstrated to be working effectively.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	29	913	928	3.13.2e	It is not clear what scope this control is intended to cover. If a single system has HVA, how would unpredictability, moving target defense, and/or non-persistence be implemented? The control only makes sense if implemented across an enterprise, but that is in direct contrast to the scope guidance provided on page 11.	Please confirm that scope of this control is only for systems containing HVA.
	MITRE (InfoSec)		T	29	913	928	3.13.2e	Although 800-171B is intended to enable billing sponsors for implementating the controls, it is not clear how this control could be billed back to a sponsor.	Provide guidance on how cost of this control could be appropriately billed to a sponsor.
	MITRE (InfoSec)		E	30	956		3.13.3e	This is not written as a requirement that can be definitively implemented or assessed. What evidence can be provided to determine if the control is implemented?	Remove this control from the initial version of -171B to gather additional guidance on how the requirement could be implemented. If left in the list, label it as "not selected" as other 800-53 controls have been.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	30	956		3.13.3e	It is not clear that this would provide actual risk reduction. What metric would provide evidence that this control is working effectively? What industry examples demonstrate effective implementation of this control?	Please clarify how the control could be demonstrated to be working effectively.
	MITRE (InfoSec)		T	30	959	974	3.13.3e	It is not clear what scope this control is intended to cover. As written, the deception and tainting would only be done on system(s) with HVA. The control only makes sense if implemented across an enterprise, but that is in direct contrast to the scope guidance provided on page 11.	Please confirm that scope of this control is only for systems containing HVA.
	MITRE (InfoSec)		T	30	959	974	3.13.3e	Although 800-171B is intended to enable billing sponsors for implementating the controls, it is not clear how this control could be billed back to a sponsor.	Provide guidance on how cost of this control could be appropriately billed to a sponsor.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		E	31	976		3.13.4e	This requirement is an extension of 800-17 3.1.3 (control the flow), and is extremely similar to 800-171B 3.1.3e (employ solutions to limit transfer of data). The Discussion section should include explicit references to both requirements, and be clear about how they differ and/or expand on each other.	Consider merging this requirement with 3.1.3e. Otherwise, link to 3.1.3 and 3.1.3e.
	MITRE (InfoSec)		E	31	976		3.13.4e	The current language implies that both physical AND logical isolation techniques must be employed for HVA systems in order to comply with the control. While there are some use cases where both can be employed, requirnig both to be employed (especially physical) significantly reduces the types of architectural options than can be considered. A single	Change to "Employ physical and/or logical isolation techniques..."

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	31	978	1013	3.13.4e	Many system options (SharePoint, email, etc.) and cloud providers are not capable of utilizing physical AND logical isolation of data. This requirement seems to imply that those types of systems would be prohibited from handling HVA.	Please clarify.
	MITRE (InfoSec)		T	33	1020	1021	3.14.1e	"Security critical or essential software" is not defined. How does this relate to HVA? The terminology is nebulous enough that it could be applied to just a handful of systems, or it could require a sizeable project just to identify all of the relevant systems.	Define "security critical or essential solution" in the context of the scope of HVA, or use HVA-specific language.
	MITRE (InfoSec)		E	33	1048		3.14.2e	As written, the control feels like it should already be in place based one or all of 800-171 3.13.1, 3.14.6, 3.14.7, and 800-171B 3.9.1e. Excplicitly describe how it enhances or differs from them, and provide links to the control(s) it relates to.	Clarify distinction from, and link to, one or more of 3.13.1, 3.14.6, 3.14.7, and 3.9.1e.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	33	1048	1063	3.14.2e	As written, this control only applies to suspicious behavior on HVA systems (per scope statement on page 11).	Please clarify that this control is only for suspicious behavior on HVA systems.
	MITRE (InfoSec)		T	34	1072		3.14.3e	The Discussion section should clarify that, per the language on page 11, the scope of this control is only for IoT that connect or interact with HVA.	Clarify scope to only address IoT interacting with HVA.
	MITRE (InfoSec)		E	34	1088	1095	3.14.3e	Much of the Discussion section is aimed at describing the risk, instead of the methods of implementing the control. This information is appropriate for a supplementary document (e.g. a risk register), but is not needed for -171B.	Remove sentences from "The recent convergence..." to "...significant cyber threat."

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		E	34	1098	1102	3.14.3e	The portion of this control dedicated to protecting devices that can not be made compliant is problematic. The purpose of an IoT device is often tied to its ability to connect directly to the Internet. While adding intermediary monitoring devices and segretating the IoT off to its own network segment make sense, isolation from the Internet does not. The language should supply a built-in exception, and should require the contractor to assess and accept the risk.	Remove sentences from "But such mitigating..." to "...hostile cyber-attacks."

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		E	34	1104	1105	3.14.4e	The control assumes organizations have the capability to have system data and configuration files that can easily be exported to a backup state, then re-imported to a new or similar system such that the new system is immediately operational. This makes some sense if the user is just working on MS Office files, but is not viable when multiple vendor OS and applications are used and a fresh install requires manual configuration. The operational and data integrity impacts of this control are significant. A more sensible version of this control is to change the focus from "twice annually" to "when there are indicators of compromise", which is a practice most mature companies should already be doing.	Suggest changing language from “at least twice annually” to “…trusted state when there are indicators of compromise.”

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	34	1107	1136	3.14.4e	This concept is only described conceptually, and does not provide evidence of tools that facilitate this capability, or provide empirical evidence that it is an effective mitigating technique to use against APT. The operational challenge and data integrity issues arising from restoring from backups make it questionable how valuable this control would be. There also is no assurance that any issues associated with APT compromise would not simply be re-installed when the system/data was restored from a backup, which would eliminate any risk mitigation benefit of implementing the control.	If the focus of the control is not changed to address systems that are suspected of compromise (see earlier comments), suggest removing this control from -171B, or changing it to "Not Selected", until it can be adequately reviewed by industry and security experts.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	35	1140	1150	3.14.5e	This requirement assumes organizations already have a way to label individual data elements, establish what appropriate ages for those elements are, and remove them automatically. Retention of CUI is often dictated by contractual requirements, which will override any other sources of retention guidance.	The requirement needs to focus on establishing and enforcing contractual requirements for purging CUI. If this is what is meant by "disposition schedules", the language should be clarified.
	MITRE (InfoSec)		T	35	1140	1150	3.14.5e	This requirement does not indicate that the scope statement on P. 11 indicates this should only be for CUI associated with HVA systems.	Please clarify that this control is only for purging CUI from HVA systems.
	MITRE (InfoSec)		E	35	1146	1149	3.14.5e	Moving information to offline storage does not meet the Description's definition of purging, and should either be removed from the Discussion section, or added to the language of the 3.14.5e requirement.	Remove the sentence "Alternatively, information…"

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	MITRE (InfoSec)		T	35	1137		3.14.5e	Some use cases of CUI (e.g. research results) are specifically intended to be retained and available after the project is completed. This use case should be addressed in the Discussion section, such that it is not unintentionally prohibited by an interpretation of the requirement language.	Add acceptable caveat for research information that it intended to be available for future use.