Washington Cyber Roundtable

Cyber Collaboration Where It Counts

Cybersecurity Acquisition Reform Report

For Congresswoman Barbara Comstock

April 2016

CYBERSECURITY ACQUISITION REFORM

Introduction

The Washington Cyber Roundtable hosted Congresswoman Barbara Comstock in March 2016 for a discussion about "Congress and Cybersecurity: The Way Ahead." She shared her views on current legislative efforts to improve the nation's cyber posture and the need for a healthy partnership between the public and private sectors. The exchange of ideas and challenges touched upon best practices, information sharing, education, forensics, and action items to bring before Congress.

A major concern of participants is how the current acquisition process is not responsive to or appropriate for the urgent need for cyber services and products. In many instances, the length of time to define government requirements and produce a Request for Proposal, review and award a contract is counter-productive, resulting in outdated or unusable cyber services and products. Additionally, a continuing resolution also deadlocks time sensitive cyber capability procurements through current means. Promoting basic cyber hygiene, requiring continuous diagnostic and mitigation efforts or other initiatives as advocated by the White House have not produced a sense of urgency nor stewardship in the cybersecurity realm. There remains a much needed culture shift in addressing the threats of poor cyber security practices.

Ironically, many of the issues were addressed in a report finalized in November 2013 in response to the government-wide implementation of EO 13636 and Presidential Policy Directive 21. This report, *Improving Cybersecurity and Resilience through Acquisition—Final Report of the Department of Defense and General Services Administration* provided a path forward with recommendations to strengthen cyber resilience of the Federal government by improving management of people, processes, and technology affected by the Federal Acquisition System. The final report is provided under separate cover.

This report is divided into two sections:

1. **How Congress Can Help**
   Identifies specific actions Congress can take to improve the situation and improve national security.

2. **Reasoning Behind Industry's Call for Action**
   Dives deeper into the background of why these actions need to be taken.

How Congress Can Help

The following points should be addressed by legislation. Reasoning behind each point is illustrated in the following section.

1. Enforce implementation and oversight of existing regulations while initiating new policy that incentivizes a cultural bias toward continuous improvement through partnership, best practice identification, simplification, and speed of implementation. Provide the Department of Defense (DoD) latitude in programming IT funds to rapidly emerging threats and capabilities. Update as appropriate to ensure policy stays abreast of changes in the cyberspace landscape.

   a. Recommend adjusting the National Defense Appropriation Act to elevate cybersecurity to the same level as counterterrorism, allowing DoD to redirect funds as needed for urgent cybersecurity matters.

   b. Enforce the Common Criteria for Information Technology Security Evaluation developed in 2005. This process builds in security and sets a higher standard for software assurance. While no product will be forever secure, this baseline allows a framework for measurement.

   c. Implement recommendations of the DoD/GSA Report on *Improving Cybersecurity and Resilience through Acquisition.*

2. Enforce Industry adherence to NIST 800-171[1] to ensure protection of services is as important as protection of products introduced to government.

3. Recommend auditing programs such as “Ability One/Source America” to ensure goals are met. Consider open competition with other socio-economic small businesses and/or eligible non-profit companies.

Reasoning Behind Industry’s Call for Action

The IT Acquisition and Services Contracting Process.

It is commonly known that the procurement cycle is not conducive to the fast-paced cyber technology. The time interval to define government requirements, produce a Request for Proposal, review and award a contract and potentially modify a contract for cyber security cannot be based on historical processes for industrial, mission-essential equipment. For example:

(a) The Department of Homeland Security (DHS) canceled a $675M Cyber Centric Mission Support Services contract in February 2016 after repeated delays and a two-year long wait. Submission date was pushed a month due to the number of vendor

[1] NIST 800-171 publication provides guidelines to ensure that sensitive federal information remains confidential when stored in nonfederal information systems and organizations.

questions. FedBizOpps[2] listed 159 interested parties and some 100 companies felt the pinch of significant bid and proposal resource loss.

(b) DHS announced 17 firms winning a $6B multiple-award Indefinite Delivery/Indefinite Quantity (IDIQ) for continuous diagnostics and mitigation (CDM) services and tools for all federal civilian departments and agencies in August 2013. The cyber threat and damage has increased according to open source research and the Federal Information Security Management Act (FISMA) report card shows the level of improvement still needed. However, less than $300M in task orders have been awarded.

Cost is a factor for industry, as well as damage to the public/private trust relationship when there are major contract delays. There were some companies that did not bid on CDM, taking the long view that it would not be a profitable undertaking based on perception of government reliability of executing cyber contracts.

- **Training for contracting officers.** What appears to be missing is an applied understanding of the Industry resources involved in researching, building a team and pursuing a government contract—especially when award delays end in a non-award. A common theme surfaced during discussions that contracting officers with few years' experience are often risk-averse, less likely to have a depth of understanding of cyber mission needs, and fall back on general processes. This risk-aversion hinders collaboration between government and industry.

    - Acquisition and Procurement **curricula** should be updated to deal with cybersecurity and its urgent nature. Examples of effective training efforts:

      (a) The Office of Management and Budget (OMB) Office of Federal Procurement Policy created the Digital Services Contracting's Professional Training and Development Program. It is intended to develop professionals who can embed with agency digital service teams as their business advisers, as well as act as advocates for digital services procurement government-wide. The U.S. Digital Services launched in 2014 supports a transformative change in the federal acquisition culture, recognizing how revolutionary digital buying can be. Digital services procurement requires creativity, critical thinking, alliance-building and stakeholder wrangling. There is a Digital Service Playbook (http://playbook.cio.gov/) as well as a TechFAR Handbook (http://playbook.cio.gov/techfar) produced to help government be agile and adopt smarter ways of acquiring high-quality digital services.

      (b) Air Combat Command's Acquisition Management and Integration Center (AMIC) developed a progressive approach to acquisitions that helps the teams deal with the inevitable challenges of change. Their solution implemented on-going learning, enabled knowledge transfer and ensured team members spoke the same language as contracting professionals

[2] Websites posting RFP information are obsolete as soon as posted. Industry teams have been formed and quite likely, the award is tilting favorably towards a team. Acquisition information access should be an equal opportunity similar to Exchange Traded Funds on Wall Street.

throughout the acquisition life cycle — from pre-award requirements gathering, to quality assurance, through contract closeout. Contracting, program management, logistics, financial management and quality assurance personnel all working together, breaking stove pipes while making acquisition a team sport.[3] This is a model to emulate.

- **Proper policy for requirement owners and strategic vehicles**. Established policies assume compliance and yet, it appears that in some organizations, there are no measurements or performance requirements to comply. At the micro level, scattered non-compliance may not have an impact. However, at the macro enterprise level, non-compliance may have far-reaching effect. The Lowest Price, Technically Acceptable (LPTA)[4] approach, while effective when requirements are clearly defined, has surfaced unintended consequences over the years. Contractors are forced to make decisions based on price regardless of the potential quality of work, compelled to offer a lower price solution that might not be in the best interest of the government, and afforded no room to deliver value-added solutions. The Federal Acquisition Regulation provides for best value continuum and a tradeoff process.[5]

- **Personnel.** A strategic view of staffing must consider the pendulum swing and logical consequences after a solution is in place. For example, the Air Force recruited/cross-trained a high number of prior service personnel to fill contracting/acquisition gaps and are now facing a shortage with retirement with that solution. This skills gap was highlighted in 2011 and recently stressed by OPM[6] – cybersecurity and contracting were two of the six mission-critical skill areas identified. A systemic adjustment to the Personnel structure is needed.

  Whereas hiring/firing is less cumbersome in the private sector, the general federal challenge is the lengthy process to advertise a position, gather a list of potential applicants, interview and hire. The security clearance process, especially for hiring cyber professionals, can be monumental. For example, DHS has yet to unravel its Entry on Duty process. At the other end of the spectrum, dismissal of a non-performer is a monumental task equaled only by the amount of paperwork involved. Managers complain of the time taken away from the operational mission to deal with administrative issues. What is needed is an end-to-end process owner who can drive efficiency through barrier removal and sub-process owner accountability.

- **Improve requirements definition process.** There is a disconnect between operational owners and the contracting community. As in the previous AMIC example, awareness and interaction across operators, engineers, program management, acquisition and contracting and industry would greatly improve elements of the procurement lifecycle. Providing appropriate acquisition training for those functional area experts responsible to define requirements would be helpful so that a draft RFP for Industry review does not

[3] http://www.strategyex.com/resources/knowledge-center/case-studies/usaf-air-combat-command

[4] http://www.informationweek.com/government/leadership/lpta-contracts-stifle-government-innovation/d/d-id/1112071

[5] FAR 15.101 Best Value Continuum ; FAR 15.101-1 Tradeoff Process; FAR.101-2 Lowest Price Technically Acceptable Source Selection Process

[6] http://www.govexec.com/management/2016/04/opm-agencies-figure-out-how-close-skills-gap-federal-workforce/127580/?oref=govexec_today_nl

result in delay or modifications. Amending RFPs adds time and risk to successful proposals.[7]

A Request for Information (RFI) oftentimes is used to validate a government assumption. While RFIs indicate that an RFP is not necessarily forthcoming, some Industry partners wait for a draft Request for Proposal before expending resources. Perhaps a better way to expedite cyber procurement is via "proof of concept" and allow the government to deploy needed cyber tools quickly while agreeing to a contracting annuity clause in compliance with the FAR. This model would pay the vendor over a specific time to include reasonable interest.

- **Streamline Cyber Request for Proposal** creation and solicitation timeline. If the requirements definition is solid, and government /industry collaboration exists, then certainly an abbreviated RFP process limited to five pages with a two-week turnaround is possible for urgent cyber services and products. Another consideration is to use oral presentations and display of solution to a qualified team of cyber professionals and requirement owners.

- **Redirect cyber resources and establish accountability**. For years cyber professionals have lamented that security should be addressed in the design phase not "bolted on after production." The focus is not on the lifecycle, most likely because of the upfront cost and the race to market. However, considering the amount of funding directed to a "fix" for a small portion of the overall cyber security problems, the original issue falls by the wayside. Inadequate cyber security at the onset persists throughout the lifecycle. Cybersecurity is as critical an issue as vehicle crash testing or building code regulations. Request the Government Accountability Office a**nalyze the lifecycle savings for the total cost of ownership reduction.**

- Adjust **risk management thinking** to include good stewardship. In general, public and private organizations should act as responsible stewards of the assets they control. Their risk management outlook should include a belief they have the duty to national and economic interests. The International Organization for Standardization (ISO) 20121 - Event Sustainability Management System-Requirements with Guidance for Use - states in paragraph 3.20 that "responsibility for sustainable development shared by all those whose actions affect environmental performance, economic activity, and social progress, reflected as both a value and a practice by individuals, organizations, communities, and competent authorities." More simply, cybersecurity is everyone's business.

  Government and Industry cannot wait for a publicized breach to act. The seriousness of the cyber threat does not diminish in time, it grows. The national and economic security relies on a concerted effort by the public/private communities.

  - The recent thrust for technology innovation via Silicon Valley engagements by Department of Defense (DoD) and DHS, and General Services Administration's (GSA) attempt to simplify the contracting process for start-up companies by *FASt Lane* or *Startup Springboard* do not take into account the need for trusted,

[7] Contracting Officers should have the authority to mod contracts as changes in cyber policy and mandates arise. This will support better services and products when an awarded contract is in the later years but still adhering to outdated references and guidance.

certified secure IT elements and supply chain validation. If consideration is not given to a rigorous assessment of secure cyber elements, perpetual vulnerabilities will continue to plague U.S. IT systems.

Enforce the common criteria for information technology. The National Institute of Standards and Technology (NIST) and the National Security Agency's National Infrastructure Assurance Partnership (NIAP) oversaw Common Criteria implementation. Products that passed are certified that they will do exactly what the vendor says. While certification via Common Criteria Testing Laboratories (CCTL) does not guarantee security, it does validate vendor claims of security attributes by an independent third party. Some type of test and evaluation should provide for software assurance.

The Washington Cyber Roundtable is pleased to have had the opportunity to provide additional information to Congresswoman Comstock and her staff regarding cybersecurity acquisition reform. We hope to work together on other issues in the future.

About the Washington Cyber Roundtable

The Washington Cyber Roundtable is a non-profit, 501(c)(6) organization representing a cross-section of leading technology, consulting, and professional services firms. An independent, executive-level body, WCR provides a collaborative venue for business and government leaders to constructively address the policy, technology, and management issues affecting the cybersecurity of private companies and government agencies.

For more information, please contact:

Barbara George, PhD
Executive Director
barbara.george@washingtoncyber.org

Kaitlin Bulavinetz
Director of Operations
bulavinetz@washingtoncyber.org