Raytheon Company
880 Technology Park Drive
Billerica, MA 01821
USA

August 1, 2019

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899

Subject: NIST Special Publication 800-171 B *Enhanced Security Requirements for Critical Programs and High Value Assets* and 800-171 Rev 2 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* Drafts Comments

Raytheon Company has reviewed the NIST's Special Publication. Our comments are included below, along with our rationale and recommendations:

SP 800-171 B

1. **Comment Type:** General
   Comment: The Defense Department (DoD) Office of Under Secretary Acquisition of Sustainment is creating a new Cybersecurity Maturity Model Certification (CMMC) to streamline DoD's cybersecurity acquisition processes. Special Assistant to DoD's Assistant Secretary of Defense Acquisition for Cyber Katie Arrington is working with Johns Hopkins University Applied Physics Laboratory and Carnegie Mellon University Software Engineering Institute in partnership with the ND-ISAC to develop maturity levels four and five for protecting CUI against advanced persistent threats (APTs). The collaborative effort is actively reviewing best practices from Cleared Defense Contractors who have successfully defended their networks from APT. The result will be the identification of process and operations that provide proven methods for successful defense of APTs.
   Suggested Change: Suspend implementation of SP 800-171 B and support the implementation of the CMMC, requiring maturity levels four and five for critical programs and high value assets.

2. **Comment Type:** General
   Comment: The vast majority of attacks for almost a decade have come in the form of socially engineered emails, yet there is no requirement or even discussion of email screening as a defense measure. Those companies that have been most successful against the APT have invested heavily in this area. This is a far better use of investment dollars, employee labor and intellectual capital than some of the other controls in this document that have been discussed for years in theory but never successfully put into practice.

Raytheon Company
880 Technology Park Drive
Billerica, MA 01821
USA

Suggested Change: Add a control for email operations in the form of email screening, sandboxing, and blocking capabilities.

3. **Comment Type:** General
   Comment: Control 3.1.1e *Employ dual authorization to execute critical or sensitive system and organizational operations.* This approach raises multiple concerns. 1. "Sensitive Operations" is a vague term that will be subject to broad interpretation by agencies or different contracting officers with a single agency. 2. Is this to be implemented as a technical control (like PKI cage work) or a policy control with auditability? Without a technical control, this has little value against advanced threats. With a technical control and large list of operations, this could quickly become a very complex and expensive effort far in excess of the risks mitigated
   Suggested Change: Remove this requirement.

4. Comment Type: General

   Comment: Control 3.3.1.3e *Employ secure information transfer solutions to control information flows between security domains on connected systems* is not appropriate for a NIST publication covering unclassified APT controls. The requirements for cross-domain solutions are controlled by DoDI 8540.01 Cross Domain Policy and other applicable regulations beyond the scope of NIST 800-171B

   Suggested Change: Remove this requirement.

5. **Comment Type:** General
   Comment: In control 3.6.1e *Establish and maintain full-time security operations center capability*, the discussion section references the differences between large and small business as to the type of strategy they should use to comply with this control. The discussion section also details an implementation example that seems to imply the need of a manned 24/7 SOC as the definition of a dedicated SOC. In practice, a SOC needs to operate during the hours appropriate to their business model. Because the vast majority of incidents start with some employee action, most businesses would be well served with a SOC operating the same hours as the employees (across all regions), which may well not be 24/7. In addition, most companies would not have employees available outside the SOC to address issues during non-business hours.
   Suggested Change: Recommend removing the requirement for 24/7 and replacing the sentence to read, "Implementation of a dedicated SOC or use of third party providers are acceptable solutions"

6. **Comment Type: General**
   Comment: Control 3.9.1e *Conduct enhanced personnel screening (vetting) for individual trustworthiness and reassess individual trustworthiness on an ongoing basis.* Depending

on what is actually required in practice by any given contract, the difference in the cost of extended investigation can be significant, especially in large companies where it would apply to thousands of employees. In addition, given the plethora of examples of data loss from highly cleared and highly vetted individuals, the effectiveness of this measure is questionable.

Suggested Change: Recommend removing this requirement beyond a requirement for basic pre-employment background investigations.

7. **Comment Type:** Technical

   Comment: Control 3.11.1e *Employ threat intelligence to inform the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.* The use of the term "threat intelligence" to inform the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, and response and recover activities is vague and should be expanded to clarify what exactly needs to be accomplished from a cyber-operational perspective from "threat intelligence" of the APT. For example, you could call out the DoD's DODCAR (formerly known as NIPRNet/SIPRNet Cyber Security Architecture Review), which was built from threat intelligence from years of APT activity and informs what architectures and TTPs should be employed to defeat the APT during the cyber-attack and exploitation lifecycle. Not citing anything and leaving it vague opens industry up to a lot of interpretation and non-standard approaches, and knowing these controls will be audited, leaves industry open to undue risk from auditors interpreting cyber approaches differently from DIB entity to DIB entity.

   Suggested Change: Recommend inserting DODCAR or other examples for acceptable threat intelligence.

8. **Comment Type:** General

   Comment: Control 3.11.3e *Employ advanced automation and analytics capabilities to predict and identify risks to organizations, systems, or system components.* This reads as a requirement to purchase and deploy artificial intelligence and machine learning in the SOC. Although there are plenty of people selling these solutions, the utility has not been demonstrated yet. Cost of such tooling might be better spent on other areas to improve overall security. Demanding “AI” in the SOC is overly prescriptive.

   Suggested Change: Remove this requirement.

9. **Comment Type:** General

   Comment: Control 3.11.4. *Document or reference in the system security plan the risk basis for security solution selection and identify the system and security architecture, system components, boundary isolation or protection mechanisms, and dependencies on external service providers.* While it is no doubt a good thing to tie investment and

architecture decisions to risk, creating a paper trail for such activities does nothing to protect against APT attacks.

Suggested Change: Remove this requirement, as it does not contribute to APT defense.

10. **Comment Type:** Technical

Comment: Control 3.13.1e *Employ diverse system components to reduce the extent of malicious code propagation.* Employing diverse system components to reduce lateral movement and cyber exploitation TTP's should be balanced with cyber risk, other available cyber defense TTPs and cost for blue force cyber operations. Additionally, there is no good metric to measure what is good enough for network diversity. This is a nightmare to manage with different software products, update cycles, contract maintenance, training cyber personnel. Diversity does not appreciably slow down the most ambitious hacker going after the "crown jewels."

Suggested Change: Strongly recommend deleting this section until and unless the government can demonstrate an instance where this has been done successfully in industry or government at scale. The government should also demonstrate that this mitigation has actually been effective in stopping data loss enough to justify the cost—which is the essence of a risk managed effort.

11. **Comment Type:** Technical

Comment: Control 3.13.2e *Disrupt the attack surface of organizational systems and system components through unpredictability, moving target defense, or non-persistence.* "Unpredictability, moving target defense, or non-persistence" is not possible even on a small scale the way it is described in this section.. The tactics described in this section such as moving storage locations and re-imaging assets are valid TTPs but do not scale, and DoD does not even do this with CUI. For Industry it would be cost prohibitive and so disruptive of on-going operations that it would do more harm than good. .

Suggested Change: Remove this requirement, as it is neither achievable nor effective at scale unless DoD can demonstrate an instance in DoD or industry where this has been done successfully at scale and can demonstrate that it has successfully mitigated attacks where no other less disruptive method would have succeeded.

12. **Comment Type:** General

Comment: *Employ technical and procedural means to confuse and mislead adversaries through a combination of misdirection, tainting, or disinformation.* None of the cited examples in this section has ever been tried at scale, much less proven to be effective enough to justify the costs. The level of effort required to implement and sustain such deceptions is high and the ability to maintain such deceptions over time and across all organizations is questionable at best.

Raytheon Company
880 Technology Park Drive
Billerica, MA 01821
USA

Suggested Change: This requirement should be removed until and unless the government can demonstrate either government or industry examples, where this measure has been successfully implemented at scale and has had the desired effect.

13. **Comment Type:** General
    Comment: Control 3.14.1 Employ *roots of trust, formal verification, or cryptographic signatures to verify the integrity and correctness of security critical or essential software.* This control, as stated in the description, is impractical for all but a very few corner cases. It is a great control in theory but in practice, it is unrealistic.
    Suggested Change: Remove this requirement until and unless the government can demonstrate that it has been successfully implemented at scale either in government or in industry and that it has been a factor in mitigating against successful attacks.

14. **Comment Type:** General
    Comment: Control 3.14.2e *Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior,* requires monitoring of "Individuals" and "System Components," both are covered independently and in conjunction in several controls on the 800-171 Rev 1, and NIST 800-171 Rev 2 Draft already. No enhancement value added from this control.
    Suggested Change: Remove this requirement.

15. **Comment Type:** General
    Comment: Control 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.* The control uses the word isolation which can be interpreted as placing systems in a non-connected environment, making it useless (i.e., camera feeds need a network connection).
    Suggested Change: Recommend changing the word to "Segregated"

16. **Comment Type:** Technical
    Comment: Control 3.14.4e *Refresh organizational systems and system components from a known, trusted state at least twice annually.* No organization in DoD or industry does this. From a cyber operational or IT sustainment perspective, this is impossible to do at scale. Rebuilding systems from scratch twice a year would bring most programs to a halt for an extended period and require a huge increase in internal or external IT support in companies with thousands of servers.
    Suggested Change: Remove this requirement, as it is neither achievable nor practical at scale.

SP 800-171 Rev 2

Raytheon Company
880 Technology Park Drive
Billerica, MA 01821
USA

1. **Comment Type:** General
   Comment: The previous 800-171 version includes the words "For Example" to provide possible solutions that can help implement a control. These two words were removed from the Rev 2 publication changing the language from a possible solution to an actual solution. In some of the controls, it seems they were removed without content consideration.
   Suggested Change: Recommend changing the word "include" to "can include."

2. **Comment Type:** General

   Comment: The reference to NARA's CUI Marking Handbook in the discussion section for Control 3.8.4 (*Mark media with necessary CUI markings and distribution limitations*) is confusing. Private contractors often receive direct instructions for marking CUI via contract from their USG agency customers such as DOD that conflict with the marking guidance in the NARA CUI Marking Handbook. In addition, USG agency customers such as DoD generally do not reference the NARA CUI Marking Handbook in their marking instructions at the current time. Therefore, the insertion of the reference to NARA's CUI Marking Handbook here risks creating misunderstandings regarding whether contractors will be deemed to have not implemented Control 3.8.4 if they duly follow USG agency-mandated marking instructions that conflict with or do not reference the NARA CUI Marking Handbook. .

   Suggested Change: Recommend deleting or clarifying this reference to the NARA CUI Marking Handbook.

3. **Comment Type:** Editorial
   Comment: The hyperlink to the NARA marking website is broken on the discussion section for Control 3.8.4 *Mark media with necessary CUI markings and distribution limitations*
   Suggested Change: Add hyperlink to the NARA CUI section - https://www.archives.gov/cui

SP 800-171 Rev 2 and 800-171 B

1. **Comment Type:** General

   Comment: The NIST 800-171 Rev 1 document made clear that the "discussion" section accompanying each control did not change the scope of each control for the purpose of audits or assessments. Specifically, it included this language: *"The discussion is not intended to extend the security requirements or the scope of the assessments of those requirements."* However, the corresponding language in the draft NIST 800-171B and NIST 800-171 Rev 2 documents drops the underlined language above and only states, *"The discussion section is not intended to extend the scope of the requirements."* This change, combined with the fact that the discussion sections no longer appear in an

Raytheon Company
880 Technology Park Drive
Billerica, MA 01821
USA

appendix and now appear right next to each corresponding control, will lead to a new source confusion about whether the discussion language changes the scope of each underlying control.

Suggested Change: Recommend inserting language in both the draft NIST 800-171B and NIST 800-171 Rev 2 documents making clear that the discussion sections **"do not"** change the scope of each control for the purpose of audits or assessments.

Thank you for soliciting and considering our comments.

Jeffrey C Brown

Digitally signed by Jeffrey C Brown
Date: 2019.08.01 21:06:36 -04'00'

Jeff Brown
Vice President and Chief Information Security Officer
Raytheon Company