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

Background

Publications in NIST's Special Publication (SP) 800 series present information of interest to the computer security community. These documents support the security and privacy needs of U.S. Federal Government information and information systems. NIST develops SP 800-series publications in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq*., Public Law (P.L.) 113-283.

Federal Government statutes (e.g., FISMA 2014), regulations, and policies (e.g., Office of Management and Budget Circular A-130) may specify whether federal agencies are required, or encouraged, to comply with NIST's SP 800-series publications. NIST's SP 800 series publications shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems.

Changes Proposed by This Document

Draft NIST SP 800-171B was developed in the spring of 2019 as a supplement to NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, to offer additional recommendations for protecting Controlled Unclassified Information (CUI) in nonfederal systems and organizations where that information runs a higher than usual risk of exposure. When CUI is part of a critical program or a high value asset (HVA), it can become a significant target for high-end, sophisticated adversaries (i.e., the advanced persistent threat (APT).

The enhanced security requirements in Draft NIST SP 800-171B are supplemental and do not impact the basic and derived security requirements contained in NIST SP 800-171, nor the scope of the implementation of the NIST SP 800-171 security requirements.

Draft NIST SP 800-171B provides a set of enhanced security requirements to protect the confidentiality of CUI in nonfederal systems and organizations from the APT. The enhanced security requirements provide the foundation for a new multidimensional, defense-in-depth protection strategy that includes three, mutually supportive and reinforcing components: (1) *penetration resistant architecture*; (2) *damage limiting operations*; and (3) designing for *cyber resiliency* and *survivability*. Please note the following section and pages as part of your review:

- All Content in Draft SP 800-171B
- Draft SP 800-171, Revision 2, General removal of APT discussions in section 1.3 and 2.0 that was shifted to Draft SP 800-171B. These changes are found on pages 3 and 4.

The enhanced security requirements are not required for any particular category or article of CUI, rather are focused on designated high value assets (HVAs) or critical programs that contain

CUI. These HVAs and critical programs are potential targets for the APT, and thus, require enhanced protection. The enhanced security requirements are to be implemented in addition to the basic and derived requirements in NIST SP 800-171, since the basic and derived requirements are not designed to address the APT.

The enhanced security requirements apply only to components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components when the designated CUI is contained in a critical program or HVA. The enhanced security requirements are only *applicable* for a nonfederal system or organization when *mandated* by a federal agency in a contract, grant, or other agreement.

This document is considered significant guidance under Executive Order (EO) 12866, *Regulatory Planning and Review*. Per OMB guidance in EO 12866 and in EO 13771, *Reducing Regulation and Controlling Regulatory Cost*s, a preliminary estimation of costs associated with this guidance document has been created and follows below.

Expected Impact of this Proposed Guidance

Background

Currently, the Defense Federal Acquisition Regulation (DFARS) clause 252.204-7012 requires contractors to implement basic cybersecurity requirements if processing DoD controlled unclassified information (CUI) on their unclassified information systems.

Draft NIST SP 800-171B is intended to apply on a contract-by-contract basis for a critical programs with the costs to implement and maintain these additional protections typically being an allowable contract cost to the government.

DoD estimates the number of contractors that develop DoD's most critical capabilities is a very small subset of the overall Defense Industrial Base, and the requirements in Draft SP 800-171B would affect less than one-half of one per cent of an overall contractor base of over 69,000 contractors that currently process DoD CUI. The companies affected range from large to small companies, with the small companies involved in developing very specialized or emerging technologies.

The impact on any particular company may vary considerably, depending on their current infrastructure and development environment, and also the composition of their customer base. The additional requirements in Draft NIST SP 800-171B affect a company's information system, so the size, complexity and how the information system is used are all relevant to the cost of implementation. Companies will determine the approach to meeting the requirements that best fits their needs.

Draft NIST SP 800-171B includes 32 new security requirements building upon the 110 requirements in NIST SP 800-171 (currently required by the DFARS clause). The primary factor affecting the cost of implementation is the Draft NIST SP 800-171B requirement to 'employ physical and logical isolation techniques in the system and security architecture' and related

requirements. This requirement generally means isolating the IT environment where critical program capabilities are developed from the IT environment processing other CUI, or developing commercial products. Other Draft NIST SP 800-171B requirement costs can be categorized into 'Process and IT configuration' costs and 'Security Operations Center (SOC)/Threat' costs.

The size of a company may affect how it implements the requirements of Draft NIST SP 800-171B and thus the overall cost. Companies involved in critical programs and technologies tend to be either large (engaged in large program/technology development) or small (focused on specialized technologies or their application), with a few medium-sized companies. Another factor is whether the company does business solely with DoD, or has a mix of commercial and DoD customers.

Large (or very large) companies, while relatively few in terms of individual firms, operate multiple facilities, often with the facility and its information network dedicated solely to DoD programs or a specific critical program (e.g., nuclear submarines). It is significantly easier to modify such a network to meet the isolation requirement than a network in another facility that supports both DoD and commercial product development. In the latter case, it may be possible to isolate the DoD activity – or it may require a new network be created for the DoD program, which can be a significant cost. Large companies also generally already meet the Draft NIST SP 800-171B 'Security Operations Center (SOC)/Threat' related costs.

Smaller companies, on the other hand, tend to operate a single information system network serving all lines of business (commercial and DoD) rather than have multiple facilities with some devoted to DoD development. While in some cases, smaller companies may focus on DoD work or may have already created a small network for DoD programs, others will have to segment a portion of their network or create a new network to meet the isolation requirements. Smaller companies may also meet some of the NIST SP 800-171B 'Security Operations Center (SOC)/Threat' related costs if they currently use a managed service provider to meet existing NIST SP 800-171 'incident response' requirements.

A. Public Cost Analysis

1. Projected Public Cost.
   a. We estimate that 69,000 contractors have controlled unclassified data. However, less than one half of 1% of DoD contractors develop critical capabilities for DoD.

   b. Costing is estimated based on size/complexity of the network subject to the Draft NIST SP 800-171B requirements, with the number of 'end-points' or workstations used as the main size descriptor. The smaller number of end-points can be reasonably associated with smaller companies or a small program activity within a larger company. Larger number of end-points might be associated with facilities operated by larger companies or upgrading most of a smaller or medium company's network to meet the Draft NIST SP 800-171B requirements. Estimates are based on networks sized at 25-50 end-points, 50-150 end-points and 750-1500 endpoints. Some or all of the Security Operations Center/Threat related requirements of Draft NIST SP 800-171B may already be

addressed by a company. Large companies typically do this for themselves while smaller companies may have already employed a managed service provider to meet the incident response requirements of NIST SP 800-171.

Estimated costs for 25-50 end-point systems:

- Process and IT configuration changes: $15K
- Network Isolation:
  - $10K to isolate existing network or existing network segment
  - $250K-500K to create new isolated network (depending on network complexity)
- Security Operations Center/Threat related costs: $75K (if not already met).

Estimated costs for 50-100 end point systems:

- Process and IT configuration changes: $50K
- Network Isolation:
  - $100K to isolate existing network or existing network segment
  - $500K-2.5M to create new isolated network (depending on network complexity)
- Security Operations Center/Threat related costs: $75K-150K (if not already met).

Estimated costs for 750-1500 end point systems:

- Process and IT configuration changes: $100K
- Network Isolation:
  - $250K to isolate existing network or existing network segment
  - $20M to create new isolated network (depending on network complexity)
- Security Operations Center/Threat related costs: $150K-1M (if not already met). Large companies are assumed to have generally implemented the SOC-related costs.

//

Cost Breakout By Company: Following estimates are based on likely types of networks configured or created to meet Draft NIST SP 800-171B requirements:

25-50 end-point networks (50 companies)

- 30 companies segment, isolate and upgrade a portion of an existing network (or upgrade an existing dedicated network):
  30 x [$15K (Process & IT Config) + $10K (isolation)] = $750K
- 20 companies create a new network, but the complexity can vary considerably:
  10 x $250K (low complexity network) and 10 x $500K (high complexity network) = $7.5M
- Half of the 50 companies are estimated to already meet the SOC/IR costs through managed services.
  25 x $75K (SOC/IR) = $1.9M

Total cost: $10.2M

Recurring costs: Recurring cost for new networks assumed to be 20% per year for new networks plus SOC/IR cost or $3.4M total. No additional recurring costs are assumed for reconfiguring portions of existing networks since maintenance costs are essentially the same.

50-100 end- point networks (10 companies)

- 5 companies segment a portion of existing network, isolate and configure: 5 x [$50K (Process & IT Config) + $100K (isolation)] = $750K
- 5 companies create new 50-100 workstation network: 2 x $500K + 3 x $2.5M = $8.5M
- 5 companies are estimated to meet the SOC/IR requirements and 5 require some augmentation: 5 x $150 K = $750K

Total cost = $10M

Recurring costs: Recurring cost for new network assumed to be 20%/yr + SOC/IR cost or $2.45M total. No additional recurring costs are assumed for reconfiguring portions of existing networks since maintenance costs are essentially the same.

750-1500 end-point networks (20 facilities/companies)

- 18 existing networks upgraded and isolated:18 x [$100K (Process & IT Config) + $250K isolation cost) = $6.3M
- 2 new networks created: 2 x $20M = $40M

Total for cost = $46.3M

Recurring costs: Recurring cost for new networks assumed to be 20% per year or $8M total. No additional recurring costs are assumed for reconfiguring portions of existing networks since maintenance costs are essentially the same.

The following table shows the calculations for the total number of networks/companies in the category (not the cost per network/ company):

Requirement	25-50 endpoint networks	50-100 endpoint networks	750-1,500 endpoint networks	Total
# Companies affected	50	10	20	80
Process & IT Configuration	$0.45M	$0.25M	$1.8M	$2.50M
Network Isolation	$7.8M	$8.5M	$44.5M	$60.8M
Security Operations Center	$1.9M	$0.75M	0 (already exist)	$2.65M
Total	$10.2M	$9.5M	$46.3M	$66.0M

Average total cost/network-firm	$0.20M	$0.95M	$3.86M	

NOTE: Since these costs will be part of a contract proposal, DoD will have the opportunity to review how a company chooses to implement the requirements. For a $5B program, creating a dedicated network for $20M (or 0.4% of program cost) might be reasonable, especially since it can be used for other programs with similar requirements. In other situations, we might not support such an expense.

2. Requests for Comment.

   a. We welcome feedback, including relevant data, on the above estimates of the number of affected entities and the per-network cost of complying with the new draft guidance. We further request comments on whether there are networks that would be affected that do not fall into the endpoint ranges noted above. We also encourage feedback on whether there are outcomes—such as bidding companies prospectively adopting the standards in the guidance but not ultimately being awarded contracts—in which not all of the incremental costs would be borne by the federal government; data that would allow for quantification of this outcome would be welcome.

3. Assumptions.

   a. We assume that contractors have already met, or will meet, the basic security requirements of NIST SP 800-171 as required by DFARS clause 252.204-7012 since August 2015. The Draft NIST SP 800-171B build upon these requirements. For example:

      - The requirement for a security operations center (SOC) and cyber incident response team is built upon the existing requirement for an operational incident handling capability. Many large companies have an established SOC and incident response team which will meet this requirement. Smaller companies may also have this capability, or may already use a managed security service.

      - The requirement for an authoritative source and repository of trusted software is built upon the existing requirements for inventories of hardware, software, firmware and baseline configurations. Many companies already use a trusted repository of software.

      - Enhanced personnel vetting builds upon existing personnel screening requirements.

      - Enhanced risk assessment actions build upon existing risk assessment requirement

   b. We assume that some contractors will create a separate ‘critical program’ development environment and consolidate development of all programs requiring the security enhancements in this single environment, although some companies may create several

environments. The physical/ logical isolation and certain other technical requirements naturally lead to this approach, in lieu of converting a company's general purpose IT business system to meet the all the enhanced requirements.

- Depending on the circumstances, a company might elect to segment and isolate a portion of its existing network to create such a critical program development environment. This might occur if that network segment was already dedicated for a program or programs that would be required to meet the enhanced requirements, as it may be more economical (and less disruptive) to convert part of the network to the enhanced requirements rather than building a new environment.

- Some companies already isolate the network they use for DoD program development from other government or commercial processing. In these circumstances, it may make economic sense to simply upgrade the security of the existing DoD segment to meet the enhanced requirements. Similarly, a company working solely on DoD programs may choose to upgrade its security to meet the enhanced requirements.

B. Government Cost Savings Analysis

1. Projected Government Cost Savings.

   a. We estimate that less than one half of 1% of the total number of contractors will be impacted by the enhanced security requirements. However, the incidents related to critical programs represent the majority of DoD forensic analysis and damage assessment, so we estimate this would save 50% of the investment DoD is making to conduct forensic analysis and damage assessment, resulting in a cost savings of $24M.

   b. DoD will benefit from not having to reinvest in new technologies to cover the loss of current critical program capabilities.

2. Projected Government Cost Avoidance.

   When information associated with a critical DoD program has been compromised or exfiltrated, there is a significant impact on DoD and ultimately the public as taxpayers. There are four basic cost drivers when a contractor has a cyber incident that results in compromise or exfiltration. In most situations these costs would be considered savings if the enhanced security requirements were implemented. We welcome comments that would facilitate quantification of cost savings or avoidance attributable to the draft standards, including in any of the following areas:

   a. Cost to repair and recover the compromised contractor information system. These costs can extend to a government system that may be interconnected with the compromised system.

Cost range: The average total cost per data breach is $3.86M (Reference: IBM Security and Ponemon Institute, 2018). The report also states that for small businesses the costs is over $2.2M per company which may drive the company out of business. In that situation, not only is the information compromised, DoD loses the diversity and unique capabilities offered by these small businesses. At this time, we do not know exactly how many breaches per year there are for critical programs and technologies.

b. Cost of loss of DoD critical program and technologies data (loss of years of investment and performance advantage) and loss of company Intellectual Property which is a loss for the company and also for DoD). We lack data and methodology with which to estimate the value of the loss of critical data. However, when an adversary is able to kill, counter or clone our technologies, the warfighter may experience loss of life, and our national security capabilities are jeopardized.

c. Cost to re-develop/re-engineer critical programs resulting from an exfiltration of critical program data and delays in fielding operational capability.
When DoD must reconstitute a capability, some portion of the DoD's Research and Development budget will be diverted for this purpose. In FY19 DoD's budget for R&D was $156.8 billion. If only a fraction of a percent of that budget is redirected, that is a significant investment that could be avoided is the enhanced security requirements were implemented.

Draft NIST SP 800-171B, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations – Enhanced Security Requirements for Critical Programs and High Value Assets,* is available at https://csrc.nist.gov/publications/detail/sp/800-171b/draft.

Technical comments on Draft NIST SP 800-171B should be submitted to via email to sec-cert@nist.gov or at docket number **NIST-2019-0002**. Comments on the cost analysis are accepted at docket number DOD-2019-OS-0072. All comments will be publicly posted without change or redaction on Regulations.gov, so commenters should not include information they do not wish to be posted (e.g., personal or business information).