SSCA Summer Working Groups 2015

Public Meeting:

Using Business Due Diligence Information in Acquisition Planning and Contract Administration

Public Meeting Agenda*

- 1130-1200 Problem, Purpose and Scope of RFI
- 1200-1230 Registered Public Speaker Comments
- 1230-1330 Lunch Break
- 1330-1415 RFI Responses and Analysis
- 1415-1500 Proposed Solution and Next Steps

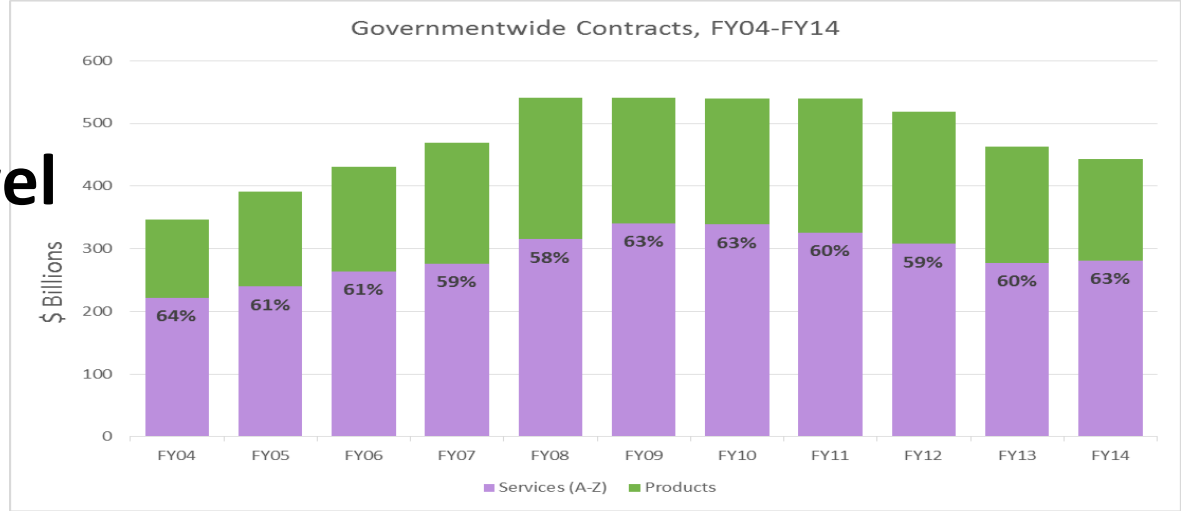
***Modified Chatham House Rules for Public Meeting:** GSA and Registered Public Speakers are providing comments for the record. Other audience participants retain non-attribution unless otherwise requested/stated.*

Buyer Choices Affect Security…

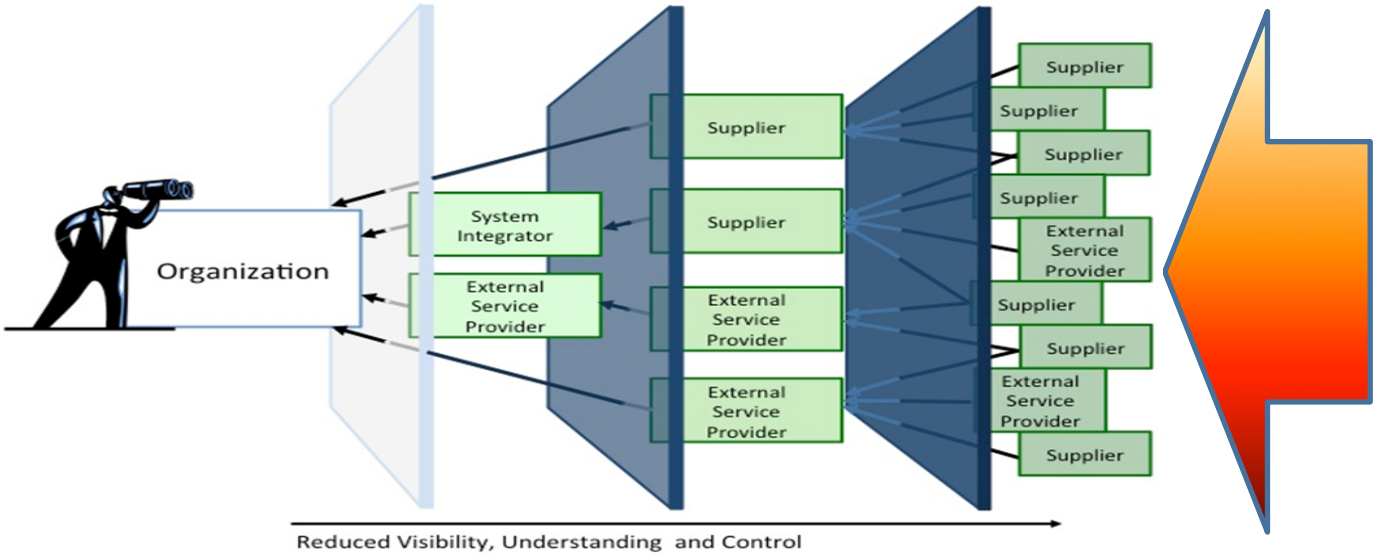
When a buyer purchases things from a seller with inadequate security in its operations or deliverables (including its supply chains), bad things happen….

….and it harms us all.

The global supply chain and a high level of reliance on services…



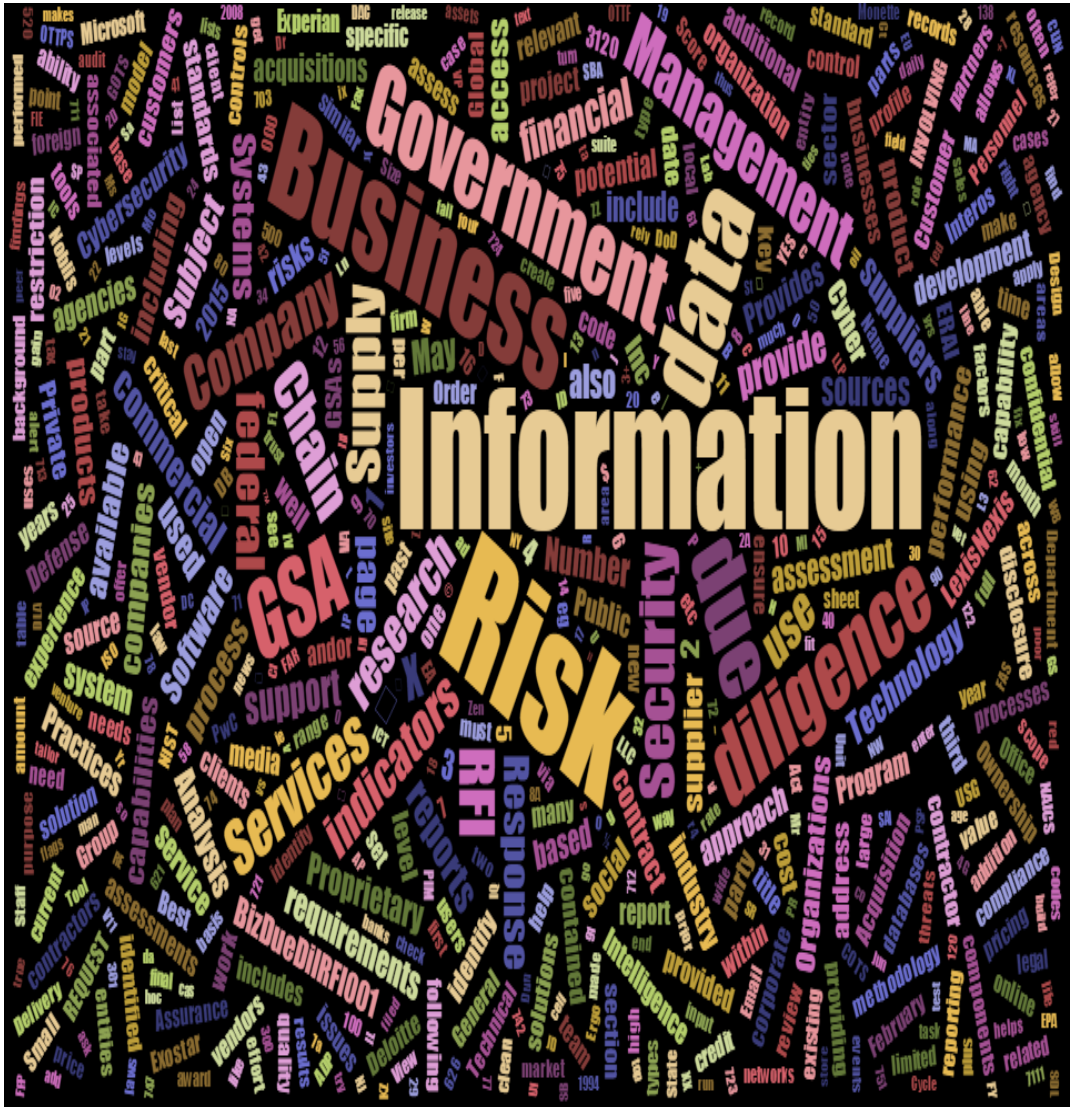
…results in lack of visibility for buyers/end users…



…and leads to risk decisions being made by people who do not own the risk or consult the risk owner.

…which is driving the need for more information about business partners.

- Better understanding of risks leads to better informed decisions.
- Information needed about Prime contractors and all tiers of the supply chain.


Information
Risk
Business
Government
Management
data
due
diligence
GSA
Supply
Chain
Company
Systems
Services
Security
Technology
Proprietary
requirements
indicators
research
RFI
Response
Subject
Cybersecurity
Microsoft
Experian
acquisitions
financial
assessment
Organizations
Program
Intelligence
Software
Analysis
Capabilities
Practices
Assurance
Exostar
Deloitte
BizDueDilRFI001
LexisNexis
Technology
Ownership
Acquisition
Contractor
Compliance
Pricing
Methodology
Reporting
Components
Online
Related
Legal
Cycle
Limited
February
Methodology
Databases
Threats
Provided
Within
Corporate
Review
Existing
Networks
Credit
State
Section
Contained
Solutions
Social
Contract
Report
Industry
Approach
Cost
Time
Party
Address
Value
Usg
Third
Processes
Year
Scope
Red
Naics
Codes
Hard
Time
Legal
Online
Pricing
Compliance
Components
Reporting
Helps
Related
Cycle
Limited
February
Methodology
Threats
Databases
Acquisition
Contractor
Ownership
Online
Processes
Third
Usg
Value
Address
Organizations
Program
Technology
Lexisnexis
Disclosure
Across
Confidential
Development
Interos
Customer
Personnel
Cases
Agency
Partners
Allows
Involving
Businesses
Product
Suppliers
Sources
Provide
Provides
Cyber
Key
Performance
Using
Capabilities
Time
Department
Allow
Boston
Areas
Years
Experience
Source
System
Software
Process
Support
Media
Clients
Capabilities
Analysis
Service
Assessments
Identified
Contractors
Current
Small
Delivery
Request
Entities
Price
Best
Group
Solution
Need
Needs
Amount
Purpose
Table
Uses
Defense
Available
Commercial
Companies
Used
Open
Vendor
Critical
Products
Private
Background
Restriction
Agencies
Including
Standards
Customers
Controls
Model
Associated
Ability
Tools
Foreign
Point
Audit
Assess
Access
Global
Similar
Relevant
Project
Standard
Control
Records
Additional
Organization
Score
Case
Date
Sector
Profile
Field
Suite
Local
Tool
Levels
Findings
Performed
Makes
Release
Specific
Order
Number
Public
Sheet
Supplier
Approach
Party
Within
Provided
Industry
Report
Contract
Social
Contained
Solutions
Section
Intelligence
Requirements
Proprietary
Level
Reports
Technical
General
Following
Identify
Users
Check
Help
Team
Market
Clean
Issues
Results
Quality
Effort
Award
Vendors
Work
Includes
Identified
Assurance
Exostar
Deloitte

Executive Order 13636 Section 8(e) – Feb. 2013

- *"Secretary of Defense and the Administrator of General Services, shall make recommendations to the President, 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

- 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

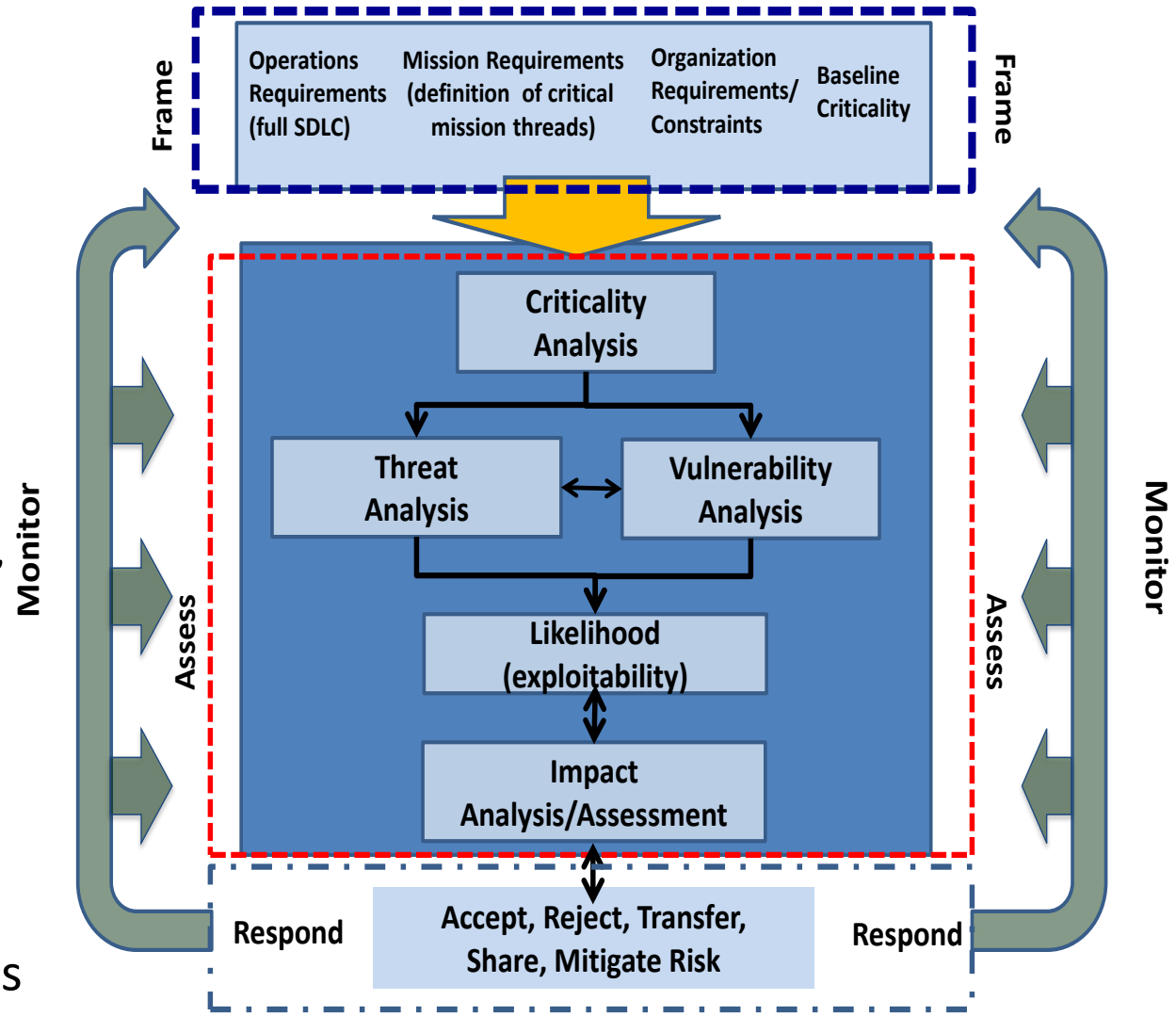
NIST Special Publication 800-39: Managing Information Security Risk

Frame: Outsourcing a Mission Requirement

Assess: ???

Respond: Technical Requirements, Solicitation Provisions, Contract Terms & Conditions

Monitor: Contract Performance Requirements & Audits



Purpose of the Business Due Diligence RFI

GSA is collaborating with stakeholders to establish a common set of risk indicators/categories that can be used by all Agencies to support government risk assessments.

- It is anticipated the business due diligence information obtained will be used by the Federal acquisition, grant, and oversight communities to support various government activities related to risk management.

- Selection of which contractors to assess will continue to be a risk-based decision made at the discretion of an agency.

Three Main Questions Presented in the RFI

1. What are the current industry best practices for conducting Supplier Risk Assessments?
2. What additional information and approach should the Government use?
3. What Solution Providers exist?

Received 28 Responses from multiple perspectives:

Independent Auditors, Consulting, Niche Provider, Big Data Aggregators, IT Product Vendors, Universities, Industry Consortium

Registered Public Speakers

1. Jennifer Bisceglie, Interos
2. Sally Long, The Open Group
3. Art Spring, Experian
4. Christopher Simkins , Chainsec

Not necessary in order of speaking line up.

All written comments submitted on June 2nd will be available to the public on regulations.gov on June 8, 2015. Search for "*meetings me-2015-01*".

Information Provides a Basis for Risk Assessment

Current Sources

- Dun & Bradstreet
  - Adequate Financial resources to preform contract
- Past Performance Information Retrieval System (PPIRS)
  - Document contractor and grantee performance information
- Federal Awardee Performance and Integrity Information System (FAPIIS)
  - Administrative Agreement
  - Defective Pricing
  - DoD Determination of Contractor Fault
  - Non-Responsibility Determination
  - Recipient Not-Qualified Determination
  - Termination for Cause
  - Termination for Default
  - Termination for Material Failure to Comply
- Suspended and Debarred Parties (EPLS/SAM)
- Small Business Administration (SBA) Certificate of Competency
  - Business demonstrates the ability to perform

FAR Requirements

- Organization's financial strength, including access to and sources of funding (see, FAR 9.104-1(a));
- Existing commercial and government clients/ customers (see, FAR 9.104-1(b));
- Record of integrity and business ethics, including but not limited to legal and regulatory issues in any nations where the company does business (see, FAR 9.104-1(d), 9.104-1(g), 9.104-6, and 9.4);
- Organizational, accounting and operational controls, and technical skills, (including, but not limited to, as appropriate, such elements as financial systems, purchasing systems, production control procedures, property control systems, quality assurance measures, safety programs, and insider threat programs) (see, FAR 9.104-1(e)); and
- Production, construction, and technical equipment and facilities (see, FAR 9.104-1(f)).

Q 1: What are the current industry best practices for conducting Supplier Risk Assessments?

- **Seller Business Practices**
  - Intellectual Property Protection Policy And Practices
  - Ensure Competitiveness/Monitor Competitor Practices
  - Require Business Ethics Program/Pledge/Code of Conduct
  - Cyber Hygiene And Threat Awareness
  - Compliance System That Includes Quality And Legal Requirements
  - Defect Management Process (Patches, etc)
- **Buyer Driven Seller Practices**
  - Compliance requirements
  - Code of Conduct requirements
  - Independent 3rd Party Assessments and Certifications
- **Buyer Risk Assessment Approaches**
  - Tiered Risk-based Approach
    - Prioritization of suppliers/product/service by the criticality of the Seller (i.e. volume of purchasing, limited number of alternative suppliers, criticality of product/service)
  - Framework That Includes A Repeatable Quantitative Scoring Methodology
  - Multiple Sources And Types Of Data
  - Automation Of Workflow
  - Risk Categories Correlated To Demonstrated Performance

Q2: WHAT ADDITIONAL INFORMATION AND APPROACH SHOULD THE GOVERNMENT USE?

General Comments (1 of 2)

- **Suggest [using] recognized certifications** (Capability Maturity Model Integration (CMMI) and International Organization of Standards (ISO)) [and] **review by a sanctioned third party** to substantiate company claims.
- **Do not think that the GSA will find significantly responsive information from public sources to adequately address cyber security risk**." Each of these five factors [6.1.1-6.1.5] are important for understanding if a vendor is acceptable … but provide little insight into the cybersecurity risk of information system purchases. **The risk indicators listed in the RFI could correctly identify business risk in federal acquisition, as long as they are verified.**
- Government must **consider the viability of organizations, especially small and medium size**, that possess the maturity to understand how to evaluate these risk factors and **justify investment in remediation.**
- Advocate for the **use of open standards and accreditation programs as the most effective way to determine trustworthiness**. Need to have a common understanding of both **factors that (taken together) contribute to risk and relationship between those factors.**

General Comments (2 of 2)

- The ability to look at historical commercial data on identities [is good], as disbarred companies will change identity in order to continue to do business - referred to as "cage hoppers".
- Indicators are mostly correct, but a **framework is needed** to assess the risk and [ensure] consistent analysis.
- [Approach] more broadly about how **to create efficiencies and increase coordination among Fed agencies**; suggest leveraging existing Gov't policies to simplify due diligence research
- More **detail is needed regarding how GSA will use these risk indicators**
- Consider the importance of suppliers' **openness and transparency with their customers**
- Important to provide for robust third-party due diligence; Take a **risk-based tiered approach**
- Advocate for **tailoring risk criteria/assessment to align to different organizations' trust level requirements**
- **Continuous due diligence workflow**; encompass both pre- and post-award

Responses to Information Used (6.1.1 &6.1.2)

6.1.1. Financial strength (access to and sources of funding)

- As this due diligence effort focuses on IT systems, multiple aspects of cyber risk should be emphasized and expanded. For example, the **cyber threat landscape should be considered** and included as part of a standard risk assessment.
- Key payment performance metrics, trade balances, and legal findings + **credit scores, and financial stability scores**
- **Predictive and descriptive components** to deliver a reliable assessment of a company's future viability

6.1.2. Existing commercial and government clients/customers

- Historical business relationships to include successful or unsuccessful business dealings with the Gov't [good].

Responses to Information Used (6.1.3)

6.1.3. Record of integrity and business ethics (legal and regulatory issues in any nations where the company does business)

- **Integrity and business ethics are poor indicators, as they are extremely subjective**. However, legal and regulatory issues are exceptional indicators of supply chain risks. Typically, legal and regulatory punishments are dispensed punitively, which also poses financial risk.
- Original bankruptcies; tax liens and judgments + "fraud scores"
- [Companies should] attest that employees complete **Code of Conduct** Training.
- Legal and regulatory issues are exceptional indicators of supply chain risks
- Include a review of **global sanctions and watch lists** for any derogatory information that may be associated with a contractor

Responses to Information Used (6.1.4 & 6.1.5)

6.1.4. Accounting and operational controls, and technical skills, (financial systems, purchasing systems, production control procedures, property control systems, quality assurance measures, safety programs, and insider threat programs)

- Operational controls, which can include the design and production of products as well as quality control
- Family tree - account linkage which is the relationship between different companies within corporate family

6.1.5. Production, construction, and technical equipment and facilities

- May be important if the subject of the contract is designed, produced, etc. on networks that have a cybersecurity risk
- Location information important: goods designed, manufactured, and distributed abroad pose a potential **foreign ownership control and influence risk as well as resiliency risk** due to regional instability or natural disasters

Responses to Information Used (6.2.1)

6.2.1. Company leadership, personnel associations

- Failed to see how company leadership can relate to cybersecurity issues(?)
- One option to consider is to **conduct cyber audits**, similar in nature to those audits conducted by DCAA and DCMA (often as pre-award criteria) to assess the viability of companies to perform contracts and effectively administer contracts, conflict of interests, previous debarment and negative judgments, liens and other derogatory findings
- Organization structure; roles and responsibilities
- **Include relatives and associates** of people such as executives

Responses to Information Used (6.2.2)

6.2.2. Supplier/subcontractor qualification requirements and enforcement mechanisms

- Suggest cyber-audits
- For foreign supplies much of the **[information] suggested will not be available or difficult to obtain**, and that database and secondary checks will not provide the needed transparency into the critical information important for risk assessments.
- **Supplier, vendor, and sub-contractors key personnel need to be vetted**
- Balances held with suppliers and trade partners, including total trade and collection balance and historical information such as high credit and 6 month average balance
- Evaluate certifications and accreditations of suppliers/subs
- Evaluate whether a company requires its suppliers or subs to adhere to its supply chain security controls
- Verify companies sourcing from approved locations/not from potential origins of concern.
- This **indicates which companies proactively manage their supply chains**

Responses to Information Used (6.2.3)

6.2.3. Cybersecurity practices (network activity, data breaches, information security practices, and hardware and software assurance)

- Cyber **threat landscape should be considered** and included as part of a standard risk assessment.
- Cyber is the **most important indicator**, and [should be] basis for this due diligence program.
- Category is **too broad**; Some but not all are covered by requirements in OTTF
- Clarify how "data breaches" might be used in evaluating a supplier...a **mere occurrence of a data breach** (which vary is severity and impact) **may not negatively affect a supplier's evaluation**
- Examine html coding and Internet Protocol (IP) addresses on associated websites.
- Be able to **monitor media and social media** for cyber threats and action against companies.
- Penetration by botnets or other APT

Responses to Information Used (6.2.4 & 6.2.5)

6.2.4. Company information (ownership, control, and management)

- **Personal Conduct**: Alcohol Consumption; Drug Involvement; Criminal Activity; Psychological Conditions; Foreign Influence and Allegiance to the United States; Handling of Protected Information; Use of Information Technology Systems
- Sources for Company Risk info - news and press releases, social media data, online patent info, online info related to SEC filings and company health
- Number of employees at specific location and companywide; Family tree - account linkage which is the relationship between different companies within corporate family
- Years in Business; Ownership Status; Proposes data sources

6.2.5. Mergers and acquisitions activity

- WRT cybersecurity vs SCRM
- Understanding of related companies parent, subsidiaries and branches; understanding of which entity is financially responsible
- **Only if relevant to the purchase**
- Provide early warning signs if a large buyer is about to become wholly or partially owned by a foreign company based in a location of concern.
- Determine historical merger and acquisition activity.

Responses to Information Used (6.2.6)

6.2.6. Financial health, including solvency and liquidity

- Credit and financial stability risk scores and payment information
- Evaluate: supplier risk - likelihood supplier will cease business ops or become inactive; supplier stability - likelihood will experience significant financial or operational instability over next 3 months; historical payment performance; financial characteristics (annual sales, net worth, net income, cas, AR/AP; total assets, inventory, total current liability, current ratio, quick ratio
- Requests for proof of financial stability, to include audited/unaudited balance sheets, profit and loss statements for current year and prior two years. Other available sources of funding, lines of credits, debt, overdue accounts, etc.
- Bond Yield to Maturity - premium or interest paid by each company over life of bond to attract investors

Responses to Information Used (6.2.7)

6.2.7. Foreign ownership, control and influence of contractor and its suppliers and manufacturing hubs

- Can be understood through corporate linkage, business ownership and business owner background
- Suggest altering risk factor by addressing risk process and control and **removing the word "foreign" and "influence"**
- Determine the extent to which foreign governments hold influence over the decision-making of the corporation.
- Establish whether companies are affiliated to entities operating in countries of concern, or with sanctioned/restricted individuals or businesses.
- Further definition of manufacturing hubs is required. Off-shore facilities?
- Family tree - account linkage which is the relationship between different companies within corporate family

Responses to Information Used (6.2.8, 6.2.9 & 6.2.10)

6.2.8. Product and component (including those of sub-suppliers/ subcontractors) company and countries of origin

- Trace parts and sub-parts back to their respective original equipment manufacturers.

6.2.9. Logistics and supply chain controls, requirements, and enforcement mechanisms

- Include both forward and reverse logistics

6.2.10. Organizational reputation, customer complaint resolution

- Suggest these two elements should be segregated; "customer complaint" is **too broad and needs to refined to be relevant**
- Copies of any audit reports/findings
- Be able to monitor social media and state/federal regulatory agency information for expressions of dissatisfaction with products and resolution actions taken by companies.
- Indicate historic trends of counterfeit or non-conformance parts, as well as breach of contract - but these indicators are subjective

Responses to Information Used (6.2.11 & 6.2.12)

6.2.11. Physical security

- Suggest GSA specify that physical security policies, procedures, technology, and regular monitoring be considered
- To what standard or certification?
- May indicate insider threats, history of counterfeit parts or theft issues

6.2.12. Manufacturing practices (component and subcomponent supply chains)

- Require suppliers develop products in accordance with mutually agreed manufacturing and assembly processes, including by meeting info security requirements
- Verify the degree to which materials are physically protected and isolated from the potential for tampering
- Should be rolled into 6.2.8.

Responses to Information Used (6.2.13)

6.2.13. *Conformance with U.S. Federal government standards (e.g., Cost Accounting Standards, Facility and Personnel security clearances, FedRAMP, FIPS, CTPAT, etc.) and/or consensus based international standards (e.g., ISO, SAE, COBIT, etc.) for any of the above indicators*

- Consider clarifying the language to **refer to demonstrated conformance with certain laws, regulations, etc.**
- Seems to be a catchall. Suggest **determining which certifications and standards are most important** and identifying compliance, non-compliance, or N/A for each entity.
- Denied parties ship to List - check the frequency of references to denied parties and look for patters to identify potential unauthorized shipments

Additional Indicators (1 of 2)

- **Digital security and access requirements**
  - Captures the importance of policies, procedures, and technology to manage personnel access to physical and intellectual property
- **Product and service testing policies and procedures**
  - Evaluates how suppliers use policies, procedures and technology to reduce risks, respond to security challenges as they emerge and improve core products and services
- **Anti-counterfeit measures**
  - Actively identity counterfeit products and services and limit ability of counterfeiters to effectively operate
- **Media activity**
  - Automatically scan traditional and social media, to include in native language, for emergent stories. Monitor for positive and negative trends in both traditional and social media on a business partner

Additional Indicators (2 of 2)

- **Legal Matters**
  - Monitor for pending or settled civil and/or criminal litigation in jurisdictions around the world in native language. This includes activity against personnel and corporate entities.
  - Open suits, judgments, petitions, or payment remarks against vendor
- **Intellectual Property**
  - Is the company selling or acquiring large quantities of patents? Who is the company selling patents to or acquiring from and is there adverse information on the second party in the transaction?
- **Safety Performance**
  - Lost time, accident ratios, etc; OSHA violations
  - HazMat filings
- **Insurance**
  - Workers comp, automobile, general liability, other + amounts of coverage
- **Risk Culture Index**
  - Consider geo-sociopolitical location, industry and organization, finished goods, and service provides and services providers; data sources proposed

Q3: What Solution Providers exist?

- RFI Respondents
  - 8-10 articulated capability potential to provide a full solution
  - 5-6 articulated capability potential to provide a partial solution
  - 14 -17 were not providers of due diligence services

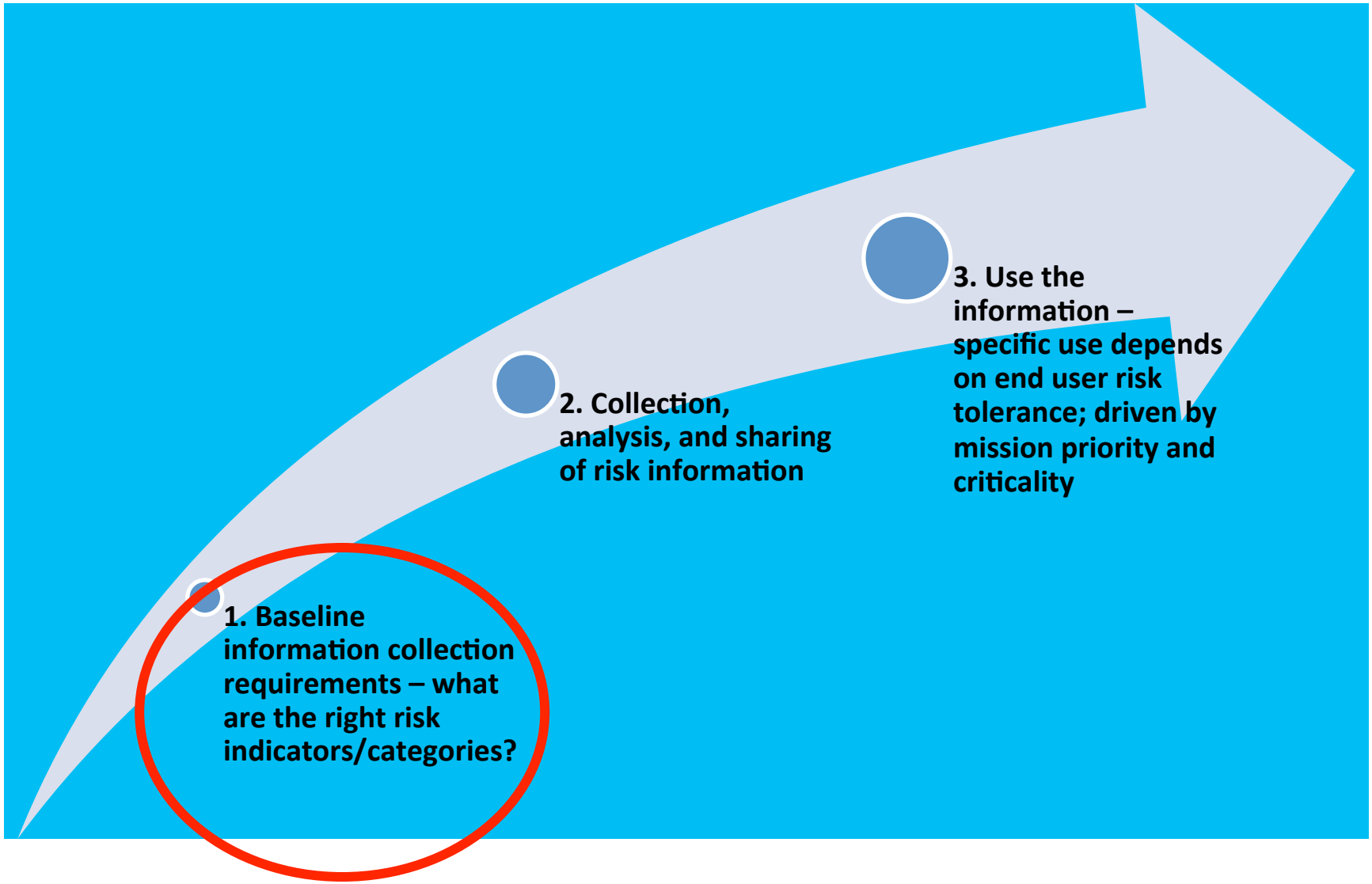
Review: Purpose of the Business Due Diligence RFI

Goal: Establish a common set of risk indicators/ categories that can be used by all Agencies to support government risk assessments.

- Information will be used by the Federal acquisition, grant, and oversight communities to support various government activities related to risk management.

- Selection of which contractors to assess will continue to be a risk-based decision made at the discretion of an agency.

Three Step Process to Increasing Buyer Access to and Use of Business Due Diligence Information….



[DRAFT] Risk Indicators/Categories

- People
  - Company leadership, ownership, management, mergers and acquisitions activity, media activity, organizational reputation, and personnel associations
  - Foreign ownership, control or influence of contractor or its suppliers
  - Insider Threat and physical security practices
- Process
  - Organization's financial health, including access to and sources of funding, solvency, and liquidity
  - Record of integrity and business ethics, including but not limited to legal and regulatory issues
  - Cybersecurity practices, including but not limited to network defense, incident response, information security practices, and participation in Information Sharing and Analysis Organizations
  - Financial systems, purchasing systems, production control procedures, property control systems, quality assurance measures, safety programs, insurance, physical security practices, and insider threat programs
  - Existing commercial and government clients/customers, small business subcontracting and diversity programs, cost performance (over/under –runs), delivery performance, customer service practices
- Technology
  - Product and component manufacturing practices including supply chains , production, construction, and technical equipment and facilities, and logistics , physical security requirements, and supplier qualification requirements, controls, requirements, and enforcement mechanisms
  - Hardware and software assurance practices, anti-counterfeit, intellectual property, and product and service testing policies and procedures

- Conformance (1st, 2nd or 3rd party) with U.S. Federal government or consensus-based market standards (e.g., Cost Accounting Standards, Facility and Personnel security clearances, FedRAMP, FIPS, CTPAT, ISO, SAE, COBIT, Open Group OTTP-S, etc.)

Inputs to Business Due Diligence

1. BUYER :

- Risk Tolerance – relative 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"

[DRAFT] Outputs of Business Due Diligence Information Shared Service

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

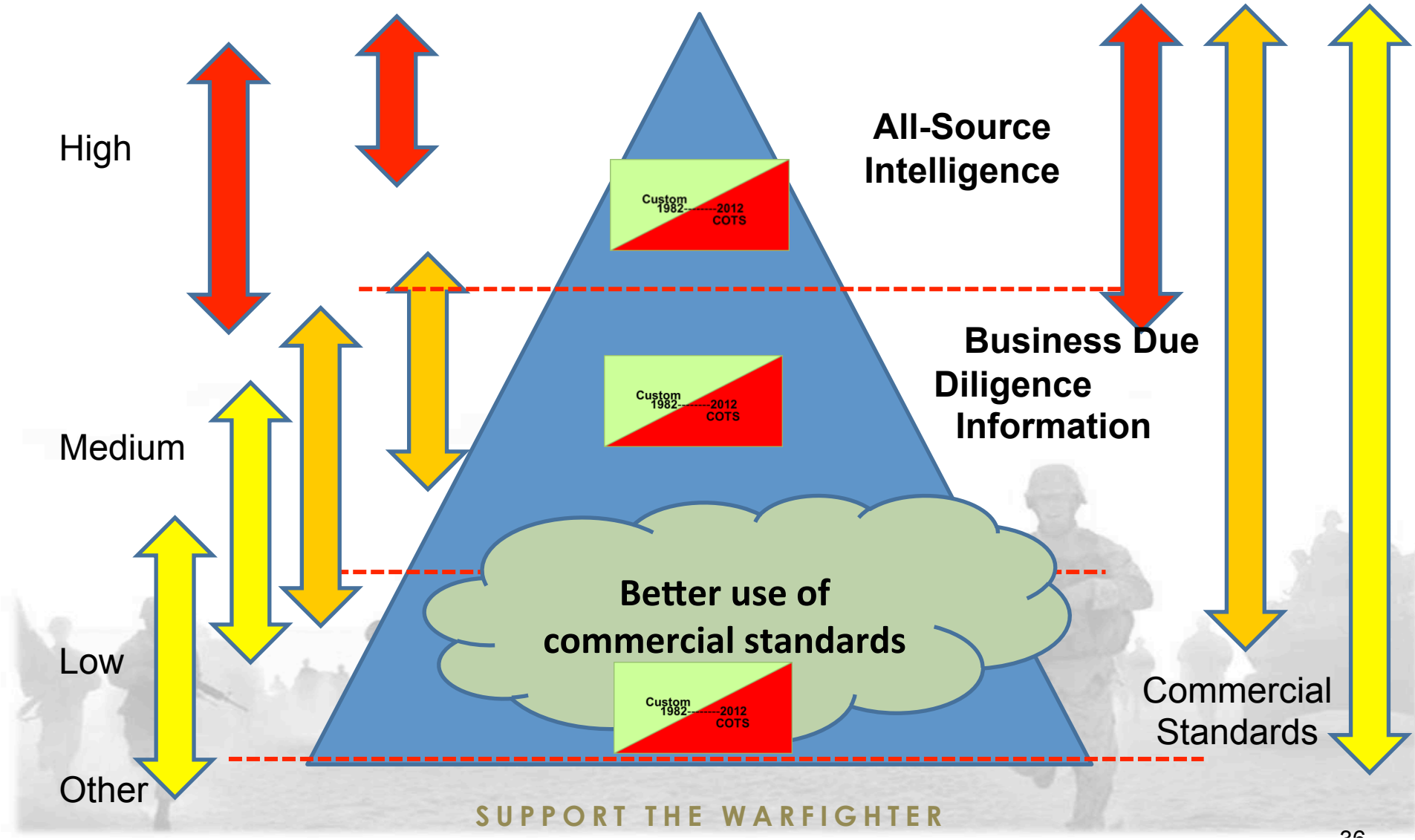
Perform Analytics

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

Conduct In-depth Investigations (as needed)

- On-site inspections
- Process reviews
- Personnel interviews

Prioritization
How to use Intel / Info to inform Risk Decision Making



Path Forward To Operationalizing The Solution

- ✓ Finalize Common Risk Indicators/Categories
- ✓ Finalize Core Capabilities Required
  - **Buyer:** Identify Seller, Specify Deliverable and Risk Tolerance
  - **Seller** (Voluntary): Information About Risk Indicators
  - **"Big Data:"** Publicly Available, Public Record, and Commercial Subscription Data about Seller
    - Initial Automated Risk Score
    - Aggregate Multiple Data Sources
    - Perform Analytics
    - Conduct In-depth Investigations (as needed)
- ✓ Justify Business Need For A Government-Wide Solution
- ✓ Create and Prototype A Government-Wide CONOPS
  - Validate Correlation of Risk Indicators to Desired Performance
  - Develop Transition Plan to Scale
  - Establish Performance Levels for similar