Before the Department of Commerce

National Institute of Standards and Technology

Washington, D.C.

In the Matter of	)	
	)	
Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets	)	Draft NIST SP 800-171B

COMMENTS OF CTIA

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

August 2, 2019

Table of Contents

I. INTRODUCTION AND SUMMARY 1

II. CTIA'S MEMBER COMPANIES SUPPORT THE VARIED MISSIONS OF FEDERAL AGENCIES WITH SOPHISTICATED AND SECURE SERVICES. 2

III. CTIA ENCOURAGES NIST TO ADDRESS IMPORTANT AMBIGUITIES SO THAT THE APPICABILITY OF SP 800-171B IS CLEAR..... 5

A. NIST Should Clarify the Draft's Discussion of Critical Programs and High Value Assets So that Contractors Can Do Necessary System and Business Planning. 5

B. NIST Should Coordinate with DoD To Clarify Flowdown Obligations Related to SP 800-171 and SP 800-171B. 7

IV. TO PROMOTE CONSISTENT PROTECTION OF INFORMATION ACROSS FEDERAL AND NON-FEDERAL SYSTEMS, SP 800-171B SHOULD BETTER ALIGN WITH SP 800-53, REVISION 5. 9

V. VARYING STANDARDS MAKE IT DIFFICULT FOR CONTRACTORS TO EFFECTIVELY PLAN FOR FUTURE COMPLIANCE. 10

A. DoD's New Cybersecurity Maturity Model Certification Creates Uncertainty about its Interaction with SP 800-171 and SP 800-171B. 11

B. NIST Should Encourage the Government to Permit Contractors to Implement System Security Plans and Plans of Actions and Milestones in Order to Achieve Compliance with Contractual Commitments and SP 800-171B. 12

C. Some of the Controls in SP 800-171B Are Ambiguous, Particularly As They May Apply to Telecommunications Services. 13

D. NIST Should Consider Providing Resources to Assist Contractors in Compliance. 16

VI. THE COSTS OF COMPLIANCE WITH SP 800-171B WILL BE HIGHER THAN ESTIMATED..... 17

VII. CONCLUSION 18

I. INTRODUCTION AND SUMMARY

CTIA[1] appreciates the opportunity to engage with NIST on Draft 800-171B, *Enhanced Security Requirements for Critical Programs and High Value Assets* ("Draft" or "Draft 800-171B").[2] CTIA's members are government contractors and are proud to use their commercial networks to support government missions. The Draft presents a significant opportunity to address the cybersecurity of non-federal systems handling Controlled Unclassified Information ("CUI") and to protect key systems and networks from sophisticated threats, including Advanced Persistent Threats ("APTs"). CTIA makes the following recommendations to improve the Draft:

- NIST should clarify the Draft to make its scope clear and application consistent. This includes providing guidance that reflects how key designations—namely of "Critical Program" ("CP") and "High Value Asset" ("HVA")—will be made and communicated. SP 800-171 applies, if at all, by contractual agreement, not general regulation. The obligation is on the contracting agency to identify a CP or HVA in contracts. NIST should add language in the Draft that makes clear it is not suggesting broad applicability of these designations or this document.

- NIST can promote its longstanding goal of consistently protecting government information across federal and non-federal networks by ensuring that the enhanced controls proposed in Draft 800-171B are aligned with and reflect corresponding controls in SP 800-53, Revision 5.

- NIST should work with the Department of Defense ("DoD") and other agencies to

---

[1] CTIA – The Wireless Association® ("CTIA") (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] Ron Ross et al., *Draft 800-171B, Enhanced Security Requirements for Critical Programs and High Value Assets*, NIST (June 2019) ("*Draft 800-171B*"), https://csrc.nist.gov/publications/detail/sp/800-171b/draft.

reduce uncertainty that is born from multiple, and sometimes inconsistent, cybersecurity standards. By doing so—and by clarifying ambiguities in the Draft's controls—NIST will help contractors to strategically plan for compliance, and will better incentivize contractors to provide cutting-edge and innovative services to the federal government. Specific to telecom contractors, NIST should coordinate with DoD to confirm that providers of commercial telecommunications services to the government do not have covered information systems under DFARs clause 252.204-7012 simply by virtue of transmitting phone calls, data, or text messages—or other similar traffic—on their commercial networks.

- NIST should reconsider its assessment of the costs of compliance with SP 800-171B, which will likely be substantial.

II. CTIA'S MEMBER COMPANIES SUPPORT THE VARIED MISSIONS OF FEDERAL AGENCIES WITH SOPHISTICATED AND SECURE SERVICES.

CTIA and its member companies have a long history of working with the government—including NIST—on cybersecurity. CTIA has provided comments to NIST on its core cybersecurity and information security publications, including SP 800-37, Revision 2 and SP 800-53, Revision 5, and both iterations of its *Framework for Improving Critical Infrastructure Cybersecurity*[3] among other important guidance documents. The Department of Homeland Security ("DHS"), NIST, and other agencies are examining many aspects of the nation's telecommunication and information technology security, from supply chains to fighting botnets, and CTIA and its members are active in this important work. For example, CTIA and several of its member companies are engaged with DHS as part of the ICT Supply Chain Task Force to "focus on potential near- and long-term solutions to manage strategic risks [related to the global ICT supply chain] through policy initiatives and opportunities for innovative public-private

[3] *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, NIST (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

partnership."[4] As another example, the wireless industry, with others in the Communications sector, leads the efforts of the Federal Communications Commission's Communications Security, Reliability and Interoperability Council ("CSRIC"), which recently published a report making key recommendations for securing the 5G supply chain.[5]

CTIA's members include the world's largest carriers, many of whom use their commercial networks to provide sophisticated voice, data and cloud-based services to the federal government under various contracts and subcontracts. This includes DoD[6] and the range of civilian agencies. For example, AT&T and Verizon received a three-year Authority to Operate ("ATO") in March 2019 under the General Service Administration's ("GSA") Enterprise Infrastructure Solutions ("EIS") contract.[7] As a government-wide contract, EIS enables federal

---

[4] *ICT Supply Chain Task Force Fact Sheet*, DHS, https://www.dhs.gov/sites/default/files/publications/18_0731_cyber-summit-supply-chain-fact-sheet.pdf.

[5] *See Working Group 3, Final Report - Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks, v.14.0*, CSRIC, (Sept. 2018), https://www.fcc.gov/files/csric6wg3sept18report5gdocx-0; *Working Group 3, Addendum to Final Report – Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks*, at A-3, CSRIC (Sept. 2018), https://www.fcc.gov/file/14855/download.

[6] For example, "Maxwell Air Force Base in Montgomery, Alabama has been working with AT&T to improve base security and force protection using the latest technology." *The Defense Network of Tomorrow—Today*, AT&T, at 3 (2018), https://www.business.att.com/content/dam/attbusiness/reports/industries-public-sector-federal-dod-network-of-future-white-paper.pdf.

[7] *EIS Business Support Systems Security Assessment and Authorization Announcement*, GSA Interact (Mar. 25, 2019), https://interact.gsa.gov/blog/eis-business-support-systems-security-assessment-and-authorization-announcement-0; *see also Enterprise Infrastructure Solutions (EIS)*, AT&T, https://www.business.att.com/industries/family/public-sector/enterprise-infrastructure-solutions.html; *Enterprise Infrastructure Solutions (EIS)*, Verizon, https://enterprise.verizon.com/solutions/public-sector/federal/contracts/eis/.

agencies to leverage the government's buying power to procure next-generation communications services, information technology, and telecommunications infrastructure.[8] Sprint supports the government through the GSA by providing the Federal Relay Service "for Federal employees who are deaf, hard of hearing, deafblind, blind and low vison, or have speech disabilities."[9] Under the Navy's Spiral 3 Wireless and Telecommunications Services contract, "T-Mobile is providing 70,000 lines of wireless service to the U.S. Department of Veterans Affairs (VA) to help make telehealth services more accessible to veterans," making T-Mobile the primary wireless provider for the VA.[10] AT&T and Verizon were named as Top 100 Government Contractors in 2018.[11] CTIA members are also subcontractors, providing connectivity and other support to a variety of agencies.

Telecom and data services occupy a unique space when it comes to government contracts. CTIA's members provide connectivity for government functions using their existing commercial networks, the operation of which is highly regulated at the federal and state level. This makes it imperative that any new data security obligations created by NIST and DoD are

---

[8] Najuma Thorpe, *Verizon Receives EIS Authority to Operate*, Verizon (Mar. 25, 2019), https://www.verizon.com/about/news/verizon-receives-eis-authority-operate.

[9] *Federal Relay Services*, Sprint, https://www.sprintrelay.com/services/federal-relay-services (last visited July 29, 2019).

[10] *U.S. Department of Veterans Affairs Partners with T-Mobile to Help Expand Access to Health Care for Veterans*, T-Mobile (Dec. 10, 2018), https://www.t-mobile.com/news/va-veterans-health-administration?icid=B2B_BB_19TFBEVRGN_XDYWUSXP417H9TQZO16875.

[11] *2018 Top 100*, Washington Technology (June 1, 2018), https://washingtontechnology.com/toplists/top-100-lists/2018.aspx; *see also Technology Solutions for Federal Agencies*, Verizon, https://enterprise.verizon.com/solutions/public-sector/federal/?gclid=CPXb5-H_p-MCFcvcswodJVgBoQ.

clear and compatible with regulatory and operational realities of modern telecom services.[12]

III. CTIA ENCOURAGES NIST TO ADDRESS IMPORTANT AMBIGUITIES SO THAT THE APPICABILITY OF SP 800-171B IS CLEAR.

A. NIST Should Clarify the Draft's Discussion of Critical Programs and High Value Assets So that Contractors Can Do Necessary System and Business Planning.

The meanings of "Critical Program" and "High Value Asset" ("HVA") are unclear. This makes some sense because of the role that contracting agencies play in making designations, but NIST should clarify its discussion to ensure that contracting agencies do not apply SP 800-171 and SP 800-171B in a confusing or overbroad way.

CTIA understands that NIST intends for the controls identified in SP 800-171B to apply to "designated" HVAs or Critical Programs, particularly those that are subject to attack from APTs,[13] and that NIST does not expect that SP 800-171B will impact the vast majority of contractors.[14] The Draft, however, does not define these terms and does not provide guidance for

---

[12] For example, the U.S. Navy's September 28, 2018, memorandum entitled, "Implementation of Enhanced Security Controls on Select Defense Industrial Base Partner Networks" requires certain contractors to allow NCIS to "install network sensors, owned and maintained by NCIS, on the contractor's information systems . . . ." It is unclear what this requirement will look like in practice, but it may be inconsistent with carriers' obligations under the Stored Communications Act and the Wiretap Act to not disclose communications to the government without proper process.

[13] Draft 800-171B appears to suggest that all Critical Programs and HVAs are targeted by APTs. Of course, APTs may target entities that do not support Critical Programs or HVAs, while some that do support Critical Programs and HVA may not be the target of APT attack. It is thus uncertain whether being the target of an APT attack is a necessary condition to being designated as a Critical Program or HVA.

[14] *Request for Comment on NIST Special Publication (SP) 800-171B, Protected Controlled Unclassified Information in Nonfederal Systems and Organizations – Enhanced Security Requirements for Critical Programs and High Value Assets*, 2, https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-and-

contracting agencies or contractors about the designation process or the basis for NIST's position that only a relatively small subset of contractors will have to meet these requirements.[15] This raises several questions for contractors. For example,

- When and how will a contractor be notified by a contracting agency that it is operating a Critical Program or HVA?
- Will agencies be authorized to designate Critical Programs or HVAs during the course of contract performance?
- Will any particular agency be charged with designations, or will each agency designate contracts as Critical Programs or HVAs on a contract-by-contract basis?

While these issues should be addressed by individual contracting agencies (or through the FAR/DFARS rulemaking process), these stakeholders will rely heavily on NIST's guidance and it will be useful to consider, or at least reference, these issues in the NIST standard document.

In the absence of guidance about what is likely to constitute a Critical Program or HVA, these questions have significant implications for the number and type of contractors that may need to comply with the requirements in SP 800-171B. If the definition is applied differently

---

dod-cost-estimate-request-for-comments.pdf (stating that it expects less than .5% of all contractors will be impacted by the enhanced security requirements) ("*Request for Comment*").

[15] Draft 800-171B refers to OMB Memorandum M-19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program. *See, e.g., Draft 800-171B* at 2, n.6; *see also Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program,* Memorandum from Mick Mulvaney for Heads of Executive Departments and Agencies, OMB, M-19-03 (Dec. 10, 2018), https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf ("*OMB M-19-03*"). That Memorandum identifies several categories of information systems which may constitute an HVA, including, somewhat circularly, an information system with "informational value" to the government or its adversaries. *See OMB M-19-03* at 3. The Memorandum also states that while agencies are principally responsible for designating HVAs, OMB and DHS may also designate HVAs. It is uncertain how NIST expects agencies to adopt these or other definitions for HVAs.

across agencies, the number of contracts that may involve an HVA will be much higher than estimated by NIST. This unpredictability will present challenges for strategic planning. Contractors may have to make considerable investment to ensure that information systems comply with the enhanced controls and should have guidance from NIST or the purchasing agencies about the scope of these terms.

Clarifying these uncertainties is important not only for compliance with DoD contracts (or those containing DFARS 252.204-7012), but also for civilian contracts, given that NARA has reiterated its intent to sponsor a "single FAR clause that will apply the requirements of the federal CUI regulation and NIST Special Publication 800-171 to contractors."[16] Uncertainty about the applicability of security regimes may increase costs and discourage companies from offering services to the government.

B. NIST Should Coordinate with DoD To Clarify Flowdown Obligations Related to SP 800-171 and SP 800-171B.

There is some uncertainty about whether and how prime contractors are expected to ensure subcontractor compliance with SP 800-171 and SP 800-171B. This is driven by the diversity of subcontracting relationships and the widely different access subcontractors have to prime contractors' and the government's data, information, and systems. CTIA encourages NIST to engage with industry on expectations for prime-subcontractor compliance with SP 800-171 and SP 800-171B. Such collaboration may result in changes to SP 800-171 and SP 800-171B and could support supplemental resources developed by NIST and DOD.

---

[16] Ron Ross et al., *Draft 800-171, Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,* NIST, at 2, n.10 (June 2019) ("*Draft 800-171, Rev. 2*"), https://csrc.nist.gov/CSRC/media/Publications/sp/800-171/rev-2/draft/documents/sp800-171r2-draft-ipd.pdf.

SP 800-171 and SP 800-171B should more accurately depict the varied relationships and expectations between prime contractors and sub-contractors. Subcontracting relationships are diverse; some subcontractors provide minimal support while others may perform a substantial portion of the effort and be closely integrated into a prime's information system. 800-171B should recognize this diversity. As an example, the Draft indicates that security requirements that are difficult or prohibitively expensive can be implemented through "external service providers," to include a prime contractor providing IT infrastructure support to a subcontractor.[17] This language in the Draft presents a simplified view of the prime-subcontractor relationship, suggesting that prime contractors will readily be willing and able to provide often-sensitive IT services to subcontractors, and conversely, that subcontractors would be willing to accept such services from their prime contractor. For a variety of business and legal reasons, prime contractors and subcontractors often may be unable or unwilling to provide IT or other similar services to each other. CTIA recommends that NIST explore with industry and DoD how contractors are expected to confirm compliance of their subcontractors.

Among other things, NIST should consider developing, with DoD, supplemental resources to guide compliance with SP 800-171 and SP 800-171B. Supplemental resources could clarify how contractors can manage subcontractors' compliance with these documents. NIST and DOD could also collaborate with industry to develop tools, training, and best practices for contractors to oversee compliance by lower-tier subcontractors. NIST is well-positioned to help develop clearer expectations for prime-subcontractor relationships by leveraging its experience working with industry and government to identify best practices and solutions.

---

[17] *See Draft 800-171B* at 9, n.22.

IV. TO PROMOTE CONSISTENT PROTECTION OF INFORMATION ACROSS FEDERAL AND NON-FEDERAL SYSTEMS, SP 800-171B SHOULD BETTER ALIGN WITH SP 800-53, REVISION 5.

NIST's release of this Draft raises questions about how it will work with other standards. NIST should ensure that the enhanced controls in the Draft do not impose requirements on contractors in excess of those required of the government. And NIST should consider delaying publication of a final SP 800-171B to allow for it to align with SP 800-53, Revision 5, which is under development.

Substantively, CTIA encourages NIST to focus on aligning the security obligations of government and its private sector partners and to consider whether SP 800-171B correlates to the standards required of the government under SP 800-53, Revision 5.

NIST has long valued consistency across federal and non-federal systems in protecting critical government information, stating that government information should be protected at comparable levels regardless of whether the federal government or a contractor stores it. An earlier revision of SP 800-171 stated that "[t]he responsibility of federal agencies to protect and ensure the control of CUI does not change when such information is shared with nonfederal partners. Therefore, a similar level of protection is needed when CUI is processed, stored, or transmitted by nonfederal organizations using nonfederal systems."[18] NIST's approach is based on three "fundamental assumptions," which reflect the importance of consistency:

- "Statutory and regulatory requirements for the protection of CUI are *consistent*, whether such information resides in federal systems or nonfederal systems including the environments in which those systems operate;

[18] Ron Ross et al., *800-171, Revision 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, NIST, at 3 (June 2018) ("*800-171, Rev. 1*"), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf.

- Safeguards implemented to protect CUI are *consistent* in both federal and nonfederal systems and organizations; and

- The confidentiality impact value for CUI is no less than *moderate* in accordance with Federal Information Processing Standards (FIPS) Publication 199."[19]

The notion that contractors and the federal government must take equal steps to protect the same information was central to the formulation of SP 800-171.

The Draft, however, does not ensure that contractors and the government implement the same controls to protect the same data. Unlike SP 800-171, which was carefully matched to the moderate baseline in NIST's SP 800-53, the Draft does not appear to match a baseline applicable to the federal government. To the contrary, it appears that contractors would be expected to implement a set of controls under SP 800-171B that are more strenuous than what the government must meet, even under the High Baseline in SP 800-53, Revision 5.[20]

NIST should ensure that its efforts on SP 800-171B are consistent with any future updates to SP 800-53, Revision 5. Because SP 800-53, Revision 5 is still in draft, and its controls refer to the controls in SP 800-171B, NIST should consider delaying finalizing SP 800-171B until it finalizes SP 800-53, Revision 5. This will help NIST ensure that the controls in SP 800-171B correspond to those required of the government under SP 800-53.

V. VARYING STANDARDS MAKE IT DIFFICULT FOR CONTRACTORS TO EFFECTIVELY PLAN FOR FUTURE COMPLIANCE.

---

[19] *Id.* at 5 (emphases in original).

[20] For example, the following controls are required by contractors under Draft 800-171B but are not required by the federal government under SP 800-53 rev 5 High: 3.1.1e, Access Enforcement, Dual Authorization; 3.1.1e, Media Sanitization, Dual Authorization; 3.6.1e, Incident Handling, Security Operations Center; 3.11.2e, System Monitoring, Indicators of Compromise.

A. DoD's New Cybersecurity Maturity Model Certification Creates Uncertainty about its Interaction with SP 800-171 and SP 800-171B.

DoD is in the process of rolling out a new Cybersecurity Maturity Model Certification ("CMMC") which will impose significant new compliance requirements on government contractors.[21] The CMMC model will interact with SP 800-171 and other standards, so it is important that NIST consider this effort as it produces SP 800-171B.

DoD is expected to promulgate a draft version of the CMMC soon, under which it will require contractors to obtain third-party certification and be subject to audit.[22] DoD is contemplating using five tiers of cybersecurity maturity and has stated that contractors will need to achieve a certain level of certified maturity in order to compete for certain work. DoD has not made clear how these five tiers will map to SP 800-171 or SP 800-171B controls.[23]

Given the lack of clarity about the relationship between the CMMC model and the NIST controls, NIST should work with DoD and industry to ensure that it is not imposing different or shifting sets of requirements. Contractors are expending significant resources to comply with SP 800-171 and other demands while trying to anticipate future obligations. The purchase of network elements and software, design of IT systems, and mapping of data flows require

---

[21] *See Cybersecurity Maturity Model Certification*, Office of the Undersecretary of Defense for Acquisition & Sustainment, https://www.acq.osd.mil/cmmc/index.html (last visited July 29, 2019).

[22] Justin Doubleday, *Defense Dept. to require new cybersecurity certification from contractors*, Inside Cybersecurity (June 3, 2019), https://insidecybersecurity.com/daily-news/defense-dept-require-new-cybersecurity-certification-contractors.

[23] DoD has recently indicated that it may consider the first three tiers of cybersecurity maturity aligned with SP 800-171, with the fourth and fifth tiers aligned with NIST SP 800-171B. *See What Contractors Need to Know about DoD's CMMC*, Professional Services Council, at 20 (Webinar, July 17, 2019) (accompanied by oral presentation).

advance planning and decision-making. Contractors will have difficulty doing strategic planning without guidance as to what controls will be required, which controls will satisfy CMMC tiers, and how the tiers will map to SP 800-171 and SP 800-171B. Coordination between NIST and DoD is critical.

B. NIST Should Encourage the Government to Permit Contractors to Implement System Security Plans and Plans of Actions and Milestones in Order to Achieve Compliance with Contractual Commitments and SP 800-171B.

DoD has recognized that some contractors have not yet implemented many of the SP 800-171 security controls.[24] In recognition of the significant time and resources needed to achieve compliance with DFARS 252.204-7012 and SP 800-171, DoD previously issued guidance[25] that contractors not yet in compliance with the requirements of SP 800-171 could meet their contractual obligations by establishing a System Security Plan ("SSP") that outlines the contractor's current state of compliance and identified compliance gaps, and by preparing a Plan of Actions and Milestones ("POAM") for completing the implementation in the future. These mechanisms are important tools to allow contractors to work towards full compliance without breaching their contractual obligations.

Given the substantial time and resources that may be necessary for some contractors to implement SP 800-171B while planning for potential compliance with DoD's CMMC model,

---

[24] Katie Arrington, Special Assistant to the Assistant Secretary of Defense for Acquisition for Cyber in the Office of the Under Secretary of Acquisition and Sustainment Remarks (June 12, 2019), https://federalnewsnetwork.com/reporters-notebook-jason-miller/2019/06/why-dods-decision-to-make-cybersecurity-an-allowable-cost-matters/ ("*Arrington Remarks*").

[25] *See DoD Guidance for Reviewing System security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented*, DoD, Docket DARS-2018-0023, 83 Fed. Reg. 17807 (Apr. 24, 2018), https://www.govinfo.gov/content/pkg/FR-2018-04-24/pdf/2018-08554.pdf.

NIST should support and adapt this approach to let contractors establish SSPs and POAMs that will provide a path towards implementation of any contractually required controls identified in SP 800-171B.

C. Some of the Controls in SP 800-171B Are Ambiguous, Particularly As They May Apply to Telecommunications Services.

The Draft of SP 800-171B contains some controls with significant room for divergent implementations, and NIST should explicitly recognize contractors' flexibility in implementation. One example is the new isolation control, which could impact a variety of mixed commercial-use/government-use systems. Many contractors' information systems are mixed use, and this is advantageous for the government because it benefits from efficiencies and scale not possible in purpose-built systems for the government.

This is especially important in the case of commercial contractors who provide services to the government on a "commercial item" basis, as do CTIA members. Relevant statutes and implementing regulations prohibit the government from imposing non-industry standard terms and conditions on commercial item contractors, precisely because such inconsistent standards can preclude commercial entities from offering their products and services to the government, which ultimately increases government costs and reduces efficiency.[26] The more NIST's Draft departs or encourages contracting agencies to depart from standard commercial practices, the less likely the government will continue to enjoy the cost and efficiency benefits of commercial item contracting to the maximum practical extent.[27]

For example, Control 3.13.4e, Physical and Logical Isolation, states that contractors need

---

[26] *See e.g.*, FAR 12.302(c).

[27] *See* FAR 12.101.

to implement "physical and logical isolation techniques applied at the architectural level of the system [which] can limit the unauthorized flow of CUI; reduce the system attack surface; constrain the number of system components that must be highly secure; and impede the movement of an adversary."[28] While the publication lists an air-gapped system as the most extreme isolation technique, it is unclear when this costly control may be required. The Draft states:

> The degree of isolation varies depending upon the boundary protection mechanisms selected. Boundary protection mechanisms include routers, gateways, and firewalls separating system components into physically separate networks or subnetworks; virtualization and micro-virtualization techniques; encrypting information flows among system components using distinct encryption keys; cross-domain devices separating subnetworks; and complete physical separation (i.e., air gaps).[29]

This range of techniques has substantial differences in cost, time, and architecture, and it would be challenging for contractors to change from a boundary protected through logical controls, like routers and firewalls, to air-gapped networks. The control states: "Isolation techniques are selected based on a risk management perspective that balances the threat, the information being protected, and the cost of the options for protection."[30]

NIST alludes to significant potential costs by stating that compliance with this control (Physical and Logical Isolation) is the "primary factor affecting the cost of implementation" of Draft SP 800-171B.[31] Given the significant disparity in the range of techniques identified under

---

[28] *Draft 800-171B* at 31.

[29] *Id.*

[30] *Id.*

[31] *Request for Comments* at 2-3.

the controls, including Control 3.13.4e, contractors should be given clearer guidance about their freedom to select controls under a risk management framework. The Draft should recognize explicitly that reasonable boundary protections (like many other controls) will vary and that the most rigorous option is identified as illustrative but is not required in all or even many cases.

The boundary protection questions are particularly complex for contractors because of the broad and ambiguous definition of unmarked Controlled Defense Information ("CDI"), the possession or transmission of which triggers the requirement to implement the isolation techniques described above.

Specifically, the second prong of the definition of "Controlled Defense Information" is ambiguous. The second prong defines CDI as CUI that is "[c]ollected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract."[32] It is unclear whether data, like voice calls or SMS messages, could ever be considered CDI that is "transmitted" by a contractor in support of the performance of the contract, where, for example, a DoD entity has contracted with the carrier to provide communications service, using the carrier's standard commercial network. If this type of data is considered CDI, then carriers would in theory be required to implement the controls in SP 800-171 Rev. 1 across their existing commercial network, which would be a monumental undertaking if not entirely cost-prohibitive. CTIA respectfully suggests that NIST coordinate with DoD to confirm that data transiting a commercial telecommunications network pursuant to a communications services contract is not considered unmarked CDI for the purposes of DFARS 252.204-7012, and that these networks are not covered information systems simply by virtue of

[32] *See* DFARS 252.204-7012(a)(2).

the information a carrier's customer may elect to send across the network (with no notice of agreement with the carrier). This is the most logical interpretation, but absent a clarification, there is ambiguity about the compliance obligations of telecommunications providers in these circumstances.

This ambiguity increases with SP 800-171B. As discussed, it is conceivable that a DoD component might deem a contract for communications services a Critical Program or a HVA, requiring the imposition of SP 800-171B controls on a carrier's network. Further, under Control 3.13.4e, the carrier's network may need to be air-gapped and isolated from commercial activity. This should not be the default expectation for contracts for commercial telecommunications and data services, where the entire purpose of the undertaking is to furnish the government with access to a carrier's existing commercial network infrastructure. NIST should ensure its Draft does not suggest that it is. CTIA encourages NIST to carefully consider these and other ambiguous controls to ensure that agencies using the standard can provide industry a clear understanding of these requirements.

D. NIST Should Consider Providing Resources to Assist Contractors in Compliance.

Due to the rapidly evolving regulatory landscape and significant definitional ambiguities, NIST should work with industry partners to develop resources to help contractors comply with the requirements of SP 800-171B. These resources would include training, best practices, and other guidance. Government leadership on compliance expectations would benefit the government and its contracting partners.

As one example of the utility of such guidance, CTIA appreciates the effort DoD has put

into the current FAQs on implementing the DFARS clause.[33] These FAQs have been helpful in addressing some ambiguities in SP 800-171. However, this non-binding guidance has left many contractors with substantial uncertainty as they design and invest in information systems. CTIA encourages NIST to work with industry and DoD on standardized resources and best practices.

VI. THE COSTS OF COMPLIANCE WITH SP 800-171B WILL BE HIGHER THAN ESTIMATED.

NIST's cost estimate appears to be understated. For example, NIST estimates that contractors with 25-50 end-point systems will incur only $15,000 in costs in process and IT configuration changes, and only $10,000 in costs to isolate an existing network. However, based on the experiences of its members, CTIA cautions that some of the individual controls listed in the Draft might cost *hundreds of thousands* of dollars (or, for more complex systems, *millions*) to implement on a system or systems. For a more complete picture of estimated costs, NIST should seek additional information regarding the basis for these costs.

NIST has also stated that the costs will "typically [be] an allowable contract cost to the government."[34] While DoD has recently indicated that costs for compliance with its CMMC model will be allowable in certain circumstances,[35] it is not yet clear how the CMMC standard relates to the NIST publications, nor does this informal statement apply to non-DoD contracts. How has NIST ensured that costs will be allowed, as stated in the request for comments? CTIA

---

[33] *Frequently Asked Questions (FAQs) Regarding the Implementation of DFARS Subpart 204.73 and PGI Subpart 204.73, DFARS Subpart 239.76 and PGI Subpart 239.76, FAQ Revision* (Apr. 2, 2018), https://dodprocurementtoolbox.com/cms/sites/default/files/resources/2018-04/Revision%20to%20Cyber%20DFARS%20FAQs%20-%20April%202%202018.pdf.

[34] *Request for Comments* at 2.

[35] *Arrington Remarks.*

encourages NIST and contracting agencies to ensure that the costs of compliance with SP 800-171B – which may be substantial, as noted above—are indeed allowable under DoD and non-DoD contracts alike.

VII. CONCLUSION

CTIA appreciates the opportunity to collaborate with NIST on this important publication. The Draft publication contains certain definitional ambiguities and raises questions regarding potential scope of application. NIST should coordinate with DoD, other government agencies, and industry partners to ensure that contractors can comply with these substantial requirements.

Respectfully Submitted,

/s/ *Thomas K. Sawanobori*

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org