

IMPROVING CYBERSECURITY RISK MANAGEMENT IN FEDERAL ACQUISITION

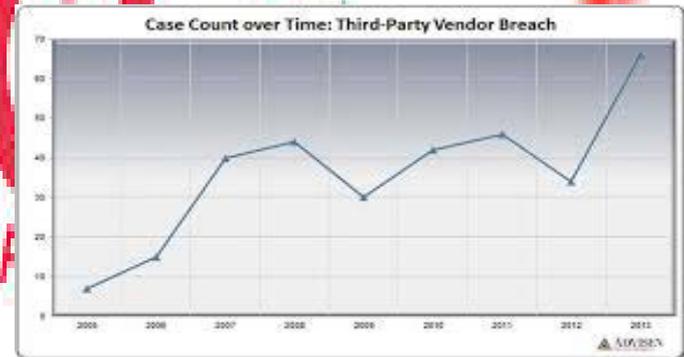
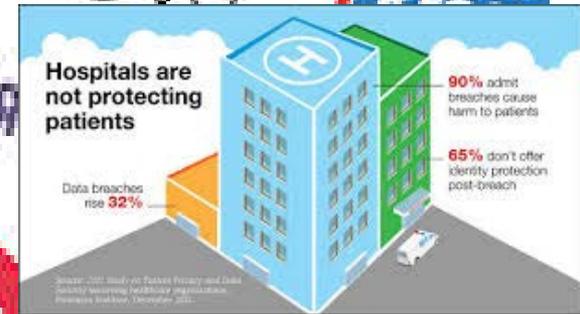
Briefing for Federal Advisory Committee on Insurance (FACI)
4 November 2015

Emile Monette
Director
Government-wide Cyber Security, Resilience, and Risk
GSA Office of Government-wide Policy
emile.monette@gsa.gov

Buyer Choices Affect Risk...

When a buyer purchases things from a seller with inadequate security built into its operations and deliverables (including its supply chains), bad things happen....

....and it harms us all.





ICT Supply Chain Risk

Threats

Adversarial: e.g. insertion of counterfeits, tampering, theft, and insertion of malicious software.

Non-adversarial: e.g. natural disaster, poor quality products/services and poor practices (engineering, manufacturing, acquisition, management, etc).

Vulnerabilities

External: e.g. weaknesses in the supply chain, weaknesses within entities in the supply chain, dependencies (power, comms, etc.)

Internal: e.g. information systems and components, organizational policy/processes (governance, procedures, etc.)

Likelihood (probability of a threat exploiting a vulnerability(s))

Adversarial: capability and intent

Non-adversarial: occurrence based on statistics/history

Impact - degree of harm

To: mission/business function

From: data loss, modification or exfiltration

From: unanticipated failures or loss of system availability

From: reduced availability of components

Risk

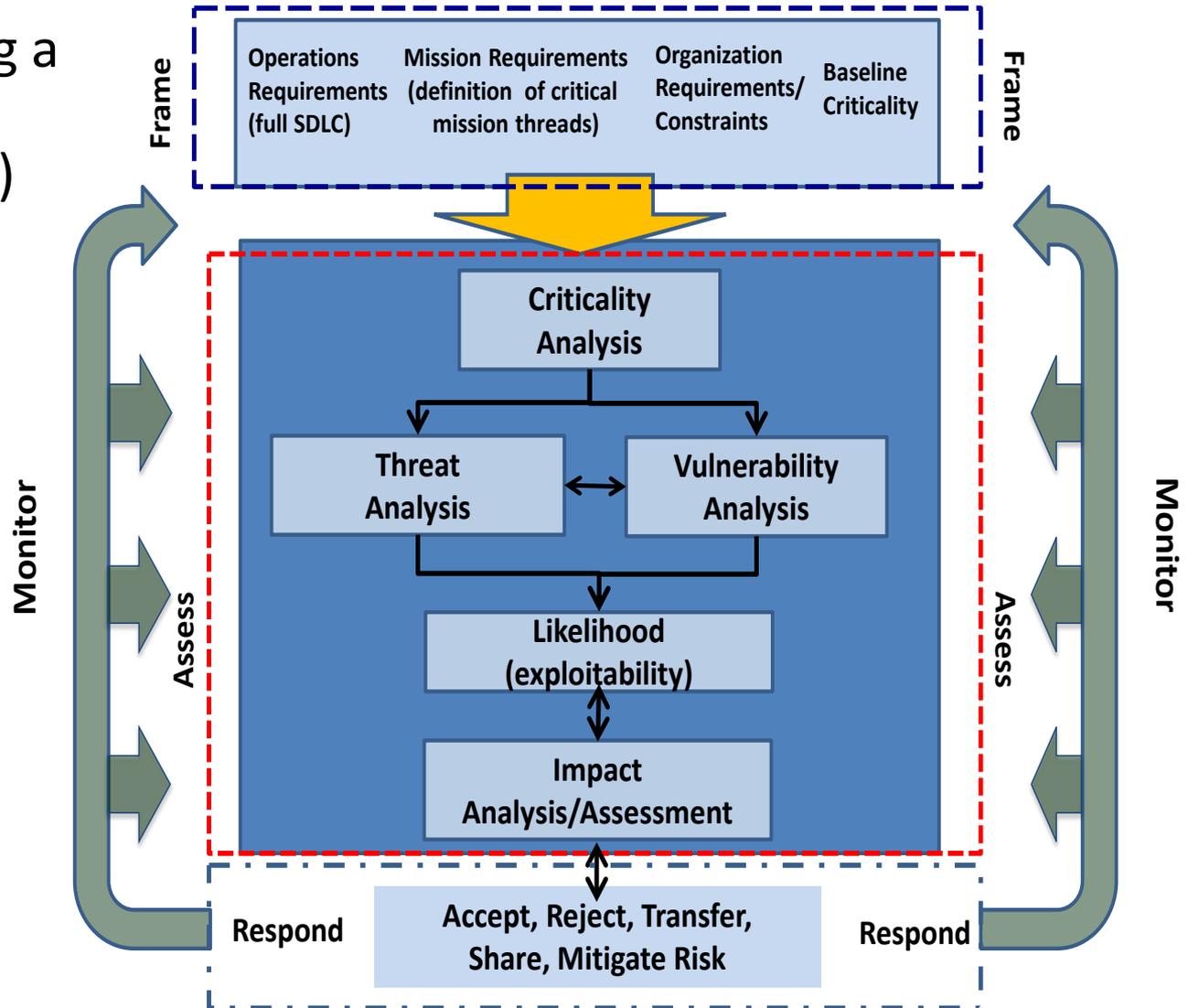
Applying the NIST Risk Management Framework

Frame: outsourcing a mission function (buying something)

Assess: ???

Respond: requirements, solicitation, and contract

Monitor: contract performance requirements



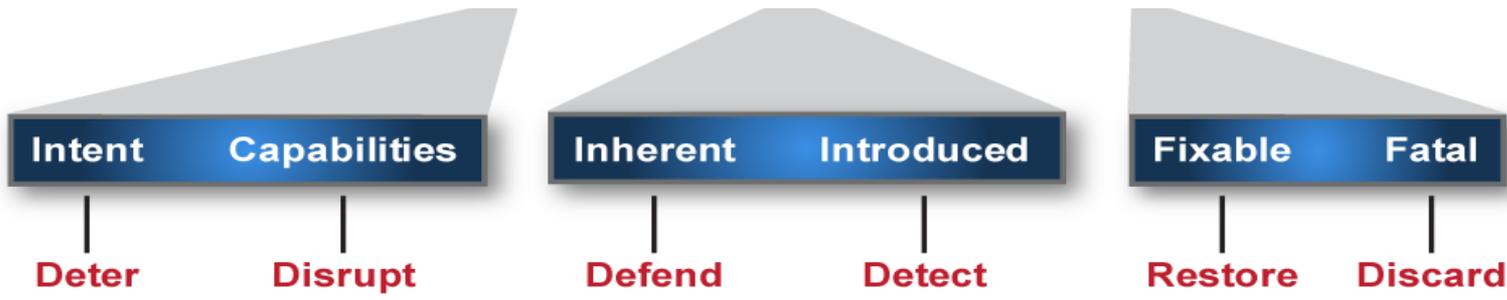


Assessing Risk

Risk = f (cost, schedule, performance)

Security Integrity

Risk = f (threat, vulnerability, consequence)



Defense Science Board Report *Resilient Military Systems and the Advanced Cyber Threat* Feb 2013

Supply Chain Life Cycle

Concept Design Manufacture Integration Deployment Maintenance Retirement

...which is driving buyers to seek more detailed risk information about business partners.



- Buyers need information about *all* sellers and *all tiers* of the seller's supply chain (*but maybe not all the time*):
 - ✓ How the goods and services they buy are developed, integrated and deployed; and
 - ✓ How sellers assure the integrity, security, resilience, and quality of those goods and services.



Things Are Not Always What They Seem...

Observable behavior of Multinational Firm	Nefarious Intent ... ?	... or Business as Usual?
Tries to purchase US firms, create joint ventures	Seeking intellectual property for hostile activities	Secure market share, distribution, and access to technology and IP
Conduct business intelligence on competition	Acts as agents for foreign government	Plans and intentions of rivals; limitations of competing products
Access to systems or networks after equipment or software install	Foreign government access for collection and exploitation	Retain access to customer systems for service, maintenance, and license compliance monitoring
Fills key overseas positions with individuals of specific nationality	Vetted trusted insiders can facilitate intelligence activities	Executives with strong ties to firm to protect IP and business interests
Uses financial structure that is complex with limited transparency	Conceals financials to appear independent and fiscally sound	Global variation in taxes incentivize complex financial structures; privately held firms limit details
Seeks contracts to supply US government	Firm may be trying to supply subverted products	US government is a large customer of products and services

Cybersecurity in Acquisition

- February, 2013, 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.

- Applicable to all acquisition planning, contract administration, and procurement activities.
- “What can we do in the Federal Acquisition System to improve cybersecurity outcomes?”

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”

2015 OMB Memo: "*Improving Cybersecurity Protections in Federal Acquisitions*"

- Draft memorandum published at <https://policy.cio.gov>
- Premise: Cybersecurity protections in Federal acquisitions can be further enhanced by performing increased “business due diligence.”
 - GSA shall provide agencies with risk information that encompasses data collected from voluntary contractor reporting, public records, publicly available and commercial subscription data, based on transparent, objective, and measurable risk indicators.
 - Within 90 days, GSA to identify risk indicators and other core requirements for the shared service.

WHAT IS BUSINESS DUE DILIGENCE?

- Central government-wide service/solution that enables agencies to perform substantially improved “business due diligence” for ICT acquisitions.
- Provides capability to research, collect, assess, and share risk indicator data about a particular vendor, product, and/or service
- The BDDIS will store, maintain, and provide access to a central (government-wide) repository of risk information

HOW WILL IT WORK?

1. BUYER:

- Risk Tolerance – relative to importance of Risk Categories
- Seller and Deliverable

2. SELLER (VOLUNTARY):

- Information about the Seller related to Risk Categories
- From the Seller

3. "BIG DATA:"

- Information about the Seller related to Risk Categories
- From "Big Data"

FUNCTIONS & OUTPUTS

DATA & INFORMATION INPUTS

Initial Automated Risk Score

- Dashboard view
- Comparison of Seller and "Big Data" inputs to Buyer's Risk Tolerance

Aggregate Multiple Data Sources

- Data supporting risk score
- Authoritative and secondary source information

Perform Analytics

- Compare Seller inputs with "Big Data" inputs
- Identify correlations

Conduct In-depth Investigations (as needed)

- On-site inspections
- Process reviews
- Personnel interviews

DRIVERS & INFLUENCES – **CYBERSECURITY IS URGENT PRIORITY**

- Administration & Congressional **Priority** – e.g., Cyber CAP Goal, New Cyber Laws, Cybersprint, PPD-21; EO 13636
- High-profile **Breaches** & Ever-increasing **Threat**
Need to **Improve** Cyber Protections in **Acquisitions**
- **Inadequate Access** to Due Diligence Data
- **Risk Management** Framework
- Private Sector & Insurance Industry - **Alignment** of Need & Approach

STAKEHOLDER & CUSTOMER OUTREACH – CONFIRMATION OF N

- Issued **RFI** – received + 30 Responses
- Extensive **Outreach & Engagement**: Qtly Software & Supply Chain Assurance Forum; RSA Conference; Open Group Forum; Defense Science Board Brief; Exostar; Cybersecurity Law Institute & Agencies (TSA, DoD ATL; State, Treasury, DHS, FBI, SSA, DoE, NASA, DNI + others)
- **Federal Register** Notice and Comments
- Interact & GSA.gov **web content**

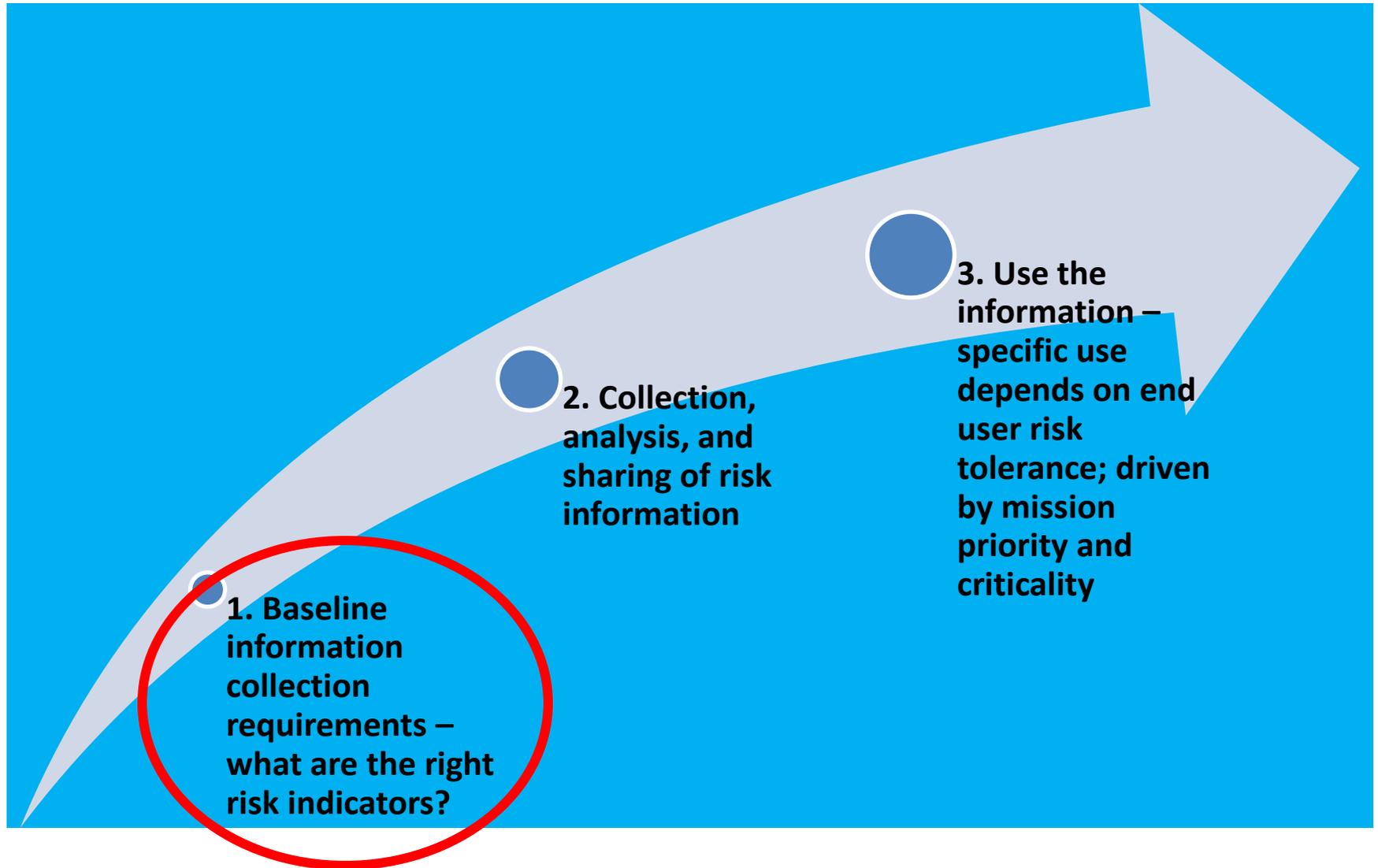
Due Diligence in Federal Acquisition

GSA piloting commercial “due diligence” service during fiscal 2016

- Results from 1st 60 companies assessed:
 - 45% of contractors more risky than buyers said they could tolerate
 - Top Overall Risks: Regional Stability (78%), Cybersecurity (52%), and Company Leadership (52%)
 - Highest Risk: Technology companies (or their value-added resellers)
 - Lowest risk: Accreditation bodies and access control companies
- Increased use of business due diligence information will improve agency risk decisions and enable greater confidence in contractors and deliverables.

“Vendor risk assessment is a smoke detector, not a fire detector.”

Three Steps to Implementation



Questions?

Comments?

Concerns?