JAN 2 3 2014

MEMORANDUM FOR ASSISTANT TO THE PRESIDENT FOR HOMELAND SECURITY
ASSISTANT TO THE PRESIDENT FOR ECONOMIC AFFAIRS

SUBJECT: Improving Cybersecurity and Resilience through Acquisition – Final Report of the Department of Defense and General Services Administration

Section 8(e) of Executive Order (EO) 13636 directed that we make recommendations to you on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration.

Attached is the final signed report of the Department of Defense and General Services Administration Joint Working Group on Improving Cybersecurity and Resilience through Acquisition, one component of the Government-wide implementation of EO 13636 and Presidential Policy Directive 21.

Chuck Hagel
Secretary of Defense

Daniel M. Tangherlini
Administrator of General Services

Attachment:
As stated

Improving Cybersecurity and Resilience through Acquisition

Final Report of the Department of Defense and General Services Administration

November 2013

The estimated cost of this report or study for the Department of Defense is approximately $208,000 in FY 2012-2013.
Cost estimate generated on November 13, 2013 RefID: 5-C493D22

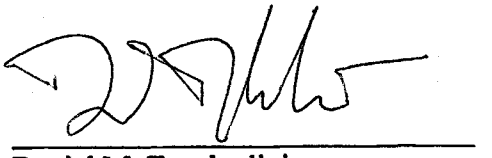
This Page Intentionally Left Blank

Foreword

The Department of Defense and the General Services Administration have prepared this report to the President in accordance with Executive Order 13636. The report provides a path forward to aligning Federal cybersecurity risk management and acquisition processes.

The report provides strategic guidelines for addressing relevant issues, suggesting how challenges might be resolved, and identifying important considerations for the implementation of the recommendations. The ultimate goal of the recommendations is strengthening the cyber resilience of the Federal government by improving management of the people, processes, and technology affected by the Federal Acquisition System.

Frank Kendall
Under Secretary of Defense
Acquisition, Technology, and Logistics



Daniel M. Tangherlini
Administrator of General Services

Preface

This document constitutes the final report of the *Department of Defense (DoD) and General Services Administration (GSA) Joint Working Group on Improving Cybersecurity and Resilience through Acquisition.* The report is one component of the government-wide implementation of Executive Order (EO) 13636 and Presidential Policy Directive (PPD) 21. It was developed in collaboration with stakeholders from Federal agencies and industry and with the assistance of the Department of Homeland Security's Integrated Task Force.[1] The Working Group also coordinated development of the recommendations closely with the Department of Commerce, National Institute of Standards and Technology's (NIST) development of a framework to reduce cyber risks to critical infrastructure[2] (Cybersecurity Framework), and in parallel to the Departments of Commerce, Treasury, and Homeland Security reports on incentives to promote voluntary adoption of the Cybersecurity Framework.[3] This jointly issued report is the culmination of a four-month process by an interagency working group comprised of topic-knowledgeable individuals selected from the Federal government.[4]

One of the major impediments to changing how cybersecurity is addressed in Federal acquisitions is the differing priorities of cyber risk management and the Federal Acquisition System.[5] The Acquisition Workforce[6] is required to fulfill numerous, sometimes conflicting, policy goals through their work, and cybersecurity is but one of several competing priorities in any given acquisition. The importance of cybersecurity to national and economic security dictates the need for a clear prioritization of cyber risk management as both an element of enterprise risk management and as a technical requirement in acquisitions that present cyber risks. The importance of cybersecurity relative to the other priorities in Federal acquisition should be made explicit.

The purpose of this report is to recommend how cyber risk management and acquisition processes in the Federal government can be better aligned. The report does not provide explicit implementation guidance, but provides strategic guidelines for addressing relevant issues, suggesting how challenges might be resolved and identifying important considerations for the implementation of the recommendations.

---

[1] The Department established an Integrated Task Force (ITF) to lead DHS implementation and coordinate interagency, and public and private sector efforts; see, http://www.dhs.gov/publication/integrated-task-force.
[2] 78 Fed. Reg. 13024 (February 26, 2013).
[3] *See*, 78 Fed. Reg. 18954 (March 28, 2013).
[4] Appendix I contains a list of the Working Group members.
[5] See, 48 C.F.R. § 1.102 (2013).
[6] *Id.*

TABLE OF CONTENTS

Foreword 3

Preface 4

Executive Summary 6

Background 9

Cyber Risk and Federal Acquisition 10

Recommendations 13

I. Institute Baseline Cybersecurity Requirements as a Condition of Contract Award for Appropriate Acquisitions 13

II. Address Cybersecurity in Relevant Training 14

III. Develop Common Cybersecurity Definitions for Federal Acquisitions 15

IV. Institute a Federal Acquisition Cyber Risk Management Strategy 15

V. Include a Requirement to Purchase from Original Equipment or Component Manufacturers, Their Authorized Resellers, or Other Trusted Sources, for Appropriate Acquisitions 17

VI. Increase Government Accountability for Cyber Risk Management 18

Conclusion 19

APPENDIX I – JOINT WORKING GROUP ROSTER 21

APPENDIX II – STAKEHOLDER ENGAGEMENTS 22

Executive Summary

When the government purchases products or services with inadequate in-built cybersecurity, the risks persist throughout the lifespan of the item purchased. The lasting effect of inadequate cybersecurity in acquired items is part of what makes acquisition reform so important to achieving cybersecurity and resiliency. Purchasing products and services that have appropriate cybersecurity designed and built in may have a higher up-front cost in some cases, but doing so reduces total cost of ownership by providing risk mitigation and reducing the need to fix vulnerabilities in fielded solutions.

Increasingly, the Federal government relies on network connectivity, processing power, data storage, and other information and communications technology (ICT) functions to accomplish its missions. The networks the government relies on are often acquired and sustained through purchases of commercial ICT products and services. These capabilities greatly benefit the government, but have also, in some cases, made the government more vulnerable to cyber attacks and exploitation.

Resilience to cyber risks has become a topic of core strategic concern for business and government leaders worldwide and is an essential component of an enterprise risk management strategy. While the report focuses its recommendations on increasing the use of cybersecurity standards in Federal acquisitions,[7] DoD and GSA view the ultimate goal of the recommendations as strengthening the cyber resilience of the Federal government by improving management of the people, processes, and technology affected by the Federal Acquisition System.

It is important to note that these recommendations are not intended to conflict with acquisition or cybersecurity requirements related to National Security Systems (NSS). The Committee on National Security Systems (CNSS) is responsible for the creation and maintenance of National-level Information Assurance operating issuances for NSS and for providing a comprehensive forum for strategic planning and operational decision-making to protect NSS for the United States.[8] The CNSS has also established acquisition practices for NSS, and those practices are explicitly not within the scope of this report.[9] The

---

[7] The terms "Federal acquisition(s)," or "acquisition(s)," are used throughout this report to mean all activities of Departments and Agencies to acquire new or modified goods or services, including strategic planning, capabilities needs assessment, systems acquisition, and program and budget development. See, e.g., *"Big "A" Concept and Map,"* available at, https://dap.dau.mil/aphome/Pages/Default.aspx.

[8] The Committee on National Security Systems (CNSS) has been in existence since 1953. The CNSS (formerly named the National Security Telecommunications and Information Systems Security Committee (NSTISSC)) was established by National Security Directive (NSD)-42, "National Policy for the Security of National Security Telecommunications and Information Systems. This was reaffirmed by Executive Order (E.O.) 13284, dated January 23, 2003, "Executive Order Amendment of Executive Orders and Other Actions in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security" and E.O. 13231, "Critical Infrastructure Protection in the Information Age" dated October 16, 2001. Under E.O. 13231, the President re-designated the NSTISSC as CNSS. The Department of Defense continues to chair the Committee under the authorities established by NSD-42.

[9] OMB policies (including OMB Reporting Instructions for FISMA and Agency Privacy Management) state that for other than national security programs and systems, federal agencies must follow certain specific NIST Special Publications. See, e.g., *Guide for Applying the Risk Management Framework to Federal Information System:*

recommendations are intended to complement and align with current processes and practices used to acquire NSS and were developed in consultation with organizations that routinely acquire NSS, including the Defense Intelligence Agency, National Security Agency, the Federal Bureau of Investigation, and the Department of Justice Office of the Chief Information Officer.

These recommendations were not created in isolation. Rather, the recommendations are designed to be considered as one part of the Federal Government's comprehensive response to cyber risks. Furthermore, the recommendations do not explicitly address how to harmonize rules. Instead, the recommendations focus on driving consistency in interpretation and application of procurement rules and incorporation of cybersecurity into the technical requirements of acquisitions. The recommendations are summarized as follows:

I. ***Institute Baseline Cybersecurity Requirements as a Condition of Contract Award for Appropriate Acquisitions.***
Basic cybersecurity hygiene is broadly accepted across the government and the private sector as a way to reduce a significant percentage of cyber risks. For acquisitions that present cyber risks, the government should only do business with organizations that meet such baseline requirements in both their own operations and in the products and services they deliver. The baseline should be expressed in the technical requirements for the acquisition and should include performance measures to ensure the baseline is maintained and risks are identified.

II. ***Address Cybersecurity in Relevant Training.***
As with any change to practice or policy, there is a concurrent need to train the relevant workforces to adapt to the changes. Incorporate acquisition cybersecurity into required training curricula for appropriate workforces. Require organizations that do business with the government to receive training about the acquisition cybersecurity requirements of the organization's government contracts.

III. ***Develop Common Cybersecurity Definitions for Federal Acquisitions.***
Unclear and inconsistently defined terms lead, at best, to suboptimal outcomes for both efficiency and cybersecurity. Increasing the clarity of key cybersecurity terms in Federal acquisitions will increase efficiency and effectiveness for both the government and the private sector. Key terms should be defined in the Federal Acquisition Regulation.

IV. ***Institute a Federal Acquisition Cyber Risk Management Strategy.***
From a government-wide cybersecurity perspective, identify a hierarchy of cyber risk criticality for acquisitions. To maximize consistency in application of procurement rules, develop and use "overlays"[10] for similar types of acquisition, starting with the types of

---

A Security Life Cycle Approach, NIST Special Publication 800-37, Revision 1 (Feb. 2010), and *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, Revision 4, (Apr. 2013).

[10] An overlay is a fully specified set of security requirements and supplemental guidance that provide the ability to appropriately tailor security requirements for specific technologies or product groups, circumstances and conditions, and/or operational environments.

acquisitions that present the greatest cyber risk.

V. ***Include a Requirement to Purchase from Original Equipment Manufacturers, Their Authorized Resellers, or Other "Trusted" Sources, Whenever Available, in Appropriate Acquisitions.***
In certain circumstances, the risk of receiving inauthentic or otherwise nonconforming items is best mitigated by obtaining required items only from original equipment manufactuers, their authorized resellers, or other trusted sources. The cyber risk threshold for application of this limitation of sources should be consistent across the Federal government.

VI. ***Increase Government Accountability for Cyber Risk Management.***
Identify and modify government acquisition practices that contribute to cyber risk. Integrate security standards into acquisition planning and contract administration. Incorporate cyber risk into enterprise risk management and ensure key decision makers are accountable for managing risks of cybersecurity shortfalls in a fielded solution.

Implementation of the recommendations should be precisely aligned with the extensive ongoing critical infrastructure and cybersecurity efforts of industry and government, most importantly the Comprehensive National Cybersecurity Initiative and the Cybersecurity Framework being developed under the Executive Order, but also the National Infrastructure Protection Plan (NIPP), the associated Sector Specific Plans, information sharing efforts on threat and vulnerability issues, the sectors' various risk assessment and risk management activities, and statutory and regulatory changes.

Cybersecurity standards are continually being established and updated through the transparent, consensus-based processes of standards development organizations (SDO).[11] Many of these processes are international in design and scope, and they routinely include active engagement by multinational corporations and various government entities that participate as developers or users of the technology. Organizations voluntarily adopt the resulting best practices and standards to best fit their unique requirements, based on their roles, business plans, and cultural or regulatory environments. The international standards regime facilitates interoperability between systems and a competitive commercial market. It also spurs the development and use of innovative and secure technologies.

Incorporation of voluntary international standards and best practices into Federal acquisitions can also be highly effective in improving cybersecurity and resilience. However, Federal agencies are required to use standards and guidelines that are developed and implemented through NIST.[12] Cybersecurity standards used in acquisitions should align to the greatest extent possible with international standards and emphasize the importance of organizational flexibility in application. Flexibility is critical to addressing dynamic threats and

[11] This includes, but is not limited to, established SDOs like ISO/IEC JTC1 and related standards (27001/2, 15408, etc.) as well as work from other international SDOs.
[12] 40 USC § 11302(d) (2013).

developing workable solutions for the widely disparate configurations and operational environments across the Federal government.

Several related changes to the acquisition rules are also underway and must be addressed prior to implementing these recommendations. Where the recommendations are closely aligned with an ongoing Federal Acquisition Regulation (FAR) or Defense Federal Acquisition Regulation Supplement (DFARS) rulemaking, a specific reference is provided. In general, implementation must be harmonized with, and be built upon as appropriate, existing international and consensus based standards, as well as statutes and regulations applicable to this field, including the Federal Information Security Management Act of 2002 (FISMA),[13] the Clinger Cohen Act of 1996,[14] the Department of Homeland Security Appropriations Act of 2007,[15] and related sections of the National Defense Authorization Acts,[16] among numerous others. Finally, implementation must be coordinated with the independent regulatory agencies.

While it is not the primary goal, implementing these recommendations may contribute to increases in cybersecurity across the broader economy, particularly if changes to Federal acquisition practices are adopted consistently across the government and concurrently with other actions to implement the Cybersecurity Framework. However, other market forces – more specifically, broad customer demand for more secure ICT products and services – will have a greater impact on the Nation's cybersecurity baseline than changes in Federal acquisition practices.[17]

Changes to the Federal Acquisition System therefore should be focused on strengthening the cybersecurity knowledge, practices, and capabilities within the Federal government's network and domain. The implementation approach should leverage the existing system of voluntary international standards development and the Cybersecurity Framework. The government should start by changing its own practices that increase cyber risk and focus on the types of acquisitions that present the greatest cyber risk and in which investment of scarce resources will provide the greatest return overall.

Background

On February 12, 2013, the President issued Executive Order 13636[18] for Improving Critical Infrastructure Cybersecurity (EO) directing Federal agencies to use their existing

---

[13] 44 U.S.C. § 3541 et seq.
[14] 40 U.S.C. §11101 et seq.
[15] P.L. 109-295, 120 Stat. 552.
[16] See, e.g., Section 806, Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Pub. L. 111-383 (Jan. 7, 2011).
[17] Input received in response to the Working Group's published Request for Information asserts that the Federal government's buying power in the global ICT marketplace, while significant, is insufficient to create a universal change in commercial practices, and reliance on this procurement power alone to shift the market will result in a number of suppliers choosing not to sell to the Federal government. See, General Services Administration (GSA) Notice: Joint Working Group on Improving Cybersecurity and Resilience through Acquisition; Notice-OERR-2013-01, available at http://www.regulations.gov/#!documentDetail;D=GSA-GSA-2013-0002-0030.
[18] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

authorities and increase cooperation with the private sector to provide stronger protections for public and private sector cyber-based systems that are critical to our national and economic security. In accordance with the EO, GSA and DoD established the Working Group to fulfill the requirements of Section 8(e) of the Executive Order, specifically:

> *"(e) Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity."*[19]

By highlighting the need to address feasibility, security benefits, and relative merits of increasing the use of security standards in Federal acquisitions, the EO highlights the need to effectively balance responses to cyber risks against the increased costs those responses might create. Furthermore, consistency in application of procurement rules can drive additional efficiencies.

Cyber Risk and Federal Acquisition

Federal acquisition is a cross-cutting function that directly impacts operations in all departments and agencies. It is most importantly a means to an end – delivery of something that will enable government to accomplish its missions. An end user is most concerned that the output of the process is delivery of the capability that meets the need. However, the acquisition of a capability is only part of the lifecycle, or series of lifecycles, where cyber risks are present.

Increasingly, the Federal government relies on network connectivity, processing power, data storage, and other information and communications technology (ICT) functions, to accomplish its missions. The networks the government relies on are often acquired and sustained through purchases of commercial ICT products and services. These increased capabilities have greatly benefitted our government, but have also, in some cases, made the government more vulnerable to cyber attacks and exploitation.

The Federal government spends more than $500 billion a year for a range of goods and services required to meet mission needs. This amount of spending is large, but in the global context,[20] it represents less than 1 percent of the total market. So while the Federal government is a significant customer, its ability to effect broad market changes through its purchasing is less significant.

---

[19] *Id.*

[20] https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html.

Procurement of commercial items is encouraged in Federal acquisitions, in part by the availability of price competition, but more importantly because it provides immediate access to rapidly evolving technology. Offshore sourcing has demonstrated its merit as a means to reduce costs, and as a result most commercial items are now produced in a global supply chain. Movement of production outside the United States has also led to growing concerns associated with foreign ownership, control, manipulation, or influence over items that are purchased by the government and used in or connected to critical infrastructure or mission essential systems.

Importantly, the problem is not a simple function of geography. Pedigree[21] is a sub-set of factors to consider in cyber risk assessments, yet there are more important factors in addressing the security or integrity of components and end items, including careful attention to the people, processes, and technology used to develop, deliver, operate, and dispose of the products and services used by the government and its contractors.

The modern ICT supply chain is a complex, globally distributed system of interconnected value-networks that are logically long with geographically diverse routes and multiple tiers of international sourcing. This system of networks includes organizations, people, processes, products, and services, and extends across the full system development life cycle, including research and development, design, development, acquisition of custom or commercial products, delivery, integration, operations, and disposal/retirement.

Vulnerabilities can be created intentionally or unintentionally and can come from inside or outside of the supply chain itself. The cyber threat presented by U.S. adversaries (foreign governments, militaries, intelligence services, and terrorist organizations) and those seeking to advance their own cause (hackers and criminal elements) without regard to U.S. national security interests, law enforcement activities, or intellectual property rights has introduced significant new risk to the Federal government and industry. The Federal government and its contractors, subcontractors, and suppliers at all tiers of the supply chain are under constant attack, targeted by increasingly sophisticated and well-funded adversaries seeking to steal, compromise, alter or destroy sensitive information. In some cases, advanced threat actors target businesses deep in the government's supply chain to gain a foothold and then "swim upstream" to gain access to sensitive information and intellectual property. However, it is important to note that most known intrusions are not caused by an adversary intentionally inserting malicious code into an ICT component through its supply chain, but are made through exploitation of unintentional vulnerabilities in code or components (e.g. remote access attacks). Nevertheless, both intentional and unintentional vulnerabilities increase risks. To achieve cyber resiliency, the Federal government must ensure it is capable of mitigating the risks of emerging threats.

The majority of Federal technical information resides on information systems susceptible to the threats and vulnerabilities described above. Therefore, the government must also take into account the risk of this information being targeted for cyber espionage campaigns. This

---

[21] Pedigree is concerned with the original creation and subsequent treatment of ICT hardware or software, including computational objects such as programs and data, and changes from one medium to another. It emphasizes integrity, chain of custody and aggregation rather than content. It is a tool for establishing trust and accountability in information or an end item. See, e.g., Wohlleben, Paul, *Information Pedigree*, (July 29, 2010); available at: http://www.fedtechmagazine.com/article/2010/07/information-pedigree.

information is often unclassified, but it includes data and intellectual property concerning mission-critical systems requirements, concepts of operations, technologies, designs, engineering, systems production, and component manufacturing. Compromises of this information would seriously impact the operational capabilities of Federal systems.

Recently, the problem of counterfeit, "grey market," or other nonconforming ICT components and subcomponents has gained significant attention as well. These materials can be introduced into systems during both initial acquisition and sustainment. As they are unlikely to have the benefit of testing and maintenance appropriate to their use, they create vulnerabilities for the end customer and increase the likelihood of premature system failure or create latent security gaps that would enable an adversary.

Additionally, significant risks are also presented in the operations and maintenance phase and the disposal process. For example, failure to maintain up to date security profiles, install a software patch in a timely fashion, or failing to include identity and access management requirements all introduce cyber risks, but can be managed through the ICT acquisition process. Similarly, an adversary could extract valuable data from improperly destroyed media. An industry stakeholder submitted that the risk of a commercial entity being sued because of improper data disposal is three times greater than the risk of legal action stemming from a data breach caused by loss or theft and six times greater than from data breaches involving the loss of financial information.[22] In addition, the ICT supply chain is vulnerable to events such as intellectual property theft,[23] service availability disruption,[24] and the insertion of counterfeits.[25] When dealing with a critical system or component, the consequences of these events can be significant, impacting the safety, security, and privacy of potentially millions of people.

While the commercial ICT supply chain is not the source of all cyber risk, it presents opportunity for creation of threats and vulnerabilities, and commercial ICT enables the connectivity that is a necessary element for cyber exploitation. Furthermore, when the Federal government acquires a solution that has inadequate cybersecurity "baked in," the government incurs increased risk throughout the lifespan and disposal of the product or service, or at least until it incurs the added cost of "bolting on" a fix to the vulnerability. It is the lasting effects of inadequate cybersecurity in fielded solutions that makes acquisition so important to achieving cybersecurity and resiliency. Purchasing products and services that have cybersecurity designed and built in may be more expensive in some cases, but doing so reduces total cost of ownership by providing risk mitigation and reducing the need to fix vulnerabilities during use and disposal.

An important way to mitigate cyber risk is adherence to security standards. Federal contracts currently require conformance to a variety of security standards as published in the

---

[22] Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition, Request for Information, 78 Fed. Reg. 27966 (May 13, 2013) (hereinafter, "GSA RFI").

[23] See, e.g., "*IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property,*" 2, The National Bureau of Asian Research (May 2013).

[24] See, e.g., "*White Paper: Managing Cyber Supply Chain Risks,*" 5, Advisen Inc., (May 2013); available at: http://www.onebeaconpro.com/sites/OneBeaconPro/blind/Advisen%20Supply%20Chain%20Risks%20Report.pdf.

[25] See, e.g., Section 818 "Detection and Avoidance of Counterfeit Electronic Parts," FY 2012 NDAA (PL 112 -81); and Defense Federal Acquisition Regulation Supplement: Detection and Avoidance of Counterfeit Electronic Parts (DFARS Case 2012-D055), Proposed Rule, 78 Fed. Reg. 28780 (May 16, 2013).

Federal Acquisition Regulation, Defense Federal Acquisition Regulation Supplement, General Services Administration Acquisition Manual, and Homeland Security Acquisition Manual. The government can immediately increase the value it obtains through the use of security standards in a cost-effective way by increasing the degree of specificity and consistency with which it applies standards to requirements in its contracts.[26] This can be accomplished by ensuring contractual requirements are explicit as to which standards, and more specifically, which sections of particular standards, need to be applied against explicitly articulated security needs for the acquired item.

A selective approach to this task is appropriate because all acquisitions do not present the same level of risk. For some acquisitions, basic cybersecurity measures are all that is required to adequately address the risks, and for other acquisitions, additional cybersecurity controls are required. The differences are primarily driven by the variations in fitness for use of the acquired items, which is closely related to the risk tolerance of the end user. For example, the same printer/copier procured to perform the same function by two different organizations might legitimately require different security protections based on operational environments and end users. Differences in risk tolerance between end users can be based on, among numerous other things, differences in information sensitivity and mission criticality that are associated with specific department and agency technical implementations.

The government must work to ensure that there is not a mismatch between mission-based cybersecurity requirements for product assurance or connectivity and what it is actually purchasing. It is important to note that implementation must be consistent with U.S. obligations under international agreements, and voluntary international standards should be applied whenever possible in Federal acquisitions. Ultimately, the government must continue striving to make innovation the standard in improving cybersecurity.

Recommendations

Commercial ICT is ubiquitous in Federal networks, even those that handle the most sensitive information and support essential functions of the government. Therefore, the recommendations focus primarily on exposure to cyber risks related to acquisitions of ICT and how those risks should be addressed. However, due to the increasing connectivity of the world and the growing sophistication of threats, the recommendations apply equally to acquisitions that are outside the boundaries of traditional definitions of ICT.

I. Institute Baseline Cybersecurity Requirements as a Condition of Contract Award for Appropriate Acquisitions.

Baseline cybersecurity refers to first-level information and security measures used to deter unauthorized disclosure, loss, or compromise. Basic protections such as[27] updated virus

[26] In some circumstances, this will reduce costs by reducing the level of effort required by the contractor to figure out which specific controls in a standard apply to the acquisition; see e.g., Microsoft response to GSA RFI, available at http://www.regulations.gov/#!documentDetail;D=GSA-GSA-2013-0002-0005.

[27] This list is intended to be illustrative only.

protection, multiple-factor logical access, methods to ensure the confidentiality of data, and current security software patches are broadly accepted across government and the private sector as ways to reduce a significant percentage of cyber risks. When the Federal government does business, directly or indirectly, with companies that have not incorporated baseline cybersecurity protections into their own operations and products, the result is increased risk. Ensuring that the people, processes, and technology with access to assets at risk are employing baseline requirements raises the level of cybersecurity across the Federal enterprise.

First-level protective measures are typically employed as part of the routine course of doing business. The cost of not using basic cybersecurity measures would be a significant detriment to contractor and Federal business operations, resulting in reduced system performance and the potential loss of valuable information. It is also recognized that prudent business practices designed to protect an information system are typically a common part of everyday operations. As a result, the benefit of protecting and reducing vulnerabilities to information systems through baseline cybersecurity requirements offers substantial value to contractors and the Government.

The baseline should be expressed in the technical requirements for the acquisition and should include performance measures to ensure the baseline is maintained and risks are indentified throughout the lifespan of the product or service acquired. Due to resource constraints and the varying risk profiles of Federal acquisitions, the government should take an incremental, risk-based approach to increasing cybersecurity requirements in its contracts beyond the baseline.

As a preliminary matter, cybersecurity requirements need to be clearly and specifically articulated within the requirements of the contract. Often, cybersecurity requirements are expressed in terms of compliance with broadly stated standards and are included in a section of the contract that is not part of the technical description of the product or service the government seeks to acquire.[28] This practice leaves too much ambiguity as to which cybersecurity measures are actually required in the delivered item. This recommendation envisions requirements for baseline cybersecurity requirements for contractor operations as well as products or services delivered to the government.

This recommendation is intended to be harmonized with the ongoing FAR and DFARS rulemakings entitled "Basic Safeguarding of Contractor Information Systems,"[29] and "Safeguarding Unclassified Controlled Technical Information."[30]

II. Address Cybersecurity in Relevant Training.

As with any change to practice or policy, there is a concurrent need to train the relevant workforces to adapt to the changes. This is particularly the case when the changes involve major

[28] See, Comment on FR Doc # 2013-11239, GSA-GSA-2013-0002-0005, Nicholas, J. Paul, Microsoft Corporation (Jun. 12, 2013), available at http://www.regulations.gov/#!docketBrowser;rpp=100;so=DESC;sb=docId;po=0;dct=PS;D=GSA-GSA-2013-0002.

[29] 77 Fed. Reg. 51496 (Aug. 24, 2012), Proposed rule, FAR Case 2011-020.

[30] DFARS Case 2011-D039, Interim Rule, under review by Office of Information and Regulatory Affairs (last accessed, June 10, 2013, http://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf).

shifts in behavior, like the risk management changes outlined in these recommendations. Additionally, the government should implement an acquisition cybersecurity outreach campaign targeted at industry stakeholders.[31] The training overall, and the industry engagement in particular, should clearly articulate that the government is changing its buying behavior relative to cybersecurity by adopting a risk-based methodology, and as a result, the government will require more from industry relative to cybersecurity in certain types of acquisition.

Increasing the knowledge of the people responsible for doing the work will facilitate appropriate cyber risk management and help avoid over-specifying cybersecurity requirements (which leads to higher costs) or under-specifying cybersecurity requirements (which leads to greater risks).

III. Develop Common Cybersecurity Definitions for Federal Acquisitions.

Increasing the clarity of key cybersecurity terms in Federal acquisitions will increase the efficiency and effectiveness of both the government and the private sector. The ability to effectively develop and fulfill requirements depends in large part on a shared understanding of the meaning each party assigns to a key terms, especially in specialized professional disciplines like cybersecurity and acquisition. This need is especially acute when these terms are included in legal instruments as part of the acquisition process.

Unclear and inconsistently defined terms lead, at best, to suboptimal outcomes for both efficiency and cybersecurity. When misunderstandings persist in the acquisition process, they may create inaccuracy or confusion about technical requirements, market research, cost estimates, budgets, purchase requests, solicitations, proposals, source selections, and award and performance of contracts. In operational activities governed by legal instruments, varying definitions can be much more difficult to address and create very real cost impacts, including contractual changes, terminations, and litigation. A good baseline for these definitions is found in consensus based, international standards.

This recommendation is intended to be harmonized with the ongoing DFARS rulemaking entitled "Detection and Avoidance of Counterfeit Electronic Parts."[32]

IV. Institute a Federal Acquisition Cyber Risk Management Strategy.

The government needs an interagency acquisition cyber risk management strategy that requires agencies to ensure their performance meets strategic cyber risk goals for acquisition and is part of the government's enterprise risk management strategy. The strategy should be based on a government-wide perspective of acquisition and be primarily aligned with the methodologies and procedures developed to address cyber risk in the Cybersecurity Framework.

---

[31] E.g., GSA provides training about its Multiple Award Schedules (MAS) program through the "Pathway to Success" training. This is a mandatory training module that provides an overview of GSA MAS contracts. Potential offerors must take the "Pathway To Success" test prior to submitting a proposal for a Schedule contract. See, https://vsc.gsa.gov/RA/research.cfm. Additionally, contractors might, in certain circumstances, be required to complete ongoing training throughout contract performance. Specific training about an acquisition might also be included in requirements to become a qualified bidder, and become a source selection criterion.

[32] 78 Fed. Reg. 28780 (May 16, 2013), Proposed Rule; DFARS Case 2012-D055.

It should identify a hierarchy of cyber risk criticality for acquisitions and include a risk-based prioritization of acquisitions. The risk analysis should be developed in alignment with the Federal Enterprise Architecture[33] and NIST Risk Management Framework (RMF).[34]

The strategy should include development of "overlays:" fully specified sets of security requirements and supplemental guidance that provide the ability to appropriately tailor security requirements for specific technologies or product groups, circumstances and conditions, and/or operational environments.[35]

When developing the strategy, the government should leverage existing risk management processes and data collection methodologies and consistently incorporate cyber risk as an element of enterprise risk management. The strategy should encompass standard network security practices to address vulnerability of information to cyber intrusions and exfiltration. The strategy should leverage supply chain risk management processes to mitigate risks of non-conforming items (such as counterfeit and tainted products). And it should include appropriate metrics to define risk and to measure the ability of agencies to apply empirical risk modeling techniques that work across both public and private organizations. In developing the strategy, the government should use the active, working partnerships between industry, the civilian agencies, and the intelligence community, and create such partnerships where they do not already exist, with the goal of leveraging validated and outcome-based risk management processes, best practices, and lessons learned.

Where appropriately defined categories of similar types of acquisitions already exist,[36] the government should develop overlays for those types of acquisitions. The overlays should be developed in collaboration with industry, and consistently applied to all similar types of Federal acquisitions. The starting point for development of the requirements should be the Cybersecurity Framework.

The overlays should encompass realistic, risk-based controls that appropriately mitigate the risks for the type of acquisition and should define the minimum acceptable controls for any acquisition that is of a similar type. The overlays should not, as a general rule, incorporate standards directly into contracts and should avoid prescriptive mandates for specific practices, tooling, or country-specific standards, because the inflexibility of those approaches often inadvertently increases costs without actually reducing risk.[37] Instead, the overlays should

---

[33] Available at http://www.whitehouse.gov/omb/e-gov/fea/.

[34] See, NIST Special Publication 800-37, Revision 1 (Feb. 2010).

[35] See, e.g., The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Available at: http://www.gsa.gov/portal/category/102375. See also, the Information Systems Security Line of Business (ISSLoB) is a comprehensive and consistently implemented set of risk-based, cost-effective controls and measures that adequately protects information contained in federal government information systems. Available at: http://www.dhs.gov/information-systems-security-line-business.

[36] See, e.g., FedRAMP, ISSLoB, and Federal Strategic Sourcing Initiative (FSSI) (available at: http://www.gsa.gov/fssi.), among others. These programs have defined categories of similar types of products and services.

[37] Directly incorporating standards could freeze the status quo and hamper or prevent the evolution of countermeasures required to address the dynamic threat and technology landscapes. It might also create a risk that other nations will adopt similar mandates which could further increase supply chain costs. Incorporating

specifically identify security controls from within standards that should be applied to the type of acquisition being conducted. The overlays should also include acquisition and contractual controls like source selection criteria and contract performance measures. Finally, to the greatest extent possible, the overlays should be expressed as technical requirements. This approach will allow the government to describe top-level cybersecurity requirements, decompose them to a lower level for an individual acquisition, and then articulate them consistent with and in a similar manner as other requirements for the fielded solution.

This recommendation is based on the fact that not all assets delivered through the acquisition system present the same level of cyber risk or warrant the same level of cybersecurity, and requiring increased cybersecurity in planning and performance of government contracts creates cost increases for contractors and the Federal government. Such cost increases must be balanced against the nature and severity of cyber risks and the corresponding cost or performance reductions in other functionality. The Federal government can mitigate the amount of any cost increases if it creates certainty by adopting cybersecurity requirements across market segments and similar types of procurement.

V. Include a Requirement to Purchase from Original Equipment or Component Manufacturers, Their Authorized Resellers, or Other "Trusted" Sources, Whenever Available, in Appropriate Acquisitions.

Ensuring that the goods provided to the government are authentic and have not been altered or tampered with is an important step in mitigating cyber risk. Inauthentic end items and components often do not have the latest security-related updates or are not built to the original equipment (or component) manufacturer's (OEM) security standards. In certain circumstances, the risk of receiving inauthentic, counterfeit, or otherwise nonconforming items is best mitigated by obtaining required items only from OEMs, their authorized resellers, or other trusted sources.[38]

OEMs have a heightened interest in ensuring the authenticity of their products, and this interest carries through into their policies for designating certain suppliers or resellers as "authorized." Limiting eligibility to only these types of sources for *all* acquisitions may not be compatible with acquisition rules, socioeconomic procurement preferences, or principles of open competition. Additional trusted sources can be identified through the use of qualified products, bidders, or manufacturers lists (QBL)[39] to ensure that identified sources meet appropriate standards for providing authentic items. The QBLs should be based on the cyber risk mitigation value provided by the use of the trusted source.

---

government-specific standards that would duplicate existing security-related standards or creating country-specific requirements that could restrict the use of long-standing and highly credible global suppliers of technology could have significant negative effects on the government's ability to acquire the products and services it needs.

[38] See, e.g., Solutions for Enterprise Wide Procurement (SEWP) V, is a multiple-award Government-Wide Acquisition Contract (GWAC) that provides IT Products and Product Solutions. SEWP is administered by NASA, and the recently released draft RFP includes this limitation of sources by requiring offerors for certain types of items to be an authorized reseller of the OEM; available at https://www.sewp.nasa.gov/sewpv/.

[39] 48 C.F.R. § 9.203 (2013).

Even with use of trusted sources, it may be possible to have "authentic" equipment that still has cyber vulnerabilities. This approach also represents a limitation of available sources and therefore should only be used for types of acquisition that present risks great enough to justify the negative impact on competition or price differences between trusted and un-trusted sources. For acquisitions that present these types of risks, the government should limit sources to OEMs, authorized resellers, and trusted suppliers, and the qualification should be incorporated into the full acquisition and sustainment life cycles, starting with requirements definition, acquisition planning, and market research.

If the government chooses to use a reseller, distributor, wholesaler, or broker that is not in a trusted relationship with the OEM, then the government should obtain assurances of the company's ability to guarantee the security and integrity of the item being purchased. Such a trusted supplier compliance requirement is especially important when acquiring obsolete, refurbished, or otherwise out-of-production components and parts.

The terms and conditions a supplier or reseller must meet to obtain status as a "trusted" source will vary between market segments, but in general suppliers will be assessed against a broad set of criteria including long-term business viability, quality control systems, order placement and fulfillment processes, customer support, customer returns policies, and past record, such as by a search in Government-Industry Data Exchange Program[40] (GIDEP). In order to establish QBLs, the substance and application of these criteria must be evaluated by the government, or a third party authorized by the government, on a regular basis to ensure the QBL designation provides continued value in actually mitigating cyber risk.

The method by which the government conducts the evaluations should be based on the cyber risk of the acquisition type. For example, for acquisition types that present the greatest risk, the appropriate evaluation method might be an audit performed by government personnel. For less risky categories, the appropriate evaluation method might be first, second, or third party attestation of company conformance to a standard. At a minimum, the qualification program should be based on the Cybersecurity Framework, have consistent and well defined processes for validation and testing, consider the use of third parties to conduct reviews and approvals, and include enforcement mechanisms.

VI. Increase Government Accountability for Cyber Risk Management.

As described above, Federal systems are subject to cyber risks throughout the development, acquisition, sustainment, and disposal life cycles. The application of cyber risk management practices must similarly cut across all phases and functionality, including but not limited to, technology and development; engineering and manufacturing; production; operations and support; security; and counterintelligence. The success of such practices will be dependent upon the integration of cybersecurity risks into existing acquisition processes to inform key stakeholders and decision makers from each of these phases and functions.

---

[40] GIDEP is a cooperative activity between government and industry participants seeking to reduce or eliminate expenditures of resources by sharing technical information. Since 1959, over $2.1 billion in prevention of unplanned expenditures has been reported. See, http://www.gidep.org.

This recommendation is intended to integrate security standards into acquisition planning and contract administration and incorporate cyber risk into enterprise risk management to ensure that key decision makers are accountable for decisions regarding the threats, vulnerabilities, likelihood, and consequences of cybersecurity risks in the fielded solution.

First, cyber risk should be addressed when a requirement is being defined and a solution is being analyzed. Based on the cybersecurity overlay requirements for the type of acquisition, the requirement developer and acquisition personnel determine which controls should be included in the requirement, identify which risk decisions are critical for the acquisition, and ensure that the critical decisions are informed by key stakeholders and the cyber risk management plan.

Next, prior to release of the solicitation, acquisition personnel should certify that appropriate cybersecurity requirements are adequately reflected in the solicitation. This includes but is not limited to incorporation into technical requirements, pricing methodology, source selection criteria and evaluation plan, and any post-award contract administration applications.

Third, during the source selection process, acquisition personnel should participate in the proposal evaluation process and ensure that the apparent best value proposal meets the cybersecurity requirements of the solicitation.

Finally, to the extent any conformance testing, reviews of technology refreshes, supply chain risk management measures, or any other post-award contract performance matters are relevant to cybersecurity, the accountable individual (e.g. program executive), with the assistance of acquisition personnel, should be required to certify that the activity was conducted in accordance with prescribed standards.

Conclusion

The recommendations in this report address feasibility, benefits, and merits of incorporating standards into acquisition planning and contracts and harmonizing procurement requirements through an initial focus on the need for baseline cybersecurity requirements, broad workforce training, and consistent cybersecurity terminology. These are suggested to be combined with incorporation of cyber risk management into enterprise risk management, development of more specific and standardized use of security controls for particular types of acquisitions, limiting purchases to certain sources for higher risk acquisitions, and increasing government accountability for cybersecurity throughout the development, acquisition, sustainment, use, and disposal life cycles.

The recommendations are much more about changing the behavior of government program managers and acquisition decision makers than they are about changing the behavior of industry segments or contracting officers. The Government cannot make all of its contracting officers into cybersecurity experts, but it can improve the cybersecurity of its acquisitions by ensuring appropriate accountability for cyber risk management is incorporated into the acquisition process. The bottom line is that the government will only achieve the goal of increasing cybersecurity and resilience through acquisitions by making sure its own practices are

not increasing risks unnecessarily. Using the methods outlined in these recommendations will allow the government to make better choices about which cybersecurity measures should be implemented in a particular acquisition. And the choices will be based on disciplined, empirical cyber risk analysis.

Achieving cyber resilience will require investments in the personnel and resources necessary to manage the risks. Building cyber resiliency also requires interagency coordination and cooperation between the public and private sectors (including between supply chain suppliers and providers). It also requires everyone from front-line employees to those in the most senior leadership positions to have greater awareness of the issue.

In summary, the government should approach this complex matter thoughtfully and collaboratively, taking affirmative steps to minimize the adverse impact on the ICT market by ensuring its own policies and practices are part of the solution.

APPENDIX I - JOINT WORKING GROUP ROSTER

The individuals listed in the table below are the core team that drafted the report and developed the recommendations. But there are many other individuals from both public and private sector organizations who also participated substantially. All brought a high degree of professionalism and knowledge to their work, and represented the equities of their organizations, functional disciplines, and the interests of the Federal government in an exemplary manner.

AGENCY	ORGANIZATION	NAME(S)
Department of Defense	Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics; Defense Procurement and Acquisition Policy	Michael Canales Mary Thomas
	Office of the Assistant Secretary of Defense for Cyber Policy	Joshua Alexander
	Office of the Chief Information Officer	Don Davidson Jenine Patterson
General Services Administration	Office of Emergency Response and Recovery	Christopher Coleman
	Federal Acquisition Service	Emile Monette Larry Hale Shondrea Lyublanovits
	Office of Governmentwide Policy	Marissa Petrusek
Office of Management and Budget	Office of Federal Procurement Policy	Jeremy McCrary
Department of Homeland Security	National Protection and Programs Directorate, Office of Cybersecurity and Communications	Joe Jarzombek Michael Echols
	Directorate for Management, Office of the Chief Procurement Officer	Camara Francis Shaundra Duggans
Department of Commerce	National Institute of Standards and Technology	Jon Boyens

APPENDIX II - STAKEHOLDER ENGAGEMENTS

The list below reflects individual engagements with stakeholders conducted by the Working Group as part of the deliberative and report-writing process. This list does not include regular meetings with the DHS ITF, or Working Group meetings. Where the ITF or an agency with members in the Working Group is identified, the engagement was conducted as an adjunct to the regular Working Group and ITF processes, or was a regular engagement that had particular significance (e.g., briefing the draft report to interagency principals).

Date	Engagement
09 Jan 13	TechAmerica
10 Jan 13	Professional Services Council
14 Jan 13	Coalition for Government Procurement
28 Jan 13	TechAmerica
29 Jan 13	Federal Bureau of Investigations
08 Feb 13	TechAmerica
12 Feb 13	Coalition for Government Procurement
15 Feb 13	DHS Integrated Task Force
19 Feb 13	DHS Integrated Task Force
26 Feb 13	Private Company
05 Mar 13	NIST Software Assurance Forum
05 Mar 13	National Defense Industry Associations
08 Mar 13	DHS Integrated Task Force
11 Mar 13	ABA Public Contract Law Section, Cybersecurity Committee
13 Mar 13	NIST Research and Development
14 Mar 13	DHS Incentives Working Group
15 Mar 13	CIPAC IT Sector Coordinating Council, Supply Chain Working Group
21 Mar 13	Private Company
25 Mar 13	CIPAC IT and Communications Sector Coordinating Councils
01 Apr 13	CNCI 11 Working Group
02 Apr 13	Defense Intelligence Agency
02 Apr 13	National Defense Industry Association
04 Apr 13	NIST Designed-in Cybersecurity for Cyber-Physical Systems
04 Apr 13	National Defense Industry Association Cyber Division meeting
16 Apr 13	CIPAC IT Sector Coordinating Council
18 Apr 13	TechAmerica Cybersecurity Committee
19 Apr 13	Professional Services Council
22 Apr 13	CIPAC IT and Communications Sector Coordinating Councils
30 Apr 13	ABA Public Contract Law Section, Cybersecurity Committee meeting
01 May 13	CIPAC IT and Communications Sector Coordinating Councils meeting
01 May 13	Private Company
02 May 13	Semiconductor Industry Association meeting
02 May 13	DHS Integrated Task Force briefing to members
02 May 13	Department of Treasury
03 May 13	Private Company
06 May 13	Private Companies (2)
07 May 13	ACT-IAC Cybersecurity Shared Interest Group meeting

07 May 13	Presentation to interagency at Cyber IPC meeting
09 May 13	Coalition for Government Procurement meeting
13 May 13	Private Companies (2)
14 May 13	Private Company
22 May 13	Internet Security Alliance Board of Directors meeting
22 May 13	National Security Agency, Contracting Policy
22 May 13	Interview, Washington Post
22 May 13	Provided background, Wall Street Journal
23 May 13	Live radio interview, Federal News Radio, "In Depth"
03 Jun 13	Private Companies (5)
03 Jun 13	Department of Treasury
03 Jun 13	Security Industry Association, Government Summit
04 Jun 13	Information Technology Industry Council
04 Jun 13	University of Maryland