Improving Cybersecurity and Resilience through Acquisition

[*DRAFT*] IMPLEMENTATION PLAN

Version *1.0*

February 2014

Table of Contents

Introduction

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

The final report of the *Department of Defense (DoD) and General Services Administration (GSA) Joint Working Group on Improving Cybersecurity and Resilience through Acquisition* was signed by the Secretary of Defense and the Administrator of General Services on January 23, 2014.[1]

The DoD-GSA report (Report) recommends six (6) strategic reforms to address issues relevant to cybersecurity in Federal acquisitions, suggests how challenges might be resolved, and identifies important considerations for the implementation of the recommendations.

Purpose

The Implementation Plan (Plan) translates the Report recommendations into on-the-ground actions that will improve cybersecurity and resilience by reforming management of the people, processes, and technology involved in Federal acquisitions. The government is committed to continuing the open, collaborative, stakeholder-centric process used to develop the recommendations in development of this Plan.

The Plan incorporates the implementation considerations identified in the Report, breaks each recommended reform into identifiable outcomes and steps to achieve each outcome, assigns one or more office of primary responsibility for each step, presents specific actions Federal agencies will take to improve cybersecurity and resilience in acquisitions, and suggests when each step will be completed.

Plan Development Process

The Plan will be developed using an iterative process to facilitate sequential and concurrent implementation of the recommendations as appropriate. Planning will be accomplished through a series of stakeholder outreach and engagement activities for each recommendation, including but not limited to requests for public comment and in-person meetings.

An Appendix to the Plan will be developed for each recommendation in the Report. Upon completion, each Appendix will provide a roadmap for implementation for the recommendation, and examples of how to accomplish the actions in the Plan.

It is important to note that the order of the recommendations in the Report is not indicative of the sequence of implementation. The Plan is being developed by addressing the recommendations in the order in which they should be implemented.

Assumptions/Clarifications/Constraints

- An open, collaborative, stakeholder-centric process will be used to accomplish all tasks required to achieve complete implementation of the Report recommendations. At a minimum, this process will include opportunities for public comment on documentation and interagency coordination through official channels.

[1] The Report is available at http://gsa.gov/portal/content/176547.

- The majority of resources required to conduct the activities identified in the Plan have not been specifically identified. A lack of dedicated resources may inhibit or delay accomplishment of the actions in the Plan.
- The definition of overlays in the Report differs slightly from the definition in NIST SP 800-53 revision 4. To clarify, the definition in NIST SP 800-53 revision 4 will be used for purposes of implementation.

Recommendation IV: Acquisition Cyber Risk Management Strategy

The first recommendation that will be implemented is number four in the Report, "*Institute a Federal Acquisition Cyber Risk Management Strategy*." This recommendation will be implemented first because the risk management strategy and processes to institute it provide the foundation that is necessary for the other recommendations to be implemented.

Not all assets delivered through the acquisition system present the same level of cyber risk or warrant the same level of cybersecurity. Furthermore, resources to address acquisition cyber risk are scarce. Therefore, the government requires a risk-based, phased approach to managing these risks.

Implementation of this recommendation draws from the sourcing practices of spend analysis, strategic categorization of buying activities, and category management, combined with application of information security controls and safeguards and procurement risk management practices like pricing methodology, source selection, and contract performance management.

The goal of this recommendation is to develop a repeatable, scalable process for addressing cyber risk in federal acquisitions based on the risk inherent to the product or service being purchased, that is flexible enough to be adapted to the various risk tolerances of end users or risk owners.

First, the government will specifically identify which types of acquisitions present cyber risk, group those types of acquisition together into Categories, and measure the comparative cyber risk presented by purchases of items[2] in the Category. Once a risk-based prioritization has been accomplished, the government can assign resources and develop Overlays that include risk mitigations drawn from both procurement and information security practices. This will include choosing security controls from NIST SP 800-53, source selection criteria, pricing methodologies, and contract performance indicators, among others.

Outputs/Completion Criteria

The implementation of this recommendation will be considered complete when the following are documented and disseminated throughout the stakeholder community:

1. A list of Categories of acquisition, prioritized by highest risk; and
2. A repeatable, scalable process for developing cyber risk Overlays for Categories of acquisition.

Overview of Major Tasks and Sub Tasks

Completion of the following sequential tasks is necessary to implement this recommendation.

1. Develop Acquisition Category Definitions
   a. Determine Taxonomy

[2] Use of the term "item" in this Plan refers to purchases of either products, services, or both.

    b. Conduct Spend Analysis
2. Conduct Acquisition Risk Assessment and Prioritization
3. Develop Methodology to Create Overlays
    a. Determine Appropriate Security Controls
    b. Determine Appropriate Acquisition Mitigations
    c. Determine Appropriate Other Safeguards

Task Descriptions

MAJOR TASK 1: Develop Acquisition Category Definitions

The purpose of this task is to develop and instantiate a repeatable, scalable process for categorizing Federal acquisitions. The output of this task will be a list of Category definitions and a process that can be used by all Federal acquisition activities to consistently categorize acquisition activities in a way that facilitates cyber risk assessment and management.

SUB TASK 1.a. Determine Taxonomy and Establish Category Definitions

The goal of this sub task is to identify and gain stakeholder acceptance of taxonomy to describe the various types of Federal acquisition spending and the grouping of similar types of acquisition activity into Categories. Establishing an agreed upon common taxonomy will facilitate grouping similar types of acquisitions into Categories that can subsequently be assessed for cyber risks which can then be appropriately mitigated through application of a single Overlay for each Category.

The taxonomy selected needs to facilitate definition of Categories that are broad enough to be understandable and provide economies of scale, but specific enough to enable development of Overlays that provide meaningful, adequate and appropriate safeguards for the types of risks presented by the products or services in the Category.

The Category definitions should group similar types of acquisitions together based on characteristics of the product or service being acquired, supplier or market segments, and prevalent customer/buyer behavior. The Categories need to be "right-sized," to enable development of Overlays.

For example, a Category that includes all Information and Communication Technology (ICT) products and services would be overly broad because the cyber risks inherent to ICT products and services are different, so the appropriate mitigations need to be different. Similarly, ICT hardware and software are best mitigated using different controls, so a Category that included both is also too broad. A Category that includes all software might be appropriate (if the preponderance of cyber risks in software can be addressed using a single set of controls), but one that includes all hardware might still be too broad because of the differences between the numerous types of hardware (e.g., network equipment, peripherals, etc).

SUB TASK 1.b. Conduct Spend Analysis

The purpose of this sub task is to determine which Categories of acquisitions do and do not require greater cybersecurity protections for purposes of determining which types of acquisitions thereby do or do not require development of a Category Overlay.

Using the agreed upon taxonomy, determine which types of acquisitions present potential cyber risk. To be accomplished properly, this task requires applied expertise in the acquisition and information security disciplines.

The reason for conducting the spend analysis is to reduce the number of Categories that need to have Overlays developed. This determination should be based on the inherent risk the type of acquisition presents for *any* end user.

This sub task is essentially a binary assessment of the cyber risks presented by purchase of items in the various Categories. The risks inherent to each Category should be assessed objectively, in the context of the risk presented by *any* use case. The objective risk assessment is intended to answer the question, "*Does this Category present cyber risk to any possible end user*?"

The Report explicitly states that acquisitions governed by CNSS are outside the scope of the recommendations, so National Security Systems, while higher risk, are not intended to be addressed in this process. In addition, certain Categories will be comprised of items that do not present cyber risks, and those Categories do not need increased cybersecurity protections.

As an example, acquisitions of paper clips, pencils, paper and other items that do not or cannot connect to a Federal network or involve handling of Federal data probably do not present cyber risk, and if not, a Category comprised of these types of items does not require application of an Overlay. However, acquisitions of items that may not fall within traditional definitions of ICT, but are connected to networks and involve use and transmission of Federal data, such as printers or copiers, likely do present cyber risks, and therefore should be required to incorporate increased cybersecurity protections, as expressed in an Overlay.

MAJOR TASK 2: Conduct Acquisition Risk Assessment and Prioritization

The output of this task is a ranked list of Categories based on the comparative cyber risk presented by acquisitions included in the Categories. Absent other factors, such as timing of a major government-wide acquisition in another (less risky) Category that might warrant Overlay development in that Category first, the Category that is determined to have the highest risk through this comparative assessment would be the first one for which an Overlay is developed.

Although all elements of the risk management cycle are important, risk assessments provide the foundation for other elements of the cycle. In addition to providing a prioritized list of Categories, this risk assessment will also provide a basis for establishing appropriate risk management controls and selecting cost-effective techniques to implement these policies. Where a Category is determined to have higher risk relative to other types of acquisitions, the level of resources expended to address those risks will also be justifiably higher.

This sub task is comprised of a comparative risk assessment that answers the question, "*Which of the Categories presents the greatest cyber risk as compared to the other Categories*?"

For example, a multi-function printer / scanner / copier can have multiple use cases and end users, and the risk the item presents varies greatly according to the specific end user, often because of differences in the sensitivity of data sent to the device and the network it is connected to.

MAJOR TASK 3: Develop Methodology to Create Overlays

Accomplishment of this task will produce a scalable, repeatable process to develop Overlays of information security, acquisition, and other controls for each Category.

The Overlays will provide a tool for acquisition officials to use throughout the acquisition lifecycle (see, Report, recommendation VI). Each Overlay will provide:

1. An articulation of the level of risk presented by the Category (this might be expressed as "high," "moderate," or "low," or by some other nominal description (i.e., level 1, 2, 3, 4 …etc.) that links the level of risk of the Category to the risk assessment conducted in Task 2, (see above);
2. A specific set of minimum controls that must be included in the technical specifications, acquisition plan, and during contract administration and performance for any acquisition in the Category;
3. The universe of additional controls that are relevant to the Category but are not required in the minimum (i.e., a "menu"), and
4. Examples of sets of the identified additional controls that apply to particular use cases (e.g., FIPS 199 High or Moderate system acquisition), as applicable.

Each Overlay will be developed using a collaborative process that includes stakeholder expertise and input from information security and acquisition (including supply chain, sustainment, procurement, and disposal) disciplines in both public and private sectors.

Because risks and threats change over time, it is important that the government periodically reassess risks and reconsider the appropriateness and effectiveness of the policies and controls selected to manage the risks. Therefore, the Overlays should be adjusted periodically (e.g., annually), and on an as-needed basis, when changes occur in technology and market conditions. Therefore, the goal is to ensure the process used to create the Overlays should be repeatable, transparent, and scalable.

SUB TASK 3.a. Determine Appropriate Security Controls

[This section is TBD based on input received from stakeholders.]

SUB TASK 3.b. Determine Appropriate Acquisition Mitigations

[This section is TBD based on input received from stakeholders.]

SUB TASK 3.b. Determine Appropriate Other Safeguards

[This section is TBD based on input received from stakeholders.]