Improving Cybersecurity and Resilience Through Acquisition

Briefing for OFPP Working Group
19 Feb 2015

Emile Monette
GSA Office of Governmentwide Policy
emile.monette@gsa.gov

Cybersecurity Threats are Sometimes Enabled by Federal Acquisition Practices

- When the government purchases products, services, or solutions from sellers with inadequate integrity, security, resilience, and quality in their deliverables or operations, the risks created for the government persist throughout the lifespan of the item purchased (or until they're fixed) and often result in increased costs to the government and contractors.
  - Cybersecurity risks are present in all purchased products, services, or solutions that connect in any way to a government information system and/or which contain, transmit, or process information provided by or generated for the government to support the operations and assets of a Federal agency.
- Federal buyers need better visibility into, and understanding of, how the products, services, and solutions they buy are developed, integrated and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of those products and services.
  - This visibility should extend through all companies directly involved in delivery of products, services, and solutions to the government, and through all tiers of the supply chain.

Executive Order 13636 Section 8(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."

- Interpretation:
  - Not limited to critical infrastructure
  - Scope is all acquisition planning, contract administration, and procurement requirements

EO13636 Section 8(e) Report

- The Final Report, "*Improving Cybersecurity and Resilience through Acquisition*," was publicly released January 23, 2014: (http://gsa.gov/portal/content/176547)

- Recommends six acquisition reforms:
  I. Institute Baseline Cybersecurity Requirements as a Condition of Contract Award for Appropriate Acquisitions
  II. Address Cybersecurity in Relevant Training
  III. Develop Common Cybersecurity Definitions for Federal Acquisitions
  IV. Institute a Federal Acquisition Cyber Risk Management Strategy
  V. Include a Requirement to Purchase from Original Equipment Manufacturers, Their Authorized Resellers, or Other "Trusted" Sources, Whenever Available, in Appropriate Acquisitions
  VI. Increase Government Accountability for Cyber Risk Management

"Ultimate goal of the recommendations is to strengthen the federal government's cybersecurity by improving management of the people, processes, and technology affected by the Federal Acquisition System"

Recommendation Implementation

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

- Strong passwords, multi-factor login, anti-virus,…
- Cybersecurity Framework Profile?
- Matched to Controlled Unclassified Information (CUI) rules?
- CUI – rulemaking in process
  - …anticipates establishing a single Federal Acquisitions Regulation (FAR) clause that will apply the requirements of the proposed rule to the contractor environment…
- OMB contract clauses working group (CAO + CIO Councils)
  - OFPP received 70 responses to the Request for Cyber/Information Security Clauses & Materials (Dec 10, 2014).
  - The spreadsheet of submissions is posted on the Cybersecurity Contracting Best Practice Submission MAX page.
  - OFPP is forming a joint CIOC/CAOC contracting clauses working group to review materials and make recommendations.
  - *Also relevant for Cybersecurity Risk Management Strategy (Rec IV)

Recommendation Implementation (cont.)

II. Address Cybersecurity in Relevant Training
- Dec 2014 - focus group meeting at the Homeland Security Acquisition Institute (HSAI) consisting of acquisition personnel from the DHS components to discuss the cyber training needs of the field.
- Preliminary report was generated based on the feedback received.

III. Develop Common Cybersecurity Definitions for Federal Acquisitions
- Federal Register Notice to be published soliciting greater participation

IV. Institute a Federal Acquisition Cyber Risk Management Strategy
- Focus on mission priority and criticality of item being purchased
- Common way to assess risk of item being purchased – includes deployed environment, hardware, software, service provision, and supply chain
- Request for Information closed 16 Feb 2015
  - https://www.fbo.gov/notices/230732591f542b7da9b9fc3e6c167eec

Recommendation Implementation (cont.)

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

- Five sub-groups:
  - Industry Best Practices for Indicating Authorized Partners & Resellers
  - Industry Best Practices for establishing and maintaining Trusted Suppliers
  - Definitions, Parameters, and Boundaries
  - Revise, Update, and Adapt Current Policy Provisions
  - Waiver / Exception Provision

VI. Increase Government Accountability for Cyber Risk Management

- Analogy to legal review – throughout Acquisition process
- Certification of (1) understanding of risk, and (2) management satisfies risk tolerance

Implementation Working Group leads

1. Institute Baseline Cybersecurity Requirements as a Condition of Contract Award for Appropriate Acquisitions
   - **Don Davidson, OSD/OCIO donald.r.davidson4.civ@mail.mil**
2. Address Cybersecurity in Relevant Training
   - **Andre Wilkins, DHS/HSAI andre.wilkins@hq.dhs.gov**
3. Develop Common Cybersecurity Definitions for Federal Acquisitions
   - **Jon Boyens, NIST jon.boyens@nist.gov**
4. Institute a Federal Acquisition Cyber Risk Management Strategy
   - **Joyce Corell, ODNI**
5. Include a Requirement to Purchase from Original Equipment Manufacturers, Their Authorized Resellers, or Other "Trusted" Sources, Whenever Available, in Appropriate Acquisitions
   - **Emile Monette, GSA/OGP emile.monette@gsa.gov**
6. Increase Government Accountability for Cyber Risk Management
   - **Joe Jarzombek, DHS/NPPD/CS&C Joe.Jarzombek@hq.dhs.gov**

- Working Groups will continue stakeholder-centric process
  - Business Due Diligence Request for Information (https://www.fbo.gov/notices/230732591f542b7da9b9fc3e6c167eec)
- Spring 2015 Software and Supply Chain Assurance Forum

BUSINESS DUE DILIGENCE INFORMATION

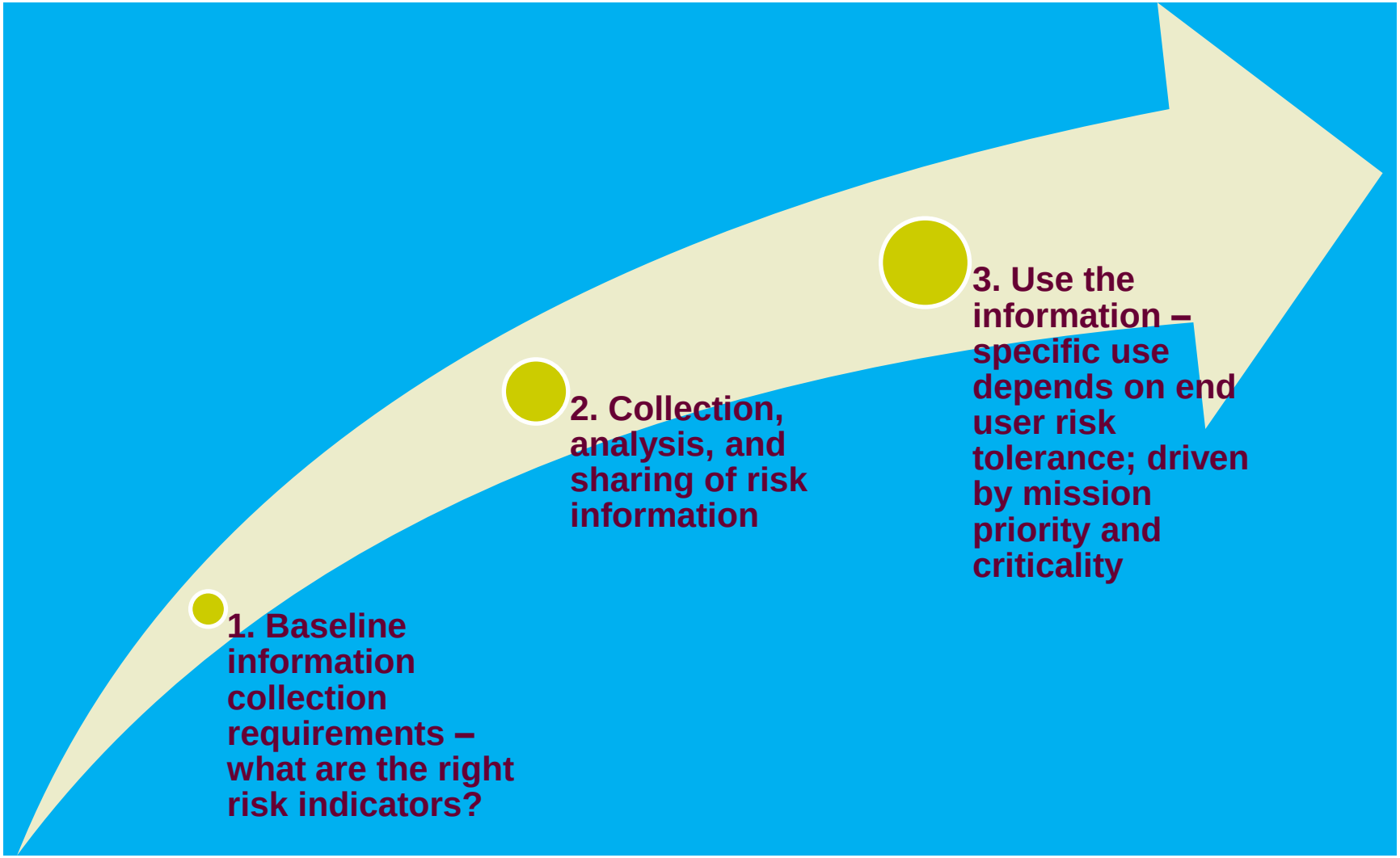
Why is GSA interested in Business Due Diligence Information?

- GSA's Mission: *Deliver the best value in real estate, acquisition, and technology services to government and the American people.*
- GSA's #1 Priority: *Delivering Better Value and Savings. By using the purchasing power of the federal government, we will drive down prices, deliver better value, and reduce costs to our customer agencies. As a result, these agencies can focus their resources and attention on their core missions.*
- Customer Demand:
  - DoD, DOE, "Commerce, Justice, and Science" agencies, and others have statutory and mission-related requirements for supply chain risk management;
  - Other D/As recognize the threats and vulnerabilities inherent to the global supply chain (e.g., SSA, GSA) and seek greater confidence in deliverables and suppliers.

Business Due Diligence Pilot

- GSA is collaborating with its customer agencies and other stakeholders to establish a common set of risk indicators and risk research methodologies that can be used as the baseline for business due diligence research.
- Six-month pilot project to conduct open-source-based “business due diligence” risk research about GSA contractors.
- Risk information being used by GSA to:
  - Engage contractors and collaboratively generate performance improvements; and
  - Inform the development of requirements for initial operating capability.
- Open source business due diligence information will better inform customer agency risk decisions and provide greater confidence in contractors and deliverables
- Request for Information closes 16 Feb 2015
  - https://www.fbo.gov/notices/230732591f542b7da9b9fc3e6c167eec

Three Step Process….



Authority to use Business Due Diligence Information in Acquisitions

- FAR 9.103 - - Policy

  ****

  - (c) The award of a contract to a supplier based on lowest evaluated price alone can be false economy if there is subsequent default, late deliveries, or other unsatisfactory performance resulting in additional contractual or administrative costs. While it is important that Government purchases be made at the lowest price, this does not require an award to a supplier solely because that supplier submits the lowest offer.

- FAR 9.104-2 -- Special Standards
  - (a) When it is necessary for a particular acquisition or class of acquisitions, the contracting officer shall develop, with the assistance of appropriate specialists, special standards of responsibility. Special standards may be particularly desirable when experience has demonstrated that unusual expertise or specialized facilities are needed for adequate contract performance.

Authority to use Business Due Diligence Information in Acquisitions (cont.)

- FAR 9.105-1 -- Obtaining Information.
  - (a) Before making a determination of responsibility, the contracting officer shall possess or obtain information sufficient to be satisfied that a prospective contractor currently meets the applicable standards…

    ****
  - (c) In making the determination of responsibility, the contracting officer shall consider…

    ******
    - (3) Commercial sources of supplier information of a type offered to buyers in the private sector.

Authority to use Business Due Diligence Information in Acquisitions (cont.)

- OFPP Memo: "*Making Better Use of Contractor Performance Information*" July 10, 2014
  - "[T]here is an increased risk of problems on high risk programs, major acquisitions, or other complex contract actions that are critical to an agency's mission. To address this risk and ensure we make awards to contractors with good performance records, as well as to encourage the use of new and innovative companies with little or no Federal experience, agencies are directed to undertake additional outreach and research to make more informed decisions."
  - "Broadening the Sources of Performance Information - The FAR allows the Government to consider information from additional sources of information beyond the Past Performance Information Retrieval System (PPIRS), including information found from conducting this additional research and outreach."