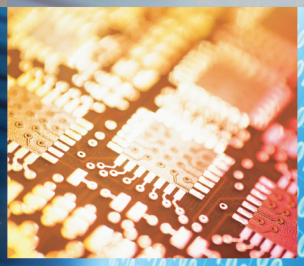


ASSESSING SCRM CAPABILITIES AND PERSPECTIVES OF THE IT VENDOR COMMUNITY:

TOWARD A CYBER-SUPPLY CHAIN CODE OF PRACTICE

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

A NIST-Sponsored Project Conducted by
The Supply Chain Management Center
Robert H. Smith School Of Business
University Of Maryland College Park

Table of Contents

List of Tables

List of Figures

Acknowledgements

The Smith supply chain management project team would like to thank Jon Boyens and Marianne Swanson of DOC/NIST and Brad Botwin DOC/BIS; Nancy Gillis of GSA; Joe Jarzombek and Kurt Seidling of DHS; Denise Peake of DOD/NSA; Don Davidson of DOD/CIO; and the other members of the CNCI Initiative 11 team-for their support and cooperation in the preparation of this report. We would also like to thank Lori Newman for her design and production support.

RH Smith School Of Business Project Team:

Dr. Sandor Boyson
Dr. Thomas Corsi
Mr. Hart Rossman
Mr. Matthew Dorin

Executive Summary

I. Project Concept

Initiative 11 (Supply Chain Risk Management) of the President's Comprehensive National Cybersecurity Initiative (CNCI) tasked the National Institute of Standards and Technology (NIST) with integrating lessons learned about cyber supply chain practices from various federal and industry initiatives into guidance for the federal enterprise and its industry partners.

NIST's Information Technology Lab awarded the Supply Chain Management Center of the Robert H. Smith School of Business at the University of Maryland in College Park a grant in support of the development of cyber supply chain best practice guidelines by NIST. In October, 2010, the Supply Chain Management Center began work on a project to develop, validate, and pilot test a research tool to assess the cyber-supply chain capabilities of the IT vendor community

This grant was aimed at addressing the fact that, at present, no readily identifiable assessment tool for industry exists that, if used extensively, could form the basis for a body of cyber-supply chain knowledge. Such a body of knowledge should contain data about current/planned corporate risk governance mechanisms, risk management audit/compliance activities, and benchmark practices against which to audit the capability and maturity of an organization.

This lack of a data-driven body of knowledge has been a major deficiency in the emerging discipline of Cyber-Supply Chain Risk Management (SCRM) and has constrained sound decision-making across government and the private sector. It was hoped that data gathered from this project could contribute to the formulation of a strawman SCRM Code of Practice that could advance the discipline and serve as a basis for ongoing dialogue between the public and private sectors.

II. Project Methodology

This project developed a tool to assess cyber-supply chain risk management capabilities by consolidating the collective inputs of the set of public and private actors engaged in supporting Initiative 11. The Department of Commerce (NIST and Bureau of Industry and Security, BIS), the Department of Homeland Security (DHS); the Department of Defense (DOD/CIO and DOD/NSA); and the Government Services Administration all provided formal inputs to design the assessment tool.

Representatives from Safe Code and Tech America's SCRM sub-committee also contributed valuable inputs.

This tool was then distributed to and validated with a sample of vendors of IT systems, software, hardware, and services. Our target participants included: small to medium-sized IT vendors traditionally under-represented in IT surveys; Chief Information Officers/Chief Security Officers nationally and in the Washington DC region; and Directors of Supply Chain.

There were 131 respondents who completed the survey from beginning to end. This means our survey response rate equaled the 1% industry bench mark for Third Party IT Surveys (source: IDG List Services). This is especially impressive given the absence of official survey distribution; the length of time it takes to fill in the survey (approximately 30 minutes); the newness of the subject discipline; and the difficulties some companies reported in routing the survey to appropriate person(s) in the organization. An additional 159 respondents completed one or more sections of the survey, but did not reach the end of the questionnaire. In total, 290 surveys were either partially or fully completed.

III. Key Results

Respondent Characteristics

The sample of research respondents reflects the fact that a number of different functional areas within firms are addressing the cyber-supply chain problem. As expected, professionals in IT, Telecom Services, and Information Security represent 63.4% of the sample, while professionals in Supply Chain Management, Procurement/Acquisition, and Risk Management accounted for an additional 36.6% of the sample.

Our respondent sample is dominated by small companies with less than $20 million in revenues, who represent 71% of the sample. By contrast, large companies with annual sales greater than $1 billion represent 10.3% of the sample. We believe these results represent one of the first times survey research in the cyber-community has reached beyond Tier 1 product companies and prime vendor/ integrators.

Software was cited as a line of business by 48.6% of respondents; hardware by 31.4%; telecom/data networking by 24.8%.; and system integration services by 62.4% of the sample.

We found that 55.4% of companies with annual sales of less than $20 million reported working across four or more IT product/service areas. We interpret this to mean that even very small companies are increasingly focused on the development and deployment of systems across traditional product/service boundaries. It also implies a trend to increasing IT Sector-wide managerial complexity. This complexity invariably leads to higher risk profiles across all classes of firms as broader sets of supply chain assets/resources need to be continuously protected from cyber threats.

About 86.8% of respondents currently serve and plan to serve the federal government.

Respondent SCRM Practices

Research results demonstrated that there is significant difference between the extent of use of strategic risk management practices in the IT supply chain and more tactical, or field level practices.

On the strategic side of risk management, 47.6% of the sample *never* uses a Risk Board or other executive mechanisms to govern enterprise risk; 46.1% *never* uses a shared risk registry/ an online database of IT supply chain risks; and 49.4% *never* uses an integrated IT supply chain dashboard/control. Even if we take away the requirement of real time supply chain systems, 44.9% say they *never* use a supply chain risk management plan.

The adaption of strategic risk management actions that does occur seems to be the province of big companies: the greater the company revenue, the greater the propensities to always or often use strategic risk measures. Only 17% of the smallest companies said they always or often use real time dashboards; compared to 50% of the biggest companies. Only 7% of smallest companies used on line risk registries always or often, compared to 63.2% of the biggest companies.

There appears to be a huge gulf between the smallest companies and the biggest companies who appear to have more real time information access and who tend to deploy that information as part of sense and respond cyber supply chain operations. One contributory factor might be that bigger companies are more risk and liability-sensitive. Additionally, they can invest more in sophisticated threat analysis techniques and in implementing enterprise-wide risk governance programs.

On the other hand, more tactical, narrowly focused cyber-SCRM practices are used much more often or always. Indeed, 67.3% of the sample often or always do personnel security reviews; 57.3% often or always use perimeter detection systems; and 49.4% often or always use a standardized process for pre-qualifying suppliers.

These more tactical defense mechanisms are indicative of single enterprise protection mechanisms, which may, in concert with other activities, provide some measure of defense in depth. However, they are not implemented with defense in breadth in mind; and can be perceived to lack the necessary executive management buy-in to influence customers and suppliers.

This deficiency of extended enterprise SCRM was further highlighted by the lack of collaboration among key actors within a supply chain evidenced in our sample: Companies report little or no collaboration with key suppliers: for example, 51.5% of companies in the sample provide no access to planning systems for their suppliers. Even the most widely accepted SCRM practice "jointly monitoring current changes, incidents, exceptions and disruptions" was only extensively used by 28.8% of the sample, less than a third of the respondents

The results seem clear: there is an overall lack of corporate emphasis on strategic defense in breadth and extended enterprise management of supply chain risks. Companies of all sizes tend to focus heavily on field-level technical practices.

Attractiveness Of Code Of Practice Elements

Finally, we asked respondents to rate the attractiveness of items for potential inclusion into a Code of Practice for IT Vendors that seeks to improve supply chain risk management**.**

Attractiveness was defined as an index score blending both operational effectiveness and feasibility of implementation.

We found a straightforward correlation: the greater the corporate revenue, the greater the corporate support for Code of Practice elements that are strategic in scope, e.g. Risk Boards and Risk Plans. Also, the largest companies are especially interested in obtaining government-designated favored supplier status: 91.7% of them rated priority status as the most effective/highly effective potential Code element as compared to 57.2% of the smallest companies.

There was across the board support for inclusion of elements that "provide additional contractual resources for SCRM" and "streamline regulations" into a Code of Practice.

On one hand, there is this desire on the part of companies of all sizes for streamlined, less burdensome or obtuse regulations and less government intervention. Yet, on the other hand, we found widespread support for government actions and information to clarify:

- What is the real threat?
- What are priority SCRM practices?
- How can expanded use of those practices by companies tie into to real corporate benefits, such as reduction of liability and overall compliance costs?

Successfully answering the latter question is especially crucial for successful adoption of a Cyber-Supply Chain Code of Practice

IV. Conclusions

There are a few critical conclusions that can be drawn from our research:

Both Large & Small Companies Seriously Under-Manage Cyber-SCRM

Both small and big companies increasingly work across hardware and software development, network management, and systems integration boundaries and have multiple product/service offerings. In other words, companies of all sizes have become complex supply chains with highly dispersed assets and resources.

Given the challenge of escalating cyber supply chain complexity, the current state of corporate SCRM capability seems inadequate for managing ***systemic risk***. The deficiency of cyber supply chain-wide risk governance strategies; the stove piped nature of risk management, cyber security and supply chain functions within corporations of all sizes; and an ongoing industry orientation toward narrowly focused process-models and technical solutions- all present serious impediments to effective SCRM in the current era.

Both Large & Small Companies Can Be Incentivized To Improve Cyber-SCRM

Small companies are highly motivated to get and use government cyber-supply chain risk management practice guidelines. This helps them to win business with the federal acquirer community; as well as to conserve scarce dollars and management time that they would otherwise have to spend themselves on cyber security compliance research.

Although their cyber security units are not well integrated into or supported by corporate risk management programs, big companies are nevertheless highly sensitive to managing regulatory demands for risk assurance and seeking to limit their own corporate liability. This sensitivity to risk and the search for shielding mechanisms have certainly been major motivating factors in developing Codes of Practice in other non-IT industries, such as the chemical industry (Code of Responsible Care) and the consumer products industry (Supply Chain Operations Reference Model).

Key challenges going forward include identifying and deploying the best incentive strategies available to assure maximum diffusion of and compliance with a core set of cyber-SCRM best practices. Such strategies might include: defining liability limits in cyber-supply chains; encouraging industry risk pooling to free up company-level capital reserves currently held for future liability claims or uninsurable risks; and implementing legislative/regulatory streamlining initiatives that ease industry compliance costs while building assurance levels.

Only by going forward together, can government and industry master the extreme challenges of cyber-SCRM in a global era.

I. PROJECT INTRODUCTION

Initiative 11 (Supply Chain Risk Management) of the President's Comprehensive National Cybersecurity Initiative (CNCI) tasked the National Institute of Standards and Technology (NIST) with integrating lessons learned about cyber supply chain practices from various federal and industry initiatives into guidance for the federal enterprise and its industry partners.

NIST's Information Technology Lab awarded the Supply Chain Management Center of the Robert H. Smith School of Business at the University of Maryland in College Park a grant in support of the development of cyber supply chain best practice guidelines by NIST. In October, 2010, the Supply Chain Management Center began work on a project to develop, validate, and pilot test a research tool to assess the cyber-supply chain capabilities of the IT vendor community.

This grant was aimed at addressing the fact that, at present, no readily identifiable assessment tool for industry exists that, if used extensively, could form the basis for a body of cyber-supply chain knowledge. Such a body of knowledge should contain data about current/planned corporate risk governance mechanisms, risk management audit/compliance activities, and benchmark practices against which to audit the capability and maturity of an organization. This lack of a data-driven body of knowledge has been a major deficiency in the emerging discipline of Cyber-Supply Chain Risk Management and has constrained sound decision-making across government and the private sector.

This project successfully developed a tool to assess cyber-supply chain risk management capabilities by consolidating the collective inputs of the set of public and private actors engaged in supporting Initiative 11. Thus, the Department of Commerce (NIST and BIS), the Department of Homeland Security(DHS), the(Department of Defense (DOD), DOD/NSA (National Security Administration), and GSA (Government Services Administration), as well as representatives from Safe Code and Tech America's SCRM (Supply Chain Risk Management) sub-committee all provided formal inputs to design the assessment tool. This tool was then distributed to and validated with a sample of vendors of IT systems, software, hardware, and services.

It is hoped that this project can provide a step toward rapid development of a shared government/industry Code of Cyber-Supply Chain Practice that could be endorsed both by industry organizations representing all vertical segments of the IT supply chain and companies of all sizes; as well as by federal policy entities.

II. BACKGROUND

What Exactly is a Code of Practice?

A Code of Practice in business is typically a written set of guidelines designed to galvanize a community in its ethics and operations. A Code of Practice is an **industry-wide initiative** to preserve the brand standing and integrity of products and services with regulators and consumers in order to limit a firm's liability as well as to reduce capital reserves held for "uninsurable risks".

It is a **"condition of membership"** to join a premiere industry organization. In other words, a company must subscribe to an agreed upon set of practices and show auditable progress towards full implementation of those practices in order to obtain and maintain membership in the organization.

One example of an effective Code of Practice is provided by the Toronto Stock Exchange (TSX). In 1994, the TSX's Dey Report to Improve Corporate Governance noted: "Many Boards have **no formal processes to evaluate risk".** Since 1994, an effective corporate risk management program has been a key requirement for a company **initially obtaining and/or maintaining its listing** on the TSX. TSX requires all listed companies to **disclose their corporate risk governance practices** each year in their annual reports or in their management information and proxy circulars.

Section 1B Of TSX Corporate Disclosure Guidelines: Disclosure Of Principal Risks

- In 1999, after reviewing the corporate governance disclosures of over 700 of its issuers, TSX proposed **specific improvements to risk management** now in effect.
- **Risk Management was made a top governance requirement**, #3 in priority after corporate stewardship and strategic planning.
- Section 1 (b) requires the **identification of the principal risks** of the corporation's business and ensuring the implementation of appropriate systems to manage these risks.
- The **Board of Directors**, through the Audit Committee, is responsible for identifying the principal risks of the company and ensuring that risk management systems are implemented.
- The **Audit Committee** meets regularly to review reports and discuss significant risk areas with the internal and external auditors.

(Source: TSX, "Corporate Governance: A Guide to Good Disclosure" http://www.ecgi.org/codes/documents/tsx_gtgd.pdf)

Another effective Code of Practice involves the American Chemistry Council's (ACC's) Responsible Care ® initiative. Since 1988, corporate members of the ACC have significantly improved their environmental, health, safety, and security performance through this initiative.

Participation in Responsible Care is mandatory for ACC member companies, all of which have made CEO-level commitments to uphold these program elements:

- Measuring and publicly reporting performance.
- Implementing the Responsible Care Security Code.
- Applying the modern Responsible Care management system to achieve and to verify results.
- Obtaining independent certification that a management system is in place and functions according to professional standards.

Responsible Care is also a global initiative that is practiced currently in 53 national associations, which share a common commitment to advancing the safe and secure management of chemical products and processes.

(Source: http://www.americanchemistry.com/s_responsiblecare/sec.asp?CID=1298&DID=4841)

More closely related to the cyber vertical**, the Supply Chain Operations Reference Model (SCOR)** is maintained by the Supply Chain Council, an independent, not-for-profit, global corporation with membership open to all companies and organizations interested in applying and advancing state-of-the-art supply chain management systems and practices**.**

- Founded in 1996
- Over 800 Company Members
- Cross-industry representation
- Chapters in Australia/New Zealand, Brazil, Europe, Japan, North America, South East Asia, and China with petitions for additional chapters pending.

The SCC developed and endorsed the SCOR model as the cross-industry standard for supply chain management. SCOR is a process framework for modeling end-to-end supply chain processes, performance, and practices. The framework delivers the well-known concepts of business process reengineering, benchmarking, and best practices into a cross-functional framework

- Standard processes: Plan, Source, Make, Deliver, Return, Enable
- Standard metrics: Perfect Delivery, Cash Cycle Time, Supply-Chain Cost, etc.

- Standard practices: SCRM, EDI (Electronic Data Interchange), CPFR (Collaborative Planning, Forecasting, and Replenishment), Cross-Training, etc.

- Pre-defined relationships between processes, metrics, and practices

Recently, a global, multi-industry team worked for one year to enhance SCOR by adding to it a module for supply chain risk that attempted to:

- To provide a process to identify potential areas of risk throughout the supply chain.

- To offer a competitive edge through identification and acceptance of controlled risks.

- To enable companies to reduce impacts and to mitigate service disruptions.

(Source: Wilkerson, Taylor "Using SCOR FOR SCRM", LMI, 2011)

These are examples of effective member-developed and enforced Codes of Practice in other industries that could be instructive in developing a Cyber-Supply Chain Code of Practice.

What Are Key Problems in Cyber Supply Chain Code of Practice Development?

We are in a *very early stage in defining cyber supply chain best practices*- similar to where product supply chains were in the mid-1990s. There are assumptions or unknowns about what really works or what doesn't-work. However, as of yet, there is not an empirical, evidence-based data to guide informed decisions. There is emphasis on defensive domain-specific technical solutions versus proactive supply chain-wide risk management programs. Persistent fragmentation of governance between the Legal Counsel/Risk Officer; the Chief Information Officer (CIO)/Chief Security Officer (CSO); and the Chief Supply Chain Officer has prevented deployment of corporate and extended enterprise supply chain risk management programs.

Indeed, "the Cyber Dimension is still being viewed in isolation, instead of as part of a single Multi-Dimensional Corporate Supply Chain currently undergoing extreme volatility." (source: Lisa Harrington, Sandor Boyson, and Thomas M. Corsi, **X-SCM: The New Science Of X-Treme Supply Chain Management**, Routledge Press, 2010)

The Multi-Dimensional Supply Chain has increasingly integrated product, service, financial and IT systems. This supply chain is highly dispersed, yet deeply networked, meaning that risks can spread across it quickly like a prairie fire. Like the physical supply chain, the cyber supply chain is experiencing instabilities of unprecedented amplitude, frequency, and duration. In the process conventional wisdom is overturned and there is a need for a new science of cyber supply chain management.

Developing a Research-Based Cyber Supply Chain Code of Practice
Our research in developing a cyber-supply chain code of practice has been conducted over a three year period:

- Phase 1: UMD/SAIC Research Project Begins/ **Literature Review and Interview Guide Development** (October –November 08).

- Phase 2: Conducted interviews with 30 thought leaders in the systems engineering, network management, software/hardware development, human factors, and supply chain risk management areas (November 2008–February, 2009).

- Phase 3: Compiled interview results, analyzed findings, and prepared a Prototype Cyber-Supply Chain Practice Model for presentation to a focus group of 25 government and industry senior executives (March, 2009).

- Phase 4: Results of this feedback incorporated into a working paper available at http://www.saic.com/news/resources.asp (June, 2009).

- Phase 5: Organizational field studies conducted to validate model (Fall/Winter 2010).

- Phase 6: NIST-sponsored research on industry perspectives. Developed extensive Code of Practice questionnaire with inputs from key CNCI Initiative 11 actors and industry.

- Validated it with a pilot sample (Fall/Winter 2011).

Going forward, our research approach emphasizes these further *development principles for a Code of Cyber Supply Chain Practice:*

- **Shared responsibility for risk identification** by all actors in the supply chain.

- **Dynamic system for prioritizing risks**, registering priority risks in a Supply Chain Risk Registry, and assigning them to process owners who self-manage the risk.

- **Process owners are incentivized to manage risks** effectively so as:

    - To hedge against excessive regulation.

- To gain greater protection from liability.
- To free up corporate financial reserves currently held for uninsurable risk.

The afore-mentioned principles are strongly aligned with Initiative 11's emphasis on "agreement processes" and SLA provisions as a way to handle the problem of guiding a complex network.

SwA's emphasis on "maximizing transparency to acquirer" can be expressed in a Code's expectation of continuous supplier due diligence monitoring and mitigation action audits.

A Code of Practice would enable the acquirer to assess supplier capability by presenting a constellation of strategic and operational practice benchmarks against which the maturity level of a vendor's supply chain risk practices can be compared.

III. PROJECT TASKS

Methodology

The Supply Chain Management Center has extensive experience in developing and validating research tools as well as managing large scale research for public and private organizations such as the Department of Energy, the Department of Transportation, and DHL.

NIST funding enabled the creation and sustainment of a team composed of Center faculty, research fellows, and graduate students to:

- Develop a multi-dimensional assessment instrument to measure the diffusion of key practices across both the existing as well as the prospective IT vendor base and to obtain their perspectives on the attractiveness of possible elements of a Code of Cyber-Supply Chain Practice.

- Define the universe of possible respondents in the pilot sample and reach out to these prospects.

- Tabulate the results and analyze findings.

Based on literature reviews and previous stages of research conducted by our Center as well as the research contained in the NIST Interagency Report, Piloting Supply Chain Risk Management Practices for Federal Information Systems (NISTIR 7622) and the DOD State of the Art Report, Security Risk Management for the Off-the-Shelf (OTS) Information Communications Technology (ICT) Supply Chain or IT Risk Management, our team compiled a comprehensive questionnaire to assess current cyber-supply risk management capabilities.

The questionnaire contained the following sections:

- *Section 1*-Company Profile contained questions related to respondent role, company size, product/service portfolio, and vendor status with the federal government.

- *Section 2*-Current Practices contained questions related to extent of corporate use of IT supply chain risk management practices as well as the perceived effectiveness of those practices. Also included in this section were questions related to the status of supply chain collaboration and visibility with suppliers and customers.

- *Section 3*-Perspectives on Improving Supply Chain Risk Management contained questions related to the company's perceptions of the best evaluation criteria and contractual requirements to control supplier risk as well as the best ways to enhance readiness capabilities in the event of cyber-attacks.

- *Section 4*- Code of Practice contained possible elements of a consensus code of cyber-supply chain practice and asked respondents to rate both the potential

operational and cost effectiveness of each code element in a combined Index Measure.

We would like to thank these core Government and industry executives who received and reviewed the draft questionnaire and offered additional inputs:

- DOC: NIST: Marianne Swanson, Jon Boyens; and BIS:Brad Botwin
- GSA: Nancy Gillis
- DHS: Joe Jarzombek, Kurt Seidling, and his GSCRM PMO Team.
- DOD/NSA: Denise Peake
- DOD/CIO: Don Davidson
- Tech America: Trey Hodgkins an the SCRM sub-committee
- Safe Code: Dan Reddy (EMC)

We would like to thank these core industry executives who received and reviewed the draft questionnaire and offered additional inputs. The end result of several iterations of feedback and modification was a document that incorporated both multi-agency and industry questions as well as best practice diffusion questions and Code of Practice items for testing/validation. (See Questionnaire Appendix 1)

Target Participants

- Small to medium-sized IT vendors are traditionally under-represented in IT surveys. GSA provided a list of recent corporate attendees at GSA IT Vendor Fairs (approximately 3000 names/email addresses)
- CIOs/CSOs nationally and in Washington DC region (derived from the following sources: All Senior titles (VP+) from *Chief Security Officer Magazine* (approximately 5,000 names/email mail addresses) and All Senior Titles (VP+) within DC/VA/MD from *CIO Magazine* (approximately 2500 names/email addresses)
- Directors of Supply Chain (derived from: All Director+ titles with supply chain within DC/VA/MD from IDG Corporate database (approximately 2500 names)

We e-mailed a cover letter containing a link to our survey website to a total universe of 13,000 target participants. There were 131 respondents who completed the survey from beginning to end, although they did not necessarily answer every question. ***This means our survey response rate equaled the 1% industry bench mark for Third Party IT Surveys*** (source: IDG List Services). This is especially impressive given the absence of official survey distribution; the

length of time it takes to fill in the survey (approximately 30 minutes); the newness of the subject discipline; and the difficulties some companies reported in routing the survey to appropriate person(s) in the organization. An additional 159 respondents completed one or more sections of the survey, but abandoned the effort prior to reaching the end of the questionnaire. In total, 290 surveys were either partially or fully completed.

Limitations of Study

The research plan for this project originally included formal NIST distribution of the questionnaire to its stakeholder groups. The decision that there would be no formal distribution due to OMB approval complexities occurred *after* funding was awarded. This caused us to have to shift project strategy quickly and attempt to locate appropriate lists of respondent prospects. We believe this lack of official distribution constrained survey response rates. As stated earlier, high-level corporate support and multi-disciplinary inputs are required to respond to the questionnaire which likely could have been strengthened by official distribution of the questionnaire.

Anecdotal reports suggest that routing of the participation request to appropriate person(s) within a corporation was sometimes made difficult due to the newness of the topic and unfamiliarity with the appropriate person with sufficient knowledge to complete the survey. We had attempted to address this issue by providing respondents with the ability to pause the survey and allow a colleague with special subject matter expertise in either risk management, cyber-security, or supply chain to go back in to fill in a relevant section, but clearly problems in harnessing multiple inputs from the same company were persistent.

IV. RESULTS

In this section, we will present the summary results of each question in the questionnaire and provide additional information about responses to questions
filtered by the revenue size or industry role of the company.

I. QUESTIONNAIRE: Respondent Profile

Table 1

What most accurately describes your company job title? (Check one)

	Frequency	Percent
Director/Associate Director/Manager, Supply Chain Management	32	11.0
Director/Associate Director/Manager, Procurement/Acquisition	46	15.9
Director/Associate Director/Manager, Product Engineering	22	7.6
Director/Associate Director/Manager, Information Technology	146	50.3
Director/Associate Director/Manager, Telecom Services	10	3.4
Director/Associate Director/Manager, Information Security	28	9.7
Director/Associate Director/Manager, Risk Management	6	2.1
Total	290	100.0

The sample reflects the fact that a number of different functional areas within firms are addressing the cyber-supply chain problem. As expected, professionals in IT, Telecom Services, and Information Security represent 63.4% of the sample, while Professionals in Supply Chain Management, Procurement/Acquisition, and Risk Management accounted for an additional 36.6% of the sample.

Table 2

How large is your company?

		Frequency	Percent
	Annual sales less than $20 million	193	71.0
	Annual sales between $20-$50 million	19	7.0
	Annual sales between $50-$100 million	15	5.5
	Annual sales between $100-$1 billion	17	6.3
	Annual sales greater than $1 billion	28	10.3
	Total	272	100.0
	Missing	18	
Total		290	

Our respondent sample is dominated by small companies, with less than $20 million in revenues, who represent 71% of the sample. In contrast, large companies, with annual sales greater than $1 billion, only represent 10.3% of the sample.

We believe these results represent one of the first times a survey in the cyber-community has reached beyond Tier 1 product companies and prime vendor integrators.

Table 3

Does your company provide Software?

	Frequency	Percent
No	149	51.4
Yes	141	48.6
Total	290	100.0

Table 4

Does your company provide Hardware?

	Frequency	Percent
No	199	68.6
Yes	91	31.4
Total	290	100.0

Table 5

Does your company provide Systems Integration Services?

	Frequency	Percent
No	109	37.6
Yes	181	62.4
Total	290	100.0

Table 6

Does your company provide Telecom/Data Network Provisioning?

	Frequency	Percent
No	218	75.2
Yes	72	24.8
Total	290	100.0

Software was cited as a line of business by 48.6% of respondents; hardware by 31.4%; telecom/data networking by 24.8%. 62.4% of the sample said that their firms provided system integration services.

If we look at the product/service profile of respondents, we find 55.4% of companies with annual sales of less than $20 million report working across four or more IT product/service areas; compared to 18.5% of companies with $1 billion or more in sales. We interpret this to mean that even small companies are increasingly focused on the development and deployment of systems across traditional product/service boundaries. It also implies increasing IT Sector-wide managerial complexity and supply chain volatility as networks of suppliers widely disperse across the globe; and protection of all assets/resources (including IT assets/resources) becomes more challenging.

Table 7

Does your company provide Hosted/Cloud Applications?

	Frequency	Percent
No	211	72.8
Yes	79	27.2
Total	290	100.0

27.2% of vendors currently supply hosted/cloud applications. This is expected to increase rapidly over time as the Obama Administration rolls out its Cloud First Initiative and spends 20% of the $80 billion IT spend of the federal government on cloud services.

Table 8

Does your company provide Other Services?

	Frequency	Percent
No	192	66.2
Yes	98	33.8
Total	290	100.0

The Other Category included a range of activities, from providing critical power and cooling data centers to technology and capital strategy. A full list can be seen in the filled out questionnaire with all results and comments in Appendix 1.

Table 9

Does your company currently supply IT products/services to the federal government?

		Frequency	Percent
	Yes	239	86.9
	No	36	13.1
	Total	275	100.0
Missing	System	15	
Total		290	

Table 10

Is your company planning to supply the federal marketplace?

		Frequency	Percent
	Within the next year	204	86.8
	Within the next three years	16	6.8
	No plans to enter the market	15	6.4
	Total	235	100.0
Missing	System	55	
Total		290	

Both tables indicate about 86.8% of sample currently serve and plan to serve the federal government.

II. QUESTIONNAIRE: Practices

In the following questions, we try to assess the extent of use and perceived effectiveness of high level supply chain risk management practices. In the right hand column, we highlight respondents who answered that each practice was used often or always to emphasize practices with strong acceptance by companies.

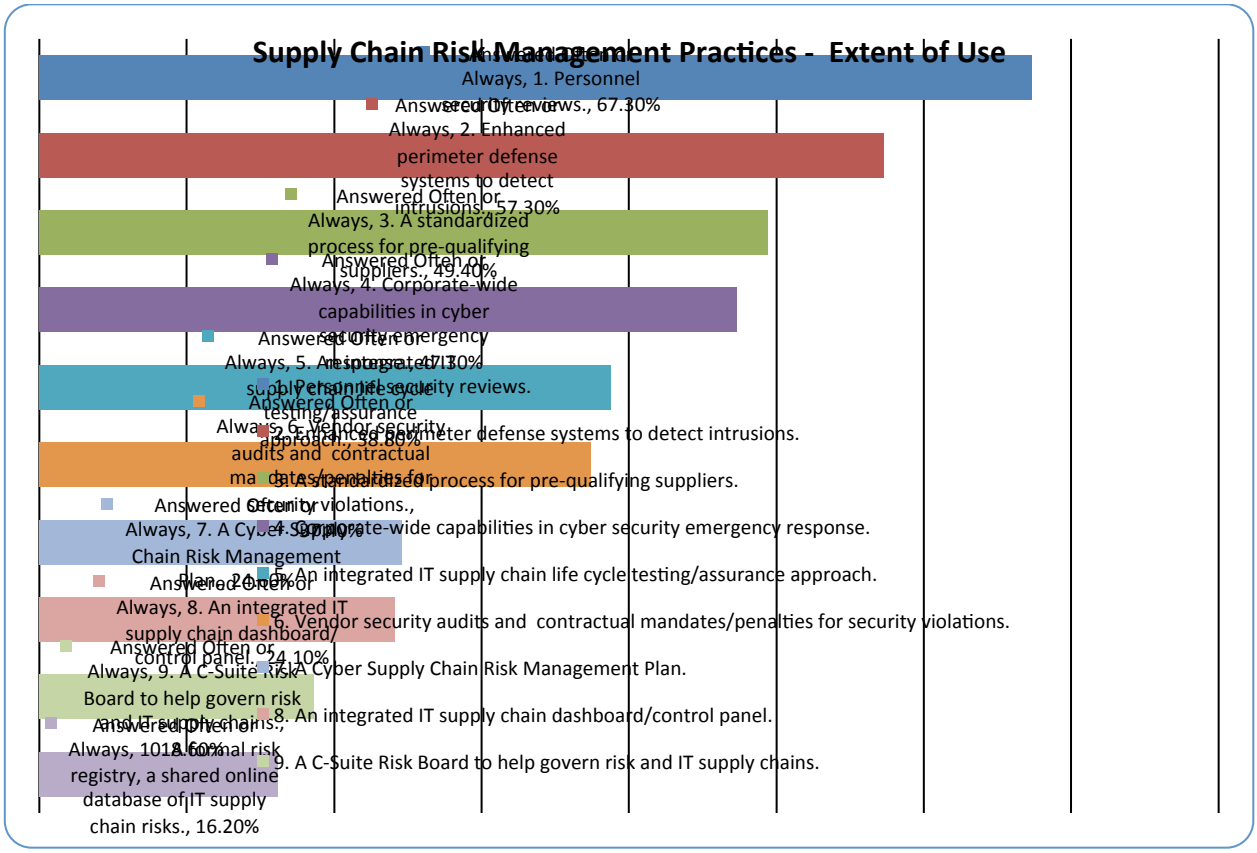
Below are higher level practices some companies are using to try to manage IT supply chain risk. For each of these practices, rate the extent of its current use in your own organization:

Table 11

Items	Never	Seldom	Sometimes	Often	Always	Often or Always
1. Personnel security reviews.	9.70%	8.50%	14.50%	21.20 %	46.10%	67.30%
2. Enhanced perimeter defense systems to detect intrusions.	23.20%	4.30%	15.20%	19.50 %	37.80%	57.30%
3. A standardized process for pre-qualifying suppliers.	17.30%	8.30%	25.00%	20.80 %	28.60%	49.40%
4. Corporate-wide capabilities in cyber security emergency response.	21.80%	12.10%	18.80%	17.00 %	30.30%	47.30%
5. An integrated IT supply chain life cycle testing/assurance approach.	35.80%	6.70%	18.80%	20.00 %	18.80%	38.80%
6. Vendor security audits and contractual mandates/penalties for security violations.	29.40%	14.10%	19.00%	17.80 %	19.60%	37.40%
7. A Cyber Supply Chain Risk Management Plan.	44.90%	9.60%	21.00%	12.00 %	12.60%	24.60%
8. An integrated IT supply chain dashboard/control panel.	49.40%	9.60%	16.90%	15.70 %	8.40%	24.10%
9. A C-Suite Risk Board to help govern risk and IT supply chains.	47.60%	16.90%	16.90%	12.00 %	6.60%	18.60%
10. A formal risk registry, a shared online database of IT supply chain risks.	46.10%	15.00%	22.80%	9.00%	7.20%	16.20%

Number of Respondents=168

Figure 1



Number of Respondents=168

What is important to note in the results is the big difference between the extent of use of strategic risk management practices in the IT supply chain and more tactical, or field level practices. On the strategic side of risk management, 47.6% of the sample *never* uses a Risk Board or other executive mechanisms to govern enterprise risk; 46.1% *never* uses a shared risk registry/ an online database of IT supply chain risks; and 49.4% *never* uses an integrated IT supply chain dashboard/control. Even if we take away the requirement of real time supply chain systems, 44.9% say they *never* use a supply chain risk management plan.

On the other hand, more tactical, more narrowly focused practices are used much more often or always. Indeed, 67.3% of the sample often or always do personnel security reviews; 57.3% often or always use perimeter detection systems; and 49.4% often or always use a standardized process for pre-qualifying suppliers. These more tactical defense mechanisms are indicative of single enterprise protection mechanisms, which may, in concert with other activities, provide some measure of defense in depth. However, they are not implemented with defense in breadth in mind; and can be perceived to lack the necessary executive management buy-in to influence customers and suppliers.

The results seem clear: there is a lack of corporate emphasis on strategic defense in breadth/ supply chain risk management activities. Companies of all sizes tend to focus heavily on field-level technical practices.

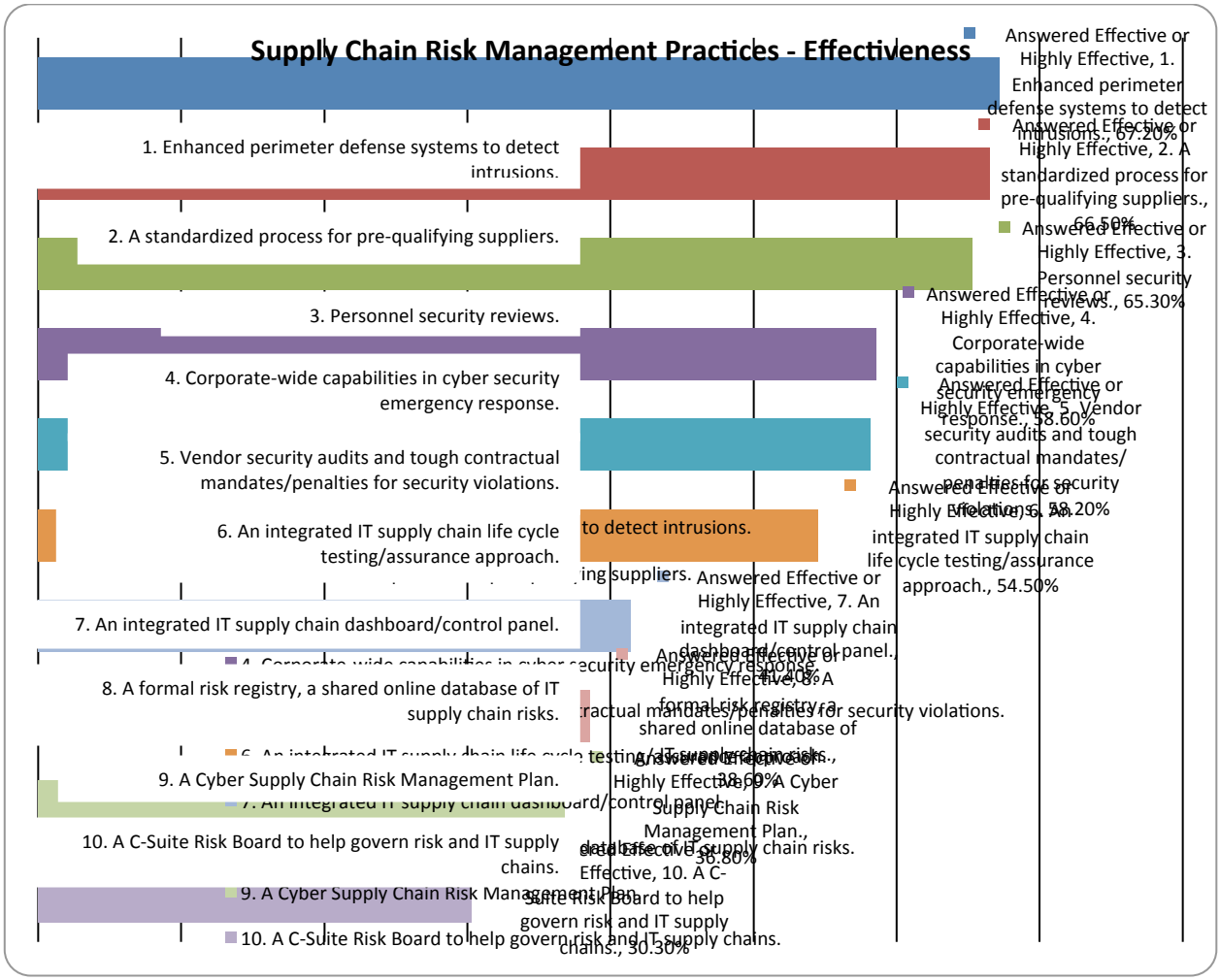
Below are higher level practices some companies are using to try to manage IT supply chain risk. For each of these practices, rate its actual or perceived effectiveness (or helpfulness) in managing risk in your extended supply chain:

Table 12

Items	Ineffective	Somewhat Effective	Moderately Effective	Effective	Highly Effective	Effective or Highly Effective
1. Enhanced perimeter defense systems to detect intrusions.	12.80%	6.00%	14.10%	33.60%	33.60%	67.20%
2. A standardized process for pre-qualifying suppliers.	9.40%	4.70%	19.50%	37.60%	28.90%	66.50%
3. Personnel security reviews.	6.70%	8.00%	20.00%	33.30%	32.00%	65.30%
4. Corporate-wide capabilities in cyber security emergency response.	14.50%	6.20%	20.70%	28.30%	30.30%	58.60%
5. Vendor security audits and tough contractual mandates/penalties for security violations.	13.00%	10.30%	18.50%	32.90%	25.30%	58.20%
6. An integrated IT supply chain life cycle testing/assurance approach.	17.70%	7.50%	20.40%	32.70%	21.80%	54.50%
7. An integrated IT supply chain dashboard/control panel.	26.20%	7.60%	24.80%	27.60%	13.80%	41.40%
8. A formal risk registry, a shared online database of IT supply chain risks.	20.70%	12.40%	28.30%	23.40%	15.20%	38.60%
9. A Cyber Supply Chain Risk Management Plan.	21.50%	18.10%	23.60%	25.00%	11.80%	36.80%
10. A C-Suite Risk Board to help govern risk and IT supply chains.	28.90%	20.40%	20.40%	21.80%	8.50%	30.30%

Number of Respondents=150

Figure 2



Number of Respondents=150

In terms of effectiveness, respondents rated the same three tactical practices that were most extensively used in their organization as also the most effective practices. As such, 67.2 % of respondents believed enhanced perimeter defense was th most effective practice; while a standardized process for pre-qualifying suppliers (66.5%) was rated as the second most effective practice; and personnel security reviews (65.3%) as the third most effective one. We interpret this to mean that the respondents are rating the practices they most frequently use as the most effective practices. While this could indicate a high level of satisfaction with the practices currently most frequently in use, it might also suggest a level of complacency with familiar practices.

Let us examine each tactical priority.

Enhanced perimeter defense can be defined as putting your defenses out on the edge of your networks. It is also called the "Wall and Moat" Model. Others describe this as representing an organization that is hard and crunchy on the outside, but soft on the inside. These terms describe

a lack of defense in depth capabilities. Once the perimeter is breached, the insides are vulnerable. An insider threat is even more ominous for a company employing this model.

A standardized process for pre-qualifying suppliers can be defined as a "set and forget" model. This model focuses on prequalifying suppliers but does not conduct frequent vendor audits or continuous monitoring of them. That this is the case is evidenced by the fact that 43.5% of respondents report seldom or never performing vendor security audits; over 59% seldom or never use real time dashboards to monitor risk; and only 16% use online risk registries.

On the basis of both extent of use and effectiveness of use, respondents overwhelmingly favor tactical risk management practices.

But there are contradictions and discrepancies in the data even while the overall trend line is clear. It is very interesting that only 18% of respondents often or always use a C-Suite Risk Board, but over 30% believe it is often or always effective. An interpretation could be that respondents may not use this strategic practice themselves, but understand its potential power from colleagues or professional contacts/and simply may not have the authority to implement collaborative risk management practices in their own organizations.

Adaption of Strategic Risk Management Actions/By Company Size

Table 13

Practice: Used Practice Always Or Often	**Risk Executive Board**	**Risk Management Plan**	**On Line Risk Registry**	**Real-Time Dashboard**
Annual sales less than $20 million	16.2%	16.6%	7.0%	17.0%
Sales $100 million to $1 billion	27.3%	33.4%	33.3%	33.4%
Sales greater than $1 billion	41.1%	61%	63.2%	50%

Number of Respondents=145: Less than $20 million=114; $100-$1billion=12; Greater than $1 billion=19

Adaption of strategic risk management actions seems to be the province of big companies: the greater the company revenue, the greater the propensity to always or often use strategic risk measures.

Bigger companies are more risk and liability-sensitive. They can invest more in sophisticated threat analysis techniques and in implementing enterprise-wide risk governance programs. Only 17% of the smallest companies said they always or often use real time dashboards; compared to 50% of the biggest companies. Only 7% of smallest companies used risk registries always or often, compared to 63.2% of the biggest companies. There is a huge gulf between the smallest companies and the biggest companies who have real time information access and who deploy that information as part of a sense and respond supply chain operation.

Yet, not all the problem lies in capital investment differences between companies- after all, risk boards can be created within an organization by organizing a management team to work

holistically and not necessarily by spending a huge amount of money on equipment. Small companies need more business guidance on ways to reengineer management systems, since they are not capable of investing significant resources into action-oriented SCRM research

Adaption of Tactical Risk Management Actions/By Company Size

Table 14

Practice: Used Practice Always Or Often	**IT Lifecycle Testing**	**Enhanced Perimeter Defense**	**Process To Pre-Qualify Suppliers**	**Vendor security Audits**	**Cyber Emergency response**	**Personnel Security Reviews**
Annual sales less than $20 million	34.5%	49.1%	43.5%	32.4%	39.3%	63.9%
Sales $100 million to $1 billion	50.0%	83.3%	41.0%	50.0%	50.0%	50.0%
Sales greater than $1 billion	61.1%	83.3%	78.9%	66.7%	94.7%	84.2%

Number of Respondents=145: Less than $20 million=114; $100-$1billion=12; Greater than $1 billion=19

As seen in the table above, the larger the company revenue, the greater the diffusion and adoption of key tactical risk management practices within their organizations. However, these tactical practices are also generally more evenly distributed than are the strategic risk management actions across the whole set of respondent companies. For example, 63.9% of the smallest companies always or often use personnel security reviews compared to 84.2% of companies with sales greater than $1 billion.

This latter finding also presents a challenge to conventional wisdom that holds "the human factor is the weak link" in the IT Supply Chain. Most companies in our pilot sample perceive themselves as actively engaged in screening and monitoring the human factor risk in the chain. However, what is not clear is what automated defense may be in place for the ongoing monitoring and mitigation of insider threat.

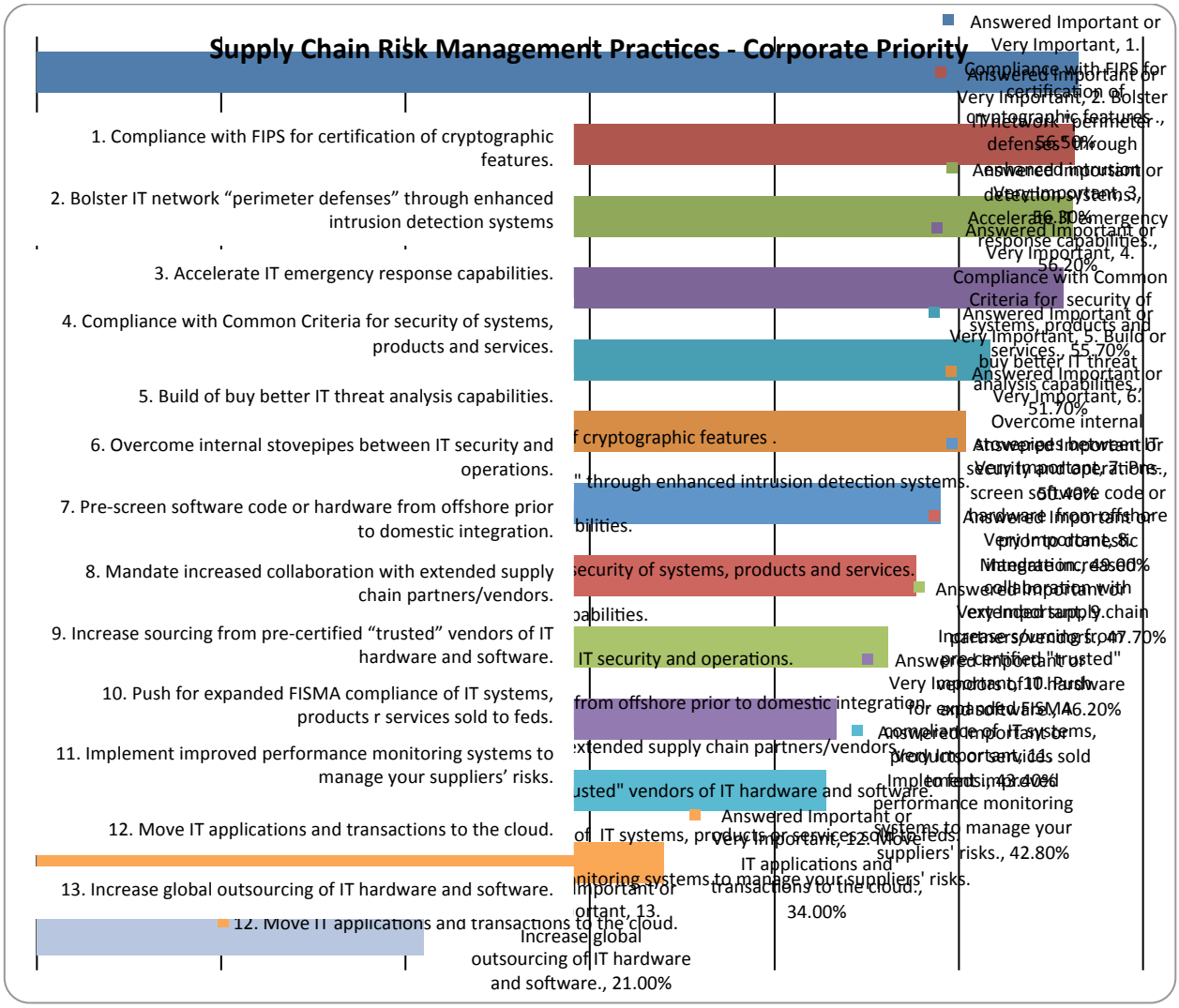
How important a corporate priority for the upcoming year is each of these supply chain risk management actions?

Table 15

Items	Unimportant	Of Little Importance	Moderately Important	Important	Very Important	Important or Very Important
1. Compliance with FIPS for certification of cryptographic features.	10.90%	8.70%	23.90%	27.50%	29.00%	56.50%
2. Bolster IT network "perimeter defenses" through enhanced intrusion detection systems.	11.10%	8.30%	24.30%	30.60%	25.70%	56.30%
3. Accelerate IT emergency response capabilities.	6.90%	9.00%	27.80%	31.90%	24.30%	56.20%
4. Compliance with Common Criteria for security of systems, products and services.	6.30%	8.50%	29.60%	27.50%	28.20%	55.70%
5. Build or buy better IT threat analysis capabilities.	9.50%	10.90%	27.90%	31.30%	20.40%	51.70%
6. Overcome internal stovepipes between IT security and operations.	11.70%	11.70%	26.20%	29.00%	21.40%	50.40%
7. Pre-screen software code or hardware from offshore prior to domestic integration.	22.00%	9.90%	19.10%	27.70%	21.30%	49.00%
8. Mandate increased collaboration with extended supply chain partners/vendors.	10.20%	9.50%	32.70%	32.70%	15.00%	47.70%
9. Increase sourcing from pre-certified "trusted" vendors of IT hardware and software.	11.20%	11.90%	30.80%	33.60%	12.60%	46.20%
10. Push for expanded FISMA compliance of IT systems, products or services sold to feds.	14.00%	11.20%	31.50%	23.10%	20.30%	43.40%
11. Implement improved performance monitoring systems to manage your suppliers' risks.	15.00%	10.70%	31.40%	27.10%	15.70%	42.80%
12. Move IT applications and transactions to the cloud.	18.10%	17.40%	30.60%	22.90%	11.10%	34.00%
13. Increase global outsourcing of IT hardware and software.	39.90%	18.90%	20.30%	14.00%	7.00%	21.00%

Number of Respondents=147

Figure 3



Number of Respondents=147

These tables illustrate a common industry approach to addressing new technological or human factors risks: cryptography and firewalls. Historically, networked ICT have had their defenses initially bolstered by cryptographic solutions and firewalling/intrusion detection as more sophisticated risk management systems and customized/integrated point solutions are designed for explicit markets, verticals, or threats. In this case, 56.50% of respondents view the need for increased availability of FIPS certified cryptographic modules and 56.30% see the need to bolster IT network perimeter defenses in the next year. What's interesting to note is how they value prioritization of enhanced emergency response capabilities (56.20%), increased usage of common criteria compliant products (55.70%), better threat analysis (51.70%), and overcoming internal stovepipes (50.40%) in the next year. We believe this may be representative of a more mature outlook from respondents who, based on their previous experiences in historically stove piped risk domains, feel a need to have increased capability in incident response, visibility into the threat landscape, and widely available commercial-off-the-shelf solutions to mitigate vulnerabilities.

Corporate Supply Chain Risk Management Priority/ For Upcoming Year, by Company Revenue Size

Table 16

Important/ Very Important Priority	Buy/build threat analysis	Overcome IT Stovepipes	Increase collaboration	Move to cloud	Increase sourcing from trusted supplies	Increase global outsourcing
Sales less than $20 million	41.0%	45.5%	39.0%	30.6%	40.2%	14.4%
Sales $100-$1 billion	69.3%	41.7%	50.0%	33.4%	25.0%	25.0%
Sales over $1 billion	81.3%	75.1%	64.7%	62.0%	62.5%	43.8%

Number of Respondents=129: Less than $20 million=100; $100-$1billion=12; Greater than $1 billion=17

"Build or buy threat analysis" is a priority across all sizes of company. Free floating anxiety about IT supply chain risks seems to be hitting across all enterprises, though the biggest companies cite threat analysis as their core supply chain risk management priority in the upcoming year at twice the rate that it is cited by the smallest companies.

Generally, companies seem to feel they do not have enough visibility into threats; there is also concern that government is asking vendors to respond to a cyber-supply chain threat it has not characterized sufficiently. This can breed confusion and anxiety about the scope and specifics of the threat profile and also leads to increased emphasis on defining the actual threat more specifically and practically.

"Overcome IT Stovepipes" is another priority. The vast majority of companies thought it was significant that IT and operations currently do not interact enough and need to interact more to manage supply chain-wide risk.

The biggest companies are moving much faster to the cloud: 62% said it was important/very important priority for the upcoming year. Only 30.6% of the smallest companies said moving to the cloud was a priority for them.

Global outsourcing also remains more of a priority for the biggest firms; the biggest companies reported increasing outsourcing as important/very important three times more frequently than was reported by the smallest companies

FISMA, FIPS, and Common Criteria Compliance are also high priorities for the upcoming year. 56.5% of companies believe FIPS is important/very important; 55.7% believe Common Criteria is important/very important; and 43.4% believe FISMA compliance is important/very important. Obviously, compliance is the key to further contracts. But, there is also a call for guidance in these results. People respond to clear signals, such as those provided in standards and seek to

comply with those signals for many self-interested reasons, such as desire for future profit or shelter from future liability claims.

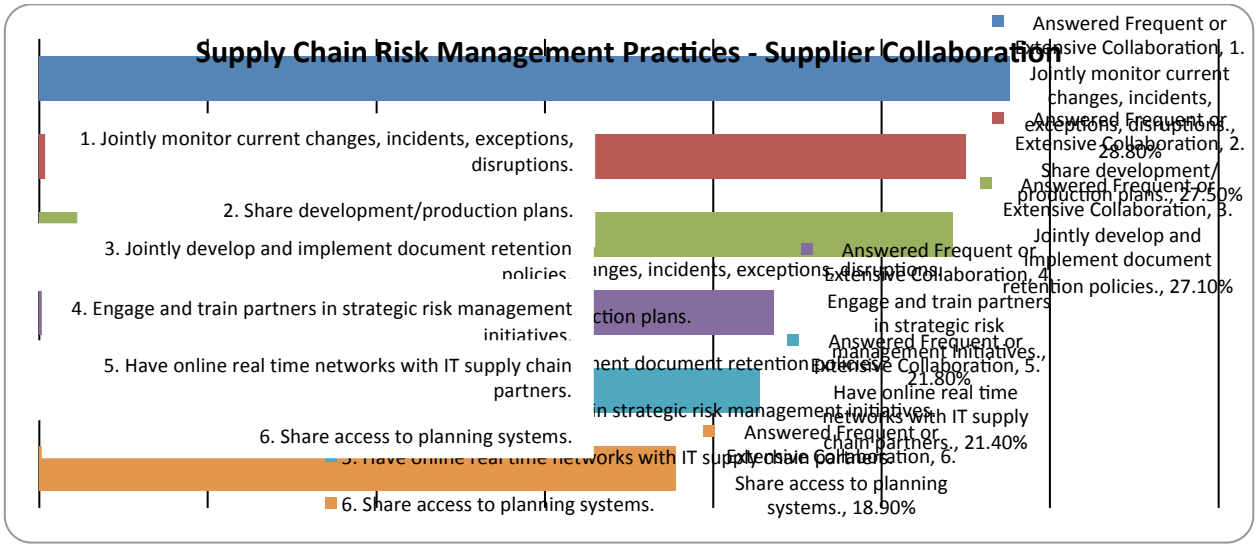
To what extent do you collaborate and organizationally integrate the following activities with your suppliers across the IT supply chain?

Table 17

Items	No Collaboration	Little Collaboration	Moderate Collaboration	Frequent Collaboration	Extensive Collaboration	Frequent or Extensive Collaboration
1. Jointly monitor current changes, incidents, exceptions, disruptions.	22.70%	17.40%	31.10%	21.20%	7.60%	28.80%
2. Share development/production plans.	22.10%	19.80%	30.50%	21.40%	6.10%	27.50%
3. Jointly develop and implement document retention policies.	24.80%	21.10%	27.10%	21.10%	6.00%	27.10%
4. Engage and train partners in strategic risk management initiatives.	22.60%	24.80%	30.80%	18.80%	3.00%	21.80%
5. Have online real time networks with IT supply chain partners.	23.70%	17.60%	37.40%	15.30%	6.10%	21.40%
6. Share access to planning systems.	28.80%	22.70%	29.50%	17.40%	1.50%	18.90%

Number of Respondents=133

Figure 4



Number of Respondents=133

There is little to no supplier collaboration across many kinds of practices: for example, 51.5% of companies in the pilot sample provide no access to planning systems. Even the most widely accepted practice: jointly monitoring current changes, incidents, exceptions, and disruptions was only cited as an extensively used practice by 28.8% of the sample, less than a third of the respondents.

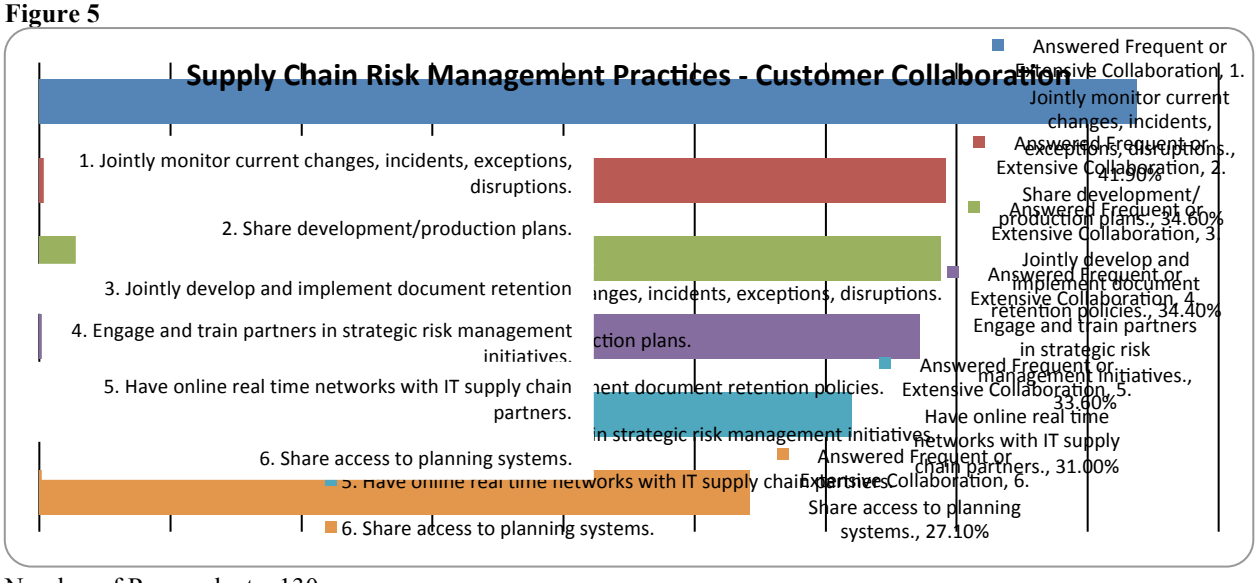
To what extent do you collaborate and organizationally integrate the following activities with your customers across the IT supply chain?

Table 18

Items	No Collaboration	Little Collaboration	Moderate Collaboration	Frequent Collaboration	Extensive Collaboration	Frequent or Extensive Collaboration
1. Jointly monitor current changes, incidents, exceptions, disruptions.	20.90%	11.60%	25.60%	25.60%	16.30%	41.90%
2. Share development/production plans.	15.00%	15.80%	34.60%	26.30%	8.30%	34.60%
3. Jointly develop and implement document retention policies.	22.90%	14.50%	28.20%	23.70%	10.70%	34.40%
4. Engage and train partners in strategic risk management initiatives.	21.60%	17.90%	26.90%	26.90%	6.70%	33.60%
5. Have online real time networks with IT supply chain partners.	21.70%	17.80%	29.50%	22.50%	8.50%	31.00%
6. Share access to planning systems.	22.60%	21.10%	29.30%	24.10%	3.00%	27.10%

Number of Respondents=130

Figure 5



Number of Respondents=130

There is a natural tendency to pay attention to and collaborate more with customers than with suppliers. As support for this statement, 41.9% of the respondents "jointly monitor current changes, incidents, exceptions, disruptions" with customers, far higher than the 28.8% of companies who collaborated on this item with their suppliers frequently or extensively.

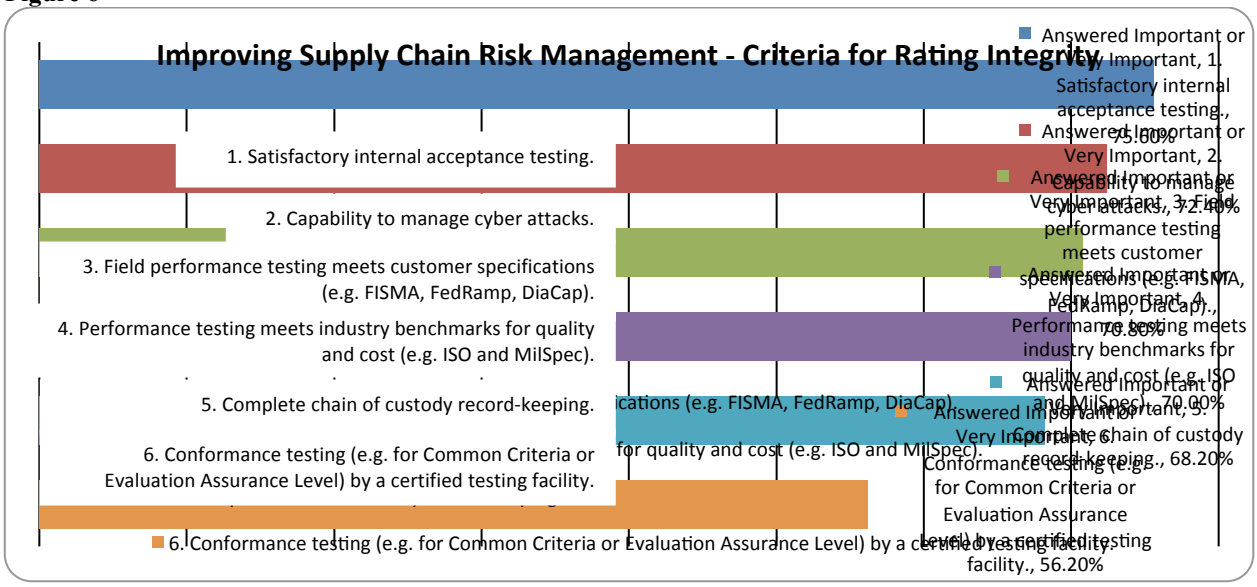
Which of the following criteria do you believe are important to use to rate the integrity of products, components, or services of critical suppliers to the federal government?

Table 19

Items	Unimportant	Of Little Importance	Moderately Important	Important	Very Important	Important or Very Important
1. Satisfactory internal acceptance testing.	3.10%	4.60%	16.80%	35.10%	40.50%	75.60%
2. Capability to manage cyber attacks.	5.40%	4.60%	17.70%	26.20%	46.20%	72.40%
3. Field performance testing meets customer specifications (e.g. FISMA, FedRamp, DiaCap).	5.40%	4.60%	19.20%	33.10%	37.70%	70.80%
4. Performance testing meets industry benchmarks for quality and cost (e.g. ISO and MilSpec).	6.90%	4.60%	18.50%	38.50%	31.50%	70.00%
5. Complete chain of custody record-keeping.	7.00%	6.20%	18.60%	27.90%	40.30%	68.20%
6. Conformance testing (e.g. for Common Criteria or Evaluation Assurance Level) by a certified testing facility.	3.10%	10.80%	30.00%	28.50%	27.70%	56.20%

Number of Respondents=126

Figure 6



Number of Respondents=126

There appears to be broad use of technical assurance testing of systems across all revenue classes. Of course, this tactical emphasis in assuring cyber-supply chains has been an ongoing theme of our results. Importance here is rated most highly for internal capabilities first (internal acceptance testing & capability to manage cyber attacks), customer capabilities second (field performance testing & industry benchmarks), supply chain capabilities third (complete chain of custody record keeping) and capabilities of their third parties/independent validators last (conformance testing by certified testing facility). This too is in-line with previous observations from the data showing a clear incentive/relationship structure which diminishes as you move from the enterprise to the customer and out to suppliers and then third parties.

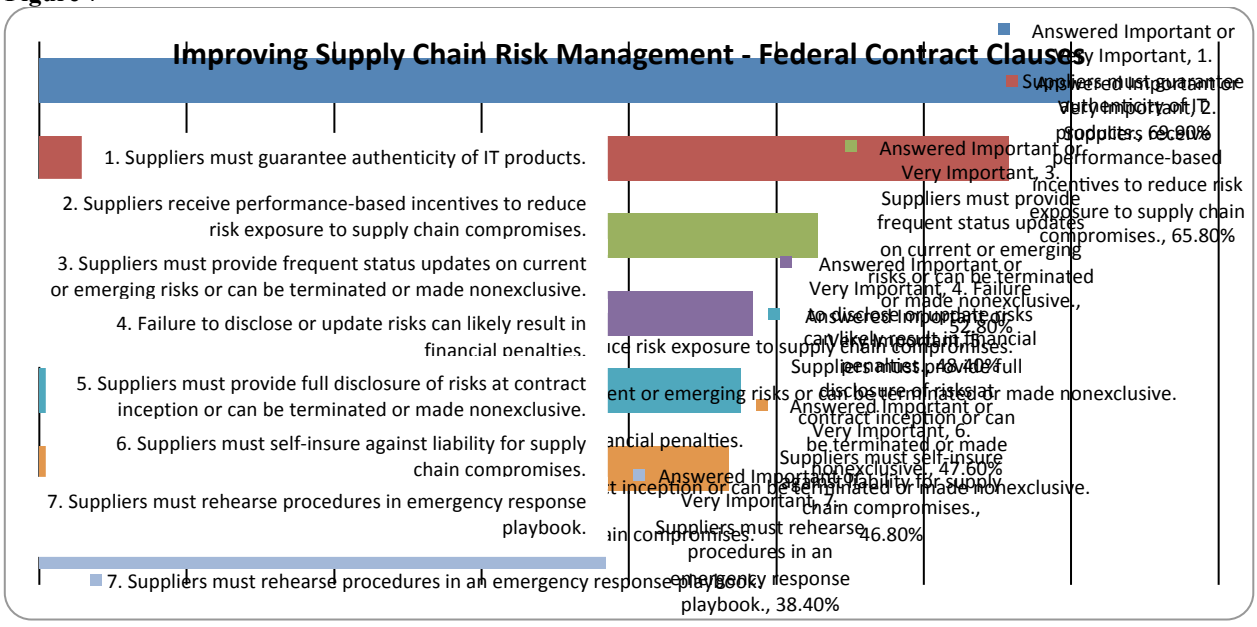
Which of the following clauses do you believe are important to specify in federal contracts to assure effective IT supply chain risk management?

Table 20

Items	Unimportant	Of Little Importance	Moderately Important	Important	Very Important	Important or Very Important
1. Suppliers must guarantee authenticity of IT products.	7.10%	4.00%	19.00%	30.20%	39.70%	69.90%
2. Suppliers receive performance-based incentives to reduce risk exposure to supply chain compromises.	7.90%	6.30%	19.80%	32.50%	33.30%	65.80%
3. Suppliers must provide frequent status updates on current or emerging risks or can be terminated or made nonexclusive.	7.20%	7.20%	32.80%	28.00%	24.80%	52.80%
4. Failure to disclose or update risks can likely result in financial penalties.	8.70%	8.70%	34.10%	20.60%	27.80%	48.40%
5. Suppliers must provide full disclosure of risks at contract inception or can be terminated or made nonexclusive.	8.10%	12.10%	32.30%	25.80%	21.80%	47.60%
6. Suppliers must self-insure against liability for supply chain compromises.	11.30%	10.50%	31.50%	27.40%	19.40%	46.80%
7. Suppliers must rehearse procedures in an emergency response playbook.	14.40%	13.60%	33.60%	22.40%	16.00%	38.40%

Number of Respondents=124

Figure 7



Number of Respondents=124

The most highly ranked item to include in a Federal contract was "suppliers must guarantee authenticity of IT products" (69.9%). Is the federal government focus on authenticity in the current environment (as signaled by a notice to proposed rulemaking) driving attention to ensuring authenticity? Is the government marketing effort working? Based on the results from the respondents, this appears to be the case.

The second most highly ranked item for inclusion was "suppliers receive performance-based incentives to reduce risk" (65.8%). Market and performance-based incentive mechanisms need a lot more attention as a lever to gain broad social compliance to a Cyber-Supply Chain Code of Practice, based on these survey results.

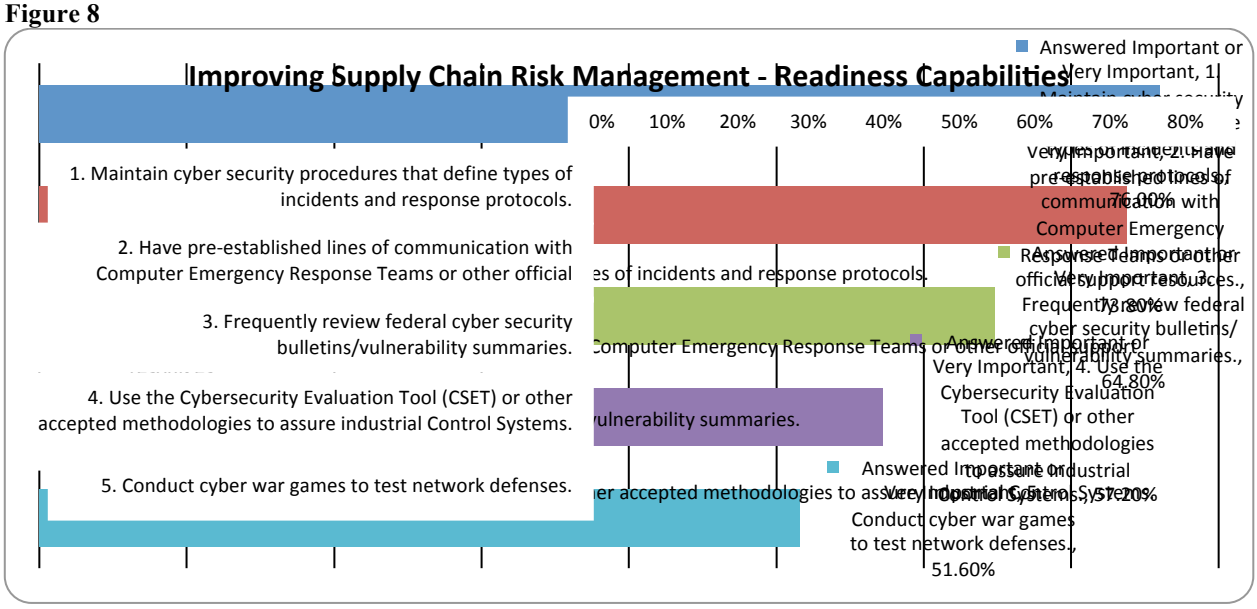
Which of the following readiness capabilities are important in IT security emergency response?

Table 21

Items	Unimportant	Of Little Importance	Moderately Important	Important	Very Important	Important or Very Important
1. Maintain cyber security procedures that define types of incidents and response protocols.	2.40%	3.20%	18.40%	33.60%	42.40%	76.00%
2. Have pre-established lines of communication with Computer Emergency Response Teams or other official support resources.	4.80%	6.30%	15.10%	25.40%	48.40%	73.80%
3. Frequently review federal cyber security bulletins/vulnerability summaries.	3.20%	9.60%	22.40%	31.20%	33.60%	64.80%
4. Use the Cybersecurity Evaluation Tool (CSET) or other accepted methodologies to assure Industrial Control Systems.	10.30%	8.70%	23.80%	31.00%	26.20%	57.20%
5. Conduct cyber war games to test network defenses.	10.20%	13.30%	25.00%	28.90%	22.70%	51.60%

Number of Respondents=126

Figure 8



Number of Respondents=124

"Maintaining cyber-security procedures" was picked as an important/very important readiness capability by 76% of the respondents, indicative of a generalized high threat awareness that drives companies to devise and maintain defensive procedures. 73.8% of respondents think having pre-established communications in place with official cyber support resources is important/very important, suggesting that companies know they need help and they are not hesitant to seek out and accept help. 64.8% think frequently reviewing federal bulletins and vulnerability summaries is important/very important. Companies are looking constantly at government cyber-supply chain messaging to try to clarify the threat and to try to learn what to do about it.

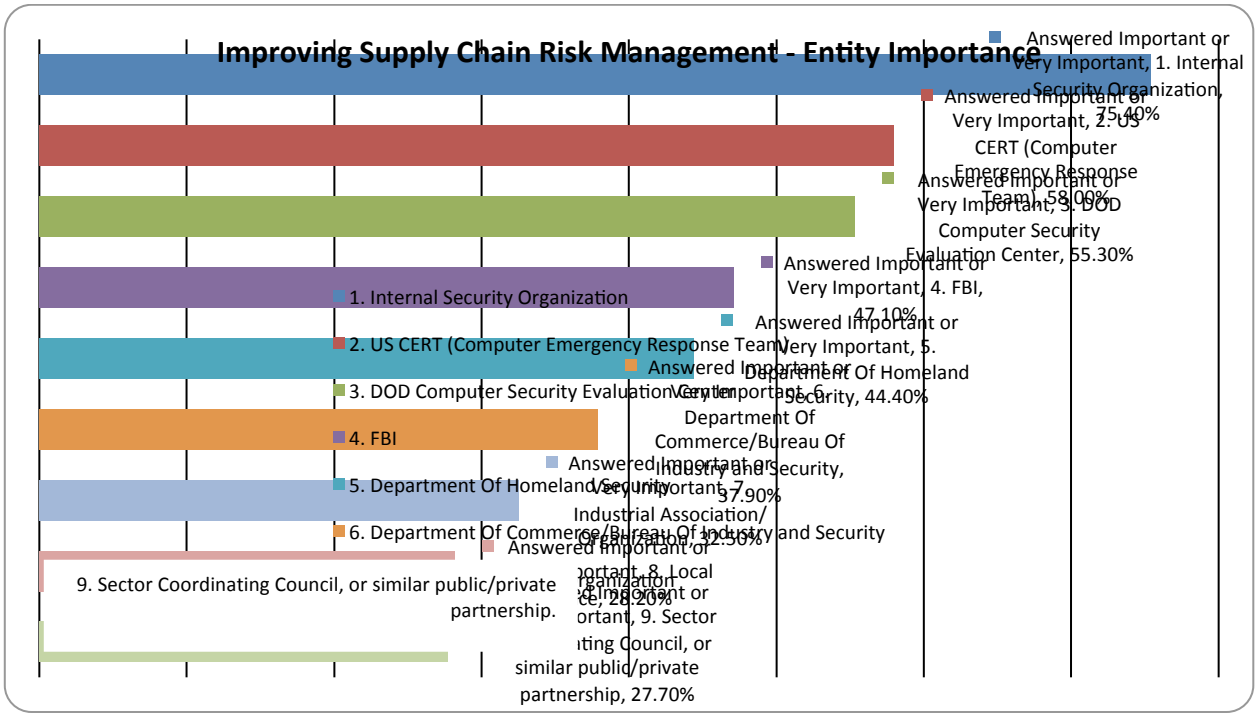
How would you rate the importance of each of the following entities in responding to a serious threat to your IT supply chain?

Table 22

Items	Unimportant	Of Little Importance	Moderately Important	Important	Very Important	Answered Important or Very Important
1. Internal Security Organization	4.10%	2.50%	18.00%	19.70%	55.70%	75.40%
2. US CERT (Computer Emergency Response Team)	8.10%	9.70%	24.20%	27.40%	30.60%	58.00%
3. DOD Computer Security Evaluation Center	9.80%	15.40%	19.50%	29.30%	26.00%	55.30%
4. FBI	8.90%	15.40%	28.50%	26.80%	20.30%	47.10%
5. Department Of Homeland Security	10.50%	18.50%	26.60%	19.40%	25.00%	44.40%
6. Department Of Commerce/Bureau Of Industry and Security	12.90%	22.60%	26.60%	18.50%	19.40%	37.90%
7. Industrial Association/Organization	17.10%	22.80%	27.60%	20.30%	12.20%	32.50%
8. Local Police	15.30%	29.00%	27.40%	16.10%	12.10%	28.20%
9. Sector Coordinating Council, or similar public/private partnership	17.10%	30.90%	24.40%	17.10%	10.60%	27.70%

Number of Respondents=124

Figure 9



Number of Respondents=124

It appears that respondents rely first and foremost on their own internal security organizations. Also there is a *major corporate focus on software breaches* e.g. there is an emphasis on seeking out CERT assistance; *but not a lot on hardware* which would require companies to seek out FBI and Department Of Commerce assistance.

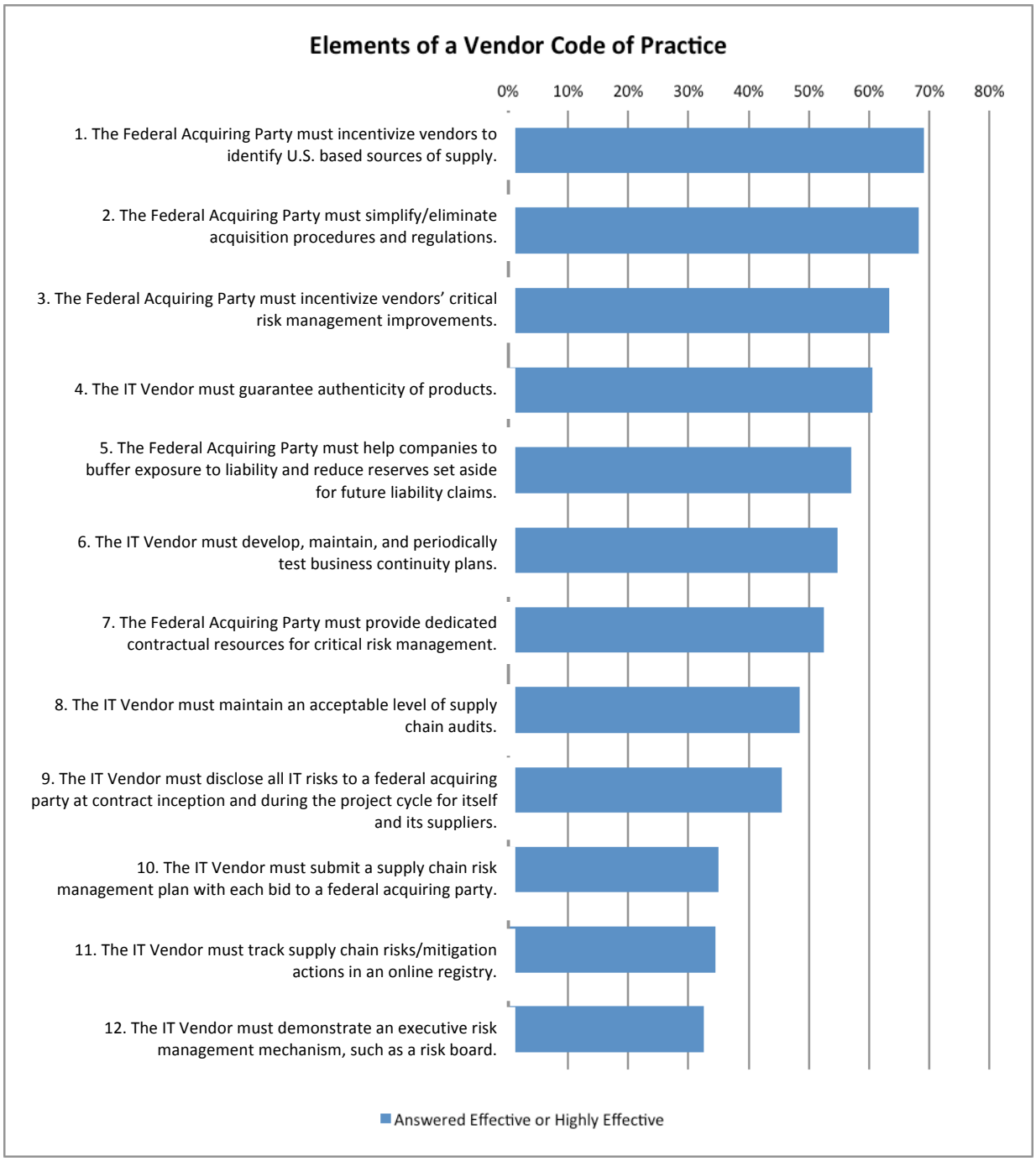
Please rate the attractiveness of each item below for potential inclusion into a Federal Code of Practice for IT Vendors that seeks to improve supply chain risk management?

Table 23

Items	Ineffective	Rarely Effective	Moderately Effective	Effective	Highly Effective	Answered Effective or Highly Effective
1. The Federal Acquiring Party must incentivize vendors to identify U.S. based sources of supply.	5.80%	7.50%	17.50%	30.80%	38.30%	69.10%
2. The Federal Acquiring Party must simplify/eliminate acquisition procedures and regulations.	5.00%	10.00%	16.70%	38.30%	30.00%	68.30%
3. The Federal Acquiring Party must incentivize vendors' critical risk management improvements.	7.30%	7.30%	22.00%	30.90%	32.50%	63.40%
4. The IT Vendor must guarantee authenticity of products.	4.80%	8.10%	26.60%	29.00%	31.50%	60.50%
5. The Federal Acquiring Party must help companies to buffer exposure to liability and reduce reserves set aside for future liability claims.	10.90%	15.10%	16.80%	31.90%	25.20%	57.10%
6. The IT Vendor must develop, maintain and periodically test business continuity plans.	10.50%	9.70%	25.00%	29.00%	25.80%	54.80%
7. The Federal Acquiring Party must provide dedicated contractual resources for critical risk management.	12.30%	9.80%	25.40%	32.80%	19.70%	52.50%
8. The IT Vendor must maintain an acceptable level of supply chain audits.	10.50%	13.70%	27.40%	28.20%	20.20%	48.40%
9. The IT Vendor must disclose all IT risks to a federal acquiring party at contract inception…	13.80%	13.00%	27.60%	30.10%	15.40%	45.50%
10. The IT Vendor must submit a supply chain risk management plan with each bid to a federal acquiring party.	14.60%	19.50%	30.90%	23.60%	11.40%	35.00%
11. The IT Vendor must track supply chain risks/mitigation actions in an online registry.	15.60%	18.90%	31.10%	22.10%	12.30%	34.40%
12. The IT Vendor must demonstrate an executive risk management mechanism, such as a risk board.	12.20%	23.60%	31.70%	22.00%	10.60%	32.60%

Number of Respondents=124

Figure 10



Number of Respondents=124

Attractiveness of Code Of Practice Elements, By Company Revenues

Table 24

Practice Effective/Highly Effective	Risk Board	Risk Plan	Risk Disclosure	Priority Status rating for IT Vendors who improve SCRM	Fed acquirer must provide additional contractual resource for SCRM	Help companies reduce capital reserves set aside to cover liability and risk	Streamline regulations and standards
Sales less than $20 million	24.7%	33.3%	40.5%	57.2%	50.6%	52.4%	63.5%
Sales $100 million-$1 billion	30%	30%	50%	70%	30%	77.8%	87.5%
Sales above $1 billion	50%	41.7%	58.3%	91.7%	66.6%	72.8%	81.8%

Number of Respondents=106: Less than $20 million=84; $100-$1billion=10; Greater than $1 billion=12

Clearly, there is a distinct and close correlation: the greater the corporate revenue, the greater the corporate support for Code of Practice elements that are strategic in scope, e.g. Risk Boards and Risk Plans.

Also, the largest companies are especially interested in obtaining government-designated favored supplier status: 91.7% of them rated priority status as the most effective/highly effective potential Code element as compared to 57.2% of the smallest companies.

There was across the board support for inclusion of elements that "provide additional contractual resources for SCRM" and "streamline regulations" into a Code of Practice. So, on one hand, there is a desire for streamlined, less burdensome or obtuse regulations, e.g. get the government off our backs. But, on the other hand, there is widespread support for government actions to clarify:

- What is the real threat?
- What are priority SCRM practices?
- How can expanded use of those practices by companies tie into to real corporate benefits, such as reduction of liability and overall compliance costs?

Successfully answering the latter question is crucial for successful adoption of a Cyber-Supply Chain Code of Practice and requires that much more cost/benefit analysis work be done. We will discuss this point further in our next section.

Overall, respondents had a lot to say about developing a Cyber-Supply Chain Code of Practice as evidenced by the diversity of their comments:

The IT Vendor must:

- Be held to a higher standard
- Make a CEO-level commitment to a list of security practices in any software development project
- Not declare as proprietary the solution details and integration technology used to meet public requirements
- Establish protocols and operate with full visibility for control and accountability
- "Demonstrate the effectiveness of products, and test results which are reasonable
- Be reasonably flexible to incorporate unforeseen contingency need into contracts
- Comply with all applicable United States laws and regulations, and all country of origin laws and regulations
- Disclose a summary of the processes and mechanisms used to ensure the authenticity and integrity of products
- Get Common Criteria, FIPS and Section 508 certified
- Be capable of maintaining a comprehensive assessment and reporting program utilizing resources available
- Provide training, support through the systems life cycle development
- Validate all pieces/parts of their product line and for software map the signatures to a centralized board

V. Conclusions/Next Steps

As just analyzed in detail in the Results Section, we found that there were a few key themes in the findings:

Both Large & Small Companies Seriously Under-Manage Cyber-SCRM

Both small and big companies work across hardware and software development, network management and integration service boundaries and have multiple product/service offerings e.g. these companies are themselves complex, integrated supply chains.

Given this complexity, the general lack of holistic supply chain management thinking; the silo'd nature of risk, cyber and supply chain/ operations functions inside corporations of all sizes; and the development of process-models and technical solutions only within narrow stovepipes presents a grave threat to managing systemic risk in cyber-supply chains.

Both Large & Small Companies Can Be Incentivized To Improve Cyber-SCRM

Small companies are highly motivated to get and use government cyber-supply chain risk management practice guidelines. This helps them to win business with the federal acquirer community; as well as to conserve scarce dollars and management time that they would otherwise have to spend themselves on cyber security compliance research.

Although their cyber units are not well integrated into or supported by corporate risk management programs, big companies are nevertheless highly sensitive to managing regulatory demands for risk assurance and seeking to limit their own corporate liability.

This sensitivity to risk has certainly been motivating in other non-IT industries developing Codes Of Practice, such as the chemical industry (Responsible Care) and the consumer products industry (SCOR). Also, big companies are well tuned to try and use supply chain assurance as a competitive weapon. For example, in the food industry, companies such as the spice company McCormack routinely use superior food safety/chain of custody capabilities to win out against competitors.

These findings lead us to emphasize further development activities that seek to achieve a few key objectives:

- **Build The Body Of Knowledge**
  Dig deeper into the dynamics of Cyber-SCRM and add to the Body of Knowledge thru further, larger data-collection efforts. DOC/NIST, DOC/BIS, GSA, DHS, DOD/CIO, DOD/NSA can all individually or collectively distribute our validated questionnaire in a much more formal way to a broader, more motivated sample. *We have only begun to collect reality-based "facts on the ground" from the frontlines of industry.*

- **Develop A Code Of Practice Prototype & An Associated Incentives Strategy**
  Our limited research results have made abundantly clear the need for consensus best

practices guidance to corporations e.g. a dynamic code of practice and an incentives strategy to help promote diffusion of the code. This guidance can come from the federal government itself; from a respected IT industry consortium that can bring together IT industry segments into a unified and holistic supply chain approach and compile & constantly update best practices across the hardware, software, network management and systems-integration segments; or-perhaps best of all- a federal/industry partnership group that can address both the government's IT security requirements and industry's implementation challenges.

There is a great need not only for research on key practices but also on incentives and rewards for compliance.

Research interviews with Chief Financial officers, Chief Risk Officers/ Legal Counsels, Chief Information Officers and Chief Supply Chain Officers, as well as Insurance Industry Experts should be conducted to:

- Help understand how to accelerate the alignment of these executive roles & functions into an integrated, holistic cyber-supply chain governance structure and how to support that alignment through a code of practice

- Identify the best regulatory/incentive levers available to assure maximum diffusion of and compliance with such a code.

Such levers might include: defining liability and liability limits in cyber-supply chains; recommending ways to do industry risk pooling and free up company-level capital reserves currently held for future liability claims and uninsurable risk; or legislative/regulatory modifications that are perceived to ease industry compliance costs.

These scientifically validated incentive structures would then be compared to the results collected by NIST from the CNCI Initiative 11 Pilots executed in compliance with NIST IR 7622 to create a fully validated public/private incentive structure and practice effectiveness model.

All these inputs could serve to build a Monte Carlo Simulation and basic Cost/Benefit Model that would provide the federal and private sectors with data on how a Cyber-Supply Chain Code of Practice might impact their bottom lines.

Research interviews should also be conducted with stakeholder associations of small and large IT vendors; general business advocacy groups, such as the Chamber of Commerce; and federal users of IT.

Taken together, all these interviews could serve as inputs into a national, industry-wide code of practice.

Federal guidance and clarification of key code of practice elements might become much more important in an environment of increasing state-level cyber security activism.

For example Texas Administrative Code, Title 1, Part 10, Chapter217, Subchapter B, Rule § 217.12) became effective in December, 2010 and specifies that all IT vendors must certify that the network hardware or software, as applicable, procured or leased under state contract, has undergone independent certification testing for known and relevant vulnerabilities. The required independent certification testing of network hardware or software for vulnerabilities must be conducted against established standards.

A national, industry-wide code of practice would help avoid the growth of a patchwork of repetitive or conflictive state codes of practice and testing.

- **Convene Two Stakeholder Summits**
  Based on research activities above, convene two stakeholder summits.

  Summit #1

  The first such summit could include representatives from across the cyber-supply chain:

  - Software trade groups e.g. Safecode, etc.
  - Hardware trade groups e.g. Supply Chain Risk leadership Council (a consortium of high tech electronics manufacturers) and the Supply Chain Council (Supply Chain Operations Reference Model consortium)
  - Network Management industry groups e.g. IEEE and *Telecommunications Industry Association*
  - Systems-Integration industry groups e.g. NDIA; Open Group

- Risk Governance industry groups e.g.

    a. PRMIA. (The Professional Risk Managers' International Association (PRMIA) is a non-profit professional association, governed by a Board of Directors directly elected by its global membership, of more than 75,186 members in 201 countries. PRMIA is represented globally by 60 chapters in major cities around the world, led by Regional Directors appointed by PRMIA's Board)

    b. ISACA (the international IT and information systems organization that offers certification in risk and information system control).

    c. RIMS (http://www.rims.org/Pages/Default.aspx). The Risk and Insurance Management Society, Inc. (RIMS) is a not-for-profit organization dedicated to advancing the practice of risk management. Founded in 1950, RIMS represents more than 3,500 industrial, service, nonprofit, charitable and governmental entities. The Society serves more than 10,000 risk management professionals around the world.

The agenda of Summit #1 might include discussion of the Code of Cyber-Supply Chain Practice Prototype Model; possible adoption of a code as a condition of membership by these stakeholder associations and their members; possible incentives for adoption; insurance and liability/warranty schema and identification of next steps to refine and finalize a consensus code.

Summit #2

The second summit would include a series of workshops designed to bring Tier 1 product vendors and integrators together with critical nodes in their own supply chains to take a more holistic view.

- 10-15 Tier 1 Product Vendors & Integrators
    - 5-10 critical supply chain nodes for each
    - 2-3 critical distributers or VARs

The agenda of Summit#2 might include:

- A table-top exercise to game out cyber supply chain incident response and management practices and develop best practices & lessons learned.

- perspectives from the legal community on liability, warranty, transfer of risk, and the regulatory landscape to include a working session on globalizing a code of practice

- Standards harmonization. Participation from a number of leading government agencies, standards bodies, and non-profits/NGOs to convene the first ever summit of all parties. This could include DoD, NIST, DHS, GSA, NSA, ISO/IEC, ISA, Open Group, AGMA, HIS Initiative, NIAP, UL, and others.

To Conclude:

The cyber supply chain discipline is currently in an early emerging state characterized by: a deficient evidence-based body of knowledge; a proliferation and fragmentation of industry best practices and standards groups, generally led by the largest firms; and a profound under-usage of supply chain-wide risk governance mechanisms inside IT vendors.

Despite the spread of in-depth but narrow technical standards, companies are clearly not adequately addressing systemic risks.

Going forward, we believe that NIST- which is widely perceived by industry as a neutral entity charged with promoting commerce-has a special role to play in brokering a consensus Cyber Supply Chain Code of Practice that can win wide support among diverse IT stakeholders.

Appendix 1:
Questionnaire and Completed Results

Controlling Supply Chain Risk: An IT Vendor Survey

Introduction

You have been identified as an IT vendor who will likely be affected by new Federal procurement and supply chain risk management (SCRM) policies, rules, and standards set for release in 2011.

The National Institute of Standards and Technology (NIST) has been charged by the Administration to lead this development effort and has tasked the Robert H. Smith School of Business at the University of Maryland to urgently survey the IT vendor community on the best ways to make these policies, rules, and standards effective and efficient. The attached survey seeks your views on the recommendations currently being considered for near term implementation.

NIST is already formulating initial policies and, in cooperation with GSA, pilot testing related procurement language:

- NIST is set to release its policy advisory (NISTIR 7622 "Piloting Supply Chain Risk Management Practices for Federal Information Systems") in the spring of 2011.

- GSA now requires submission of supply chain risk management plans as part of the Managed Trusted Internet Protocol Service (MTIPS) procurement.

Now is the time to act: as an IT executive who is a current or future supplier to the federal government, you have a crucial voice in helping make these new federal procurement and SCRM policies effective and efficient.

Simply follow the instructions provided and fill out the survey by yourself; or share it with colleagues in your company who can help fill in the questions that cover the areas of cyber security, operations/supply chain, and risk management.

All answers will be kept strictly confidential and only aggregate, anonymous results will be disclosed as part of the survey recommendations.

All answers will be kept strictly confidential and only aggregate, anonymous results will be disclosed as part of the survey recommendations.

Survey results will be compiled and recommendations presented to NIST and GSA by March 31, 2011 for possible incorporation into final policies, rules, and standards. The full results of this

survey will be made available to all respondent companies in a White Paper in spring 2011. You will be notified by e-mail and provided a link to download the White Paper when it is available.

Thank you for your consideration and participation.

Definitions Used

A. IT Vendor: Any company that is presently engaged in selling information/communications technology systems, products, and services to the federal government; or is planning to do so in the near future.

B. IT Supply Chain: The set of IT companies engaged in coordinating the development and deployment of a system, product, or service for a federal acquiring party.

C. Key IT Supply Chain Actors: We have identified the following key actors in the IT supply chain ecosystem. As a respondent to this survey, you will likely fit into one of these roles:

- *Acquisition Specialists* who seek to acquire IT goods and services for their organizations
- *System Integrators* who act as tier I coordinators of cross-vendor products and services
- *Software Developers* who must manage software pedigree, code integrity, and kernel evaluation assurance levels
- *Hardware/Component Developers* who must manage tier II suppliers, assure the quality of both production and embedded software/logic needed to operate the hardware, and guard against counterfeits entering the system
- *Network Providers* who supply the bandwidth and connectivity for data, video and voice communications
- *Hosted/Cloud Application Providers* who offer on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released

D. Supply Chain Risk Management: The set of risk identification and mitigation activities undertaken by a single company or group of companies working together to limit the incidence of hardware counterfeits and malware, software vulnerabilities, and network intrusions across the supply chain.

E. Supply Chain Risk Management Plan: A formal management plan to identify and mitigate risks in the IT supply chain.

Basic Survey Instructions

Recommended web browsers: Microsoft Internet Explorer (PC), Mozilla Firefox (PC), Google Chrome (PC), Safari (Mac).

In order to progress through this survey, please use the following navigation buttons:

- Click the Next button at the bottom of the current page to continue to the next page

- Click the Back button at the bottom of the current page to return to the previous page

- Click the Submit button at the bottom of the final page to complete the survey

We are striving for a holistic view of your company. Completing this survey may require input from managers in your organization with knowledge of IT security, supply chain management/operations, and risk management. For this reason, we have made it easy for you save the survey and then return to where you left off at a later point in time or have a colleague access any individual section of the survey.

In order to save your progress so that you can return to where you left off in the survey at a later point in time, please follow these instructions:

1. Click the Save and Continue Survey Later link at the top of the current page.

2. Please supply your email address and click the "save" button. A unique link will be emailed to you that will allow you to return to the survey at your convenience. Your answers will be saved up to the page where you paused. To ensure data is saved on the current page, use the Save and Continue Survey Later link on the next page.

In order to save your progress so that a colleague can access any individual section of the survey, please follow these instructions:

1. Click the Save and Continue Survey Later link at the top of the current page.

2. Please supply a colleague's email address and click the "save" button.

3. A unique link will be sent to the email address specified that will allow your colleague to return to the survey at his or her convenience. This email to your colleague will be sent by SurveyGizmo. It is important you also contact your colleague to let him or her know they will be receiving an email from SurveyGizmo and they need to help you complete the survey.

4. The saved survey will begin on the page where the survey was most recently paused. It is strongly recommended you let your colleague know the specific question numbers where

input is needed. Your colleague may need to use the Next or Back buttons at the bottom of the survey pages to navigate to
these questions.

5. Your colleague should be instructed to use the Save and Continue Survey Later link at the top of the next page once he or she completes the desired questions to send the survey back to your email address.

Your time is valuable and we appreciate your participation. Thank you!

Please contact Dr. Sandor Boyson or Dr. Thomas M. Corsi with any questions:

Dr. Sandor Boyson
Research Professor and Co-Director,
Supply Chain Management Center

Robert H. Smith School of Business
Supply Chain Management Center
3355 Van Munching Hall
College Park, MD 20742
Phone: 301-405-2205
E-mail: sboyson@rhsmith.umd.edu

Dr. Thomas M. Corsi
Michelle E. Smith Professor of Logistics and Co-Director,
Supply Chain Management Center

Robert H. Smith School of Business
Supply Chain Management Center
3321 Van Munching Hall
College Park, MD 20742
Phone: 301-405-2197
E-mail: tcorsi@rhsmith.umd.edu

Section I:
Company Profile

1) What most accurately describes your company job title? (Check one)
(11%) Director/Associate Director/Manager, Supply Chain Management
(15.9%) Director/Associate Director/Manager, Procurement/Acquisition
(7.6%) Director/Associate Director/Manager, Product Engineering
(50.3%) Director/Associate Director/Manager, Information Technology
(3.4) Director/Associate Director/Manager, Telecom Services
(9.7%) Director/Associate Director/Manager, Information Security
(2.1%) Director/Associate Director/Manager, Risk Management

2) Please provide the following information:
Company Name: _____
Address: _____
City: _____
State: _____
Zip Code: _____
Country: _____
Web Address (URL): _____

3) How large is your company? (Check one)
(71.0%) Annual sales less than $20 million
(7.0%) Annual sales between $20-$50 million
(5.5%) Annual sales between $50-$100 million
(6.3%) Annual sales between $100-$1 billion
(10.3%) Annual sales greater than $1 billion

4) Does your company provide: (Check all applicable items)
[48.6%] Software
[31.4%] Hardware
[62.4%] Systems Integration Services
[24.8%] Telecom/Data Network Provisioning
[27.2%] Hosted/Cloud Applications
[33.8%] Other, please specify:

- Security Support Services
- Process Improvement
- Discrete switches
- Critical Power & Cooling Data Centers

- Business Continuity
- Consulting Services
- Consumable supplies
- Technology and capital strategy
- Business Development
- IT Infrastructure Management
- Information Security
- Software implementation and project management
- Logistics and Engineering Services
- Auto CAD & Auto Quotes
- Custom software development
- SOA, Enterprise Architecture, BI & EDW, Program Management
- Auditing, Policy Development
- Engineering, Program Management, Training and Logistics
- Independent Verification and Validation
- IT-Disaster Recovery services
- Backup, recovery & restore
- BPO Services
- Conferencing Services
- Threat Intelligence
- Scientific studies

5) Does your company <u>currently</u> supply IT products/services to the federal government?

(86.9%) Yes
(13.1%) No

6) Is your company planning to supply the federal marketplace?
(86.8%) Within the next year
(6.8%) Within the next three years
(6.4%) No plans to enter the market

Section II:
Supply Chain Risk Management Practices

7) Below are higher level practices some companies are using to try to manage IT supply chain risk. For each of these practices, rate the extent of its current use in your own organization:

	Never	Seldom	Sometimes	Often	Always
A C-Suite Risk Board to help govern risk and IT supply chains.	(47.6%)	(16.9%)	(16.9%)	(12.0%)	(6.6%)
A Cyber Supply Chain Risk Management Plan.	(44.9%)	(9.6%)	(21.0%)	(12.0%)	(12.6%)
A formal risk registry, a shared online database of IT supply chain risks.	(46.1%)	(15.0%)	(22.8%)	(9.0%)	(7.2%)
An integrated IT supply chain dashboard/control panel.	(49.4%)	(9.6%)	(16.9%)	(15.7%)	(8.4%)
An integrated IT supply chain life cycle testing/assurance approach.	(35.8%)	(6.7%)	(18.8%)	(20.0%)	(18.8%)
Enhanced perimeter defense systems to detect intrusions.	(23.2%)	(4.3%)	(15.2%)	(19.5%)	(37.8%)
A standardized process for pre-qualifying suppliers.	(17.3%)	(8.3%)	(25.0%)	(20.8%)	(28.6%)
Vendor security audits and tough contractual mandates/penalties for security violations.	(29.4%)	(14.1%)	(19.0%)	(17.8%)	(19.6%)
Corporate-wide capabilities in cyber security emergency response.	(21.8%)	(12.1%)	(18.8%)	(17.0%)	(30.3%)
Personnel security reviews.	(9.7%)	(8.5%)	(14.5%)	(21.2%)	(46.1%)

8) Below are higher level practices some companies are using to try to manage IT supply chain risk. For each of these practices, rate its actual or perceived effectiveness (or helpfulness) in managing risk in your extended supply chain:

	Ineffective	Somewhat Effective	Moderately Effective	Effective	Highly Effective

A C-Suite Risk Board to help govern risk and IT supply chains.	(28.9%)	(20.4%)	(20.4%)	(21.8%)	(8.5%)
A Cyber Supply Chain Risk Management Plan.	(21.5%)	(18.1%)	(23.6%)	(25.0%)	(11.8%)
A formal risk registry, a shared online database of IT supply chain risks.	(20.7%)	(12.4%)	(28.3%)	(23.4%)	(15.2%)
An integrated IT supply chain dashboard/control panel.	(26.2%)	(7.6%)	(24.8%)	(27.6%)	(13.8%)
An integrated IT supply chain life cycle testing/assurance approach.	(17.7%)	(7.5%)	(20.4%)	(32.7%)	(21.8%)
Enhanced perimeter defense systems to detect intrusions.	(12.8%)	(6.0%)	(14.1%)	(33.6%)	(33.6%)
A standardized process for pre-qualifying suppliers.	(9.4%)	(4.7%)	(19.5%)	(37.6%)	(28.9%)
Vendor security audits and tough contractual mandates/penalties for security violations.	(13.0%)	(10.3%)	(18.5%)	(32.9%)	(25.3%)
Corporate-wide capabilities in cyber security emergency response.	(14.5%)	(6.2%)	(20.7%)	(28.3%)	(30.3%)
Personnel security reviews.	(6.7%)	(8.0%)	(20.0%)	(33.3%)	(32.0%)

9) How important a corporate priority for the upcoming year is each of these supply chain risk management actions?

	Unimportant	Of Little Importance	Moderately Important	Important	Very Important
Build or buy better IT threat analysis capabilities.	(9.5%)	(10.9%)	(27.9%)	(31.3%)	(20.4%)
Overcome internal stovepipes between IT security and operations.	(11.7%)	(11.7%)	(26.2%)	(29.0%)	(21.4%)
Mandate increased collaboration with extended supply chain partners/vendors.	(10.2%)	(9.5%)	(32.7%)	(32.7%)	(15.0%)
Bolster IT network "perimeter defenses" through enhanced intrusion detection systems.	(11.1%)	(8.3%)	(24.3%)	(30.6%)	(25.7%)
Move IT applications and transactions to the cloud.	(18.1%)	(17.4%)	(30.6%)	(22.9%)	(11.1%)
Increase global outsourcing of IT hardware and software.	(39.9%)	(18.9%)	(20.3%)	(14.0%)	(7.0%)
Increase sourcing from pre-certified "trusted" vendors of IT hardware and software.	(11.2%)	(11.9%)	(30.8%)	(33.6%)	(12.6%)
Better pre-screen software code or hardware sourced from offshore prior to incorporation into domestic IT systems.	(22.0%)	(9.9%)	(19.1%)	(27.7%)	(21.3%)
Design and implement improved performance monitoring systems to manage your suppliers' risks.	(15.0%)	(10.7%)	(31.4%)	(27.1%)	(15.7%)
Push for expanded Federal Information Security Management Act (FISMA) compliance of critical IT systems, products or services sold to federal government.	(14.0%)	(11.2%)	(31.5%)	(23.1%)	(20.3%)
Compliance with Common Criteria for general security of systems, products and services.	(6.3%)	(8.5%)	(29.6%)	(27.5%)	(28.2%)
Compliance with Federal Information Processing Standards (FIPS) for certification of cryptographic features of systems, products and services.	(10.9%)	(8.7%)	(23.9%)	(27.5%)	(29.0%)
Accelerate IT emergency response capabilities.	(6.9%)	(9.0%)	(27.8%)	(31.9%)	(24.3%)

10) Please specify any other supply chain risk management action that is a corporate priority for the upcoming year:

- Physical Security
- Eliminate holes in the supply chain

- Common sense systems monitoring and vendor surveillance
- Vet out foreign supplier
- Database platform in which software is hosted, and integration methodology
- Increased Cyber Security and Device specific security at the wireless access point vs. core concentration
- Consolidation of Subcontractor/Vendor performance information
- Eliminate unnecessary bottlenecks in the supply chain process.
- More supply chain risk analysis that encompasses the risks associated both internally and externally
- Eliminate offshore resources
- Common and uniform FISMA C&A process, FedRAMP
- Audit and improve current SCRM policies and processes
- Integrating our supply chain risk practices into the Business Continuity Maturity Model
- Simplify and standardize risk profile/disclosure/reporting format and methodologies
- Separate financial systems used by federal agencies
- Use of primary federal risk controls for private and government programs
    1) Prescreen software code or hardware from domestic sourcing;
    2) Process for prescreening integrated software applications
- Electronic Data Interchange, Point of Sale, and Firewalls
- Trusted chains, where results are securely passed through the chain
- Verification testing within the environment

11) To what extent do you collaborate and organizationally integrate the following activities with your <u>suppliers</u> across the IT supply chain?

	No Collaboration	Little Collaboration	Moderate Collaboration	Frequent Collaboration	Extensive Collaboration
Engage and train partners in strategic risk management initiatives.	(22.6%)	(24.8%)	(30.8%)	(18.8%)	(3.0%)
Share access to planning systems.	(28.8%)	(22.7%)	(29.5%)	(17.4%)	(1.5%)
Share development/production plans.	(22.1%)	(19.8%)	(30.5%)	(21.4%)	(6.1%)
Have online real time networks with IT supply chain partners.	(23.7%)	(17.6%)	(37.4%)	(15.3%)	(6.1%)
Jointly monitor current changes, incidents, exceptions, disruptions.	(22.7%)	(17.4%)	(31.1%)	(21.2%)	(7.6%)
Jointly develop and implement document retention policies.	(24.8%)	(21.1%)	(27.1%)	(21.1%)	(6.0%)

12) To what extent do you collaborate and organizationally integrate the following activities with your <u>customers</u> across the IT supply chain?

	No Collaboration	Little Collaboration	Moderate Collaboration	Frequent Collaboration	Extensive Collaboration
Engage and train partners in strategic risk management initiatives.	(21.6%)	(17.9%)	(26.9%)	(26.9%)	(6.7%)
Share access to planning systems.	(22.6%)	(21.1%)	(29.3%)	(24.1%)	(3.0%)
Share development/production plans.	(15.0%)	(15.8%)	(34.6%)	(26.3%)	(8.3%)
Have online real time networks with IT supply chain partners.	(21.7%)	(17.8%)	(29.5%)	(22.5%)	(8.5%)
Jointly monitor current changes, incidents, exceptions, disruptions.	(20.9%)	(11.6%)	(25.6%)	(25.6%)	(16.3%)
Jointly develop and implement document retention policies.	(22.9%)	(14.5%)	(28.2%)	(23.7%)	(10.7%)

Section III:

Perspectives on Improving Supply Chain Risk Management

13) Which of the following criteria do you believe are important to use to rate the integrity of products, components, or services of critical suppliers to the federal government?

	Unimportant	Of Little Importance	Moderately Important	Important	Very Important
Capability to manage cyber attacks.	(5.4%)	(4.6%)	(17.7%)	(26.2%)	(46.2%)
Complete chain of custody record-keeping.	(7.0%)	(6.2%)	(18.6%)	(27.9%)	(40.3%)
Satisfactory internal acceptance testing.	(3.1%)	(4.6%)	(16.8%)	(35.1%)	(40.5%)
Conformance testing (e.g. for Common Criteria or Evaluation Assurance Level) by a certified testing facility.	(3.1%)	(10.8%)	(30.0%)	(28.5%)	(27.7%)
Field performance testing meets customer specifications (e.g. FISMA, FedRamp, DiaCap).	(5.4%)	(4.6%)	(19.2%)	(33.1%)	(37.7%)
Performance testing meets industry benchmarks for quality and cost (e.g. ISO and MilSpec).	(6.9%)	(4.6%)	(18.5%)	(38.5%)	(31.5%)

14) Please specify any <u>other</u> criteria you believe should be used to rate the integrity of products, components or services of critical suppliers to the federal government?

- All should be open-source. This 'trial by fire' will purge systems that are leaky.
- Infrastructure, back-up, Co-location
- Operating costs, punch list completion time and cost, known enhancement time and cost
- Consistent and standardized security protocols updated for technical advances
- Use independent body to carry out testing of components and services, etc
- Other criteria include speed, consistency and integrity of products and services
- Perform an automated code review (i.e., static analysis)
- Disaster Resiliency

- FSIO-compliance
- Definition and acceptance of common baseline criteria with version control that incorporates all aspects
- Development of empirical evidence that support claims of service
- We also consider stability of the product provider. This becomes more of a concern for Open Source
- Acceptance testing by the Federal government
- CMMI, Agility and Scrum Mastering of Products and Costs
- A federal standard for application (database) performance and testing.
- A transparent internal process, and process improvement program that is geared towards product integrity
- NIST should have all IT vendors standards and specification
- Integrated monitoring capability, reporting to known standards, of both operational and security mea

15) Which of the following clauses do you believe are important to specify in federal contracts to assure effective IT supply chain risk management?

	Unimportant	Of Little Importance	Moderately Important	Important	Very Important
Suppliers must provide full disclosure of risks at contract inception or can be terminated or made nonexclusive.	(8.1%)	(12.1%)	(32.3%)	(25.8%)	(21.8%)
Suppliers must provide frequent status updates on current or emerging risks or can be terminated or made nonexclusive.	(7.2%)	(7.2%)	(32.8%)	(28.0%)	(24.8%)
Failure to disclose or update risks can likely result in financial penalties.	(8.7%)	(8.7%)	(34.1%)	(20.6%)	(27.8%)
Suppliers must rehearse procedures in an emergency response playbook.	(14.4%)	(13.6%)	(33.6%)	(22.4%)	(16.0%)
Suppliers must guarantee authenticity of IT products.	(7.1%)	(4.0%)	(19.0%)	(30.2%)	(39.7%)
Suppliers must self-insure against liability for supply chain compromises.	(11.3%)	(10.5%)	(31.5%)	(27.4%)	(19.4%)
Suppliers receive performance-based incentives to reduce risk exposure to supply chain compromises.	(7.9%)	(6.3%)	(19.8%)	(32.5%)	(33.3%)

16) Please specify any <u>other</u> contract clause that should be specified in federal contracts to assure effective IT supply chain risk management.

- Bayh-Dole should be enforced, but with shorter timelines
- More oversight on prime contractors' rather than self certification
- Suppliers must guarantee route diversity for any network-related supply chain products
- Balanced penalties and incentives for fulfilling performance requirements
- Item 15 constitutes typical government efforts to put all performance risk on the Contractor
- Government regulations must not affect the efficiency of suppliers.

- Provision for assertions about authenticity and integrity
- Suppliers must have a defined process for ensuring the integrity of delivered components.
- Service disruption due to supply chain impacts
- Standardized incident and periodic reporting to Federal customer based upon agreed-upon criteria
- Specifically detail desired capability in empirical terms. Often the details are not known at contractor level
- Suppliers need to provide design, installation, and change management documentation

17) Which of the following readiness capabilities are important in IT security emergency response?

	Unimportant	Of Little Importance	Moderately Important	Important	Very Important
Maintain cyber security procedures that define types of incidents and response protocols.	(2.4%)	(3.2%)	(18.4%)	(33.6%)	(42.4%)
Frequently review federal cyber security bulletins/vulnerability summaries.	(3.2%)	(9.6%)	(22.4%)	(31.2%)	(33.6%)
Have pre-established lines of communication with Computer Emergency Response Teams or other official support resources.	(4.8%)	(6.3%)	(15.1%)	(25.4%)	(48.4%)
Conduct cyber war games to test network defenses.	(10.2%)	(13.3%)	(25.0%)	(28.9%)	(22.7%)
Use the Cybersecurity Evaluation Tool (CSET) or other accepted methodologies to assure Industrial Control Systems.	(10.3%)	(8.7%)	(23.8%)	(31.0%)	(26.2%)

18) Please specify any <u>other</u> readiness capability that is important in IT security emergency response?

- Plan and demonstrate contingency operations in de-centralized configuration

- Offsite, full scale, backup facility to ensure continuous operations and remote access during emergency
- Suppliers should make recommendations when vulnerabilities are perceived
- Seek and develop technical details of current and potential threats and provide information on detection events
- Product scans by 3rd party; documented and tested recovery & response plans
- Impact analysis for business operations, data integrity, potential damage to the organization and contractor
- National Computer Data Center and laboratory
- The requirements related to emergency response should be specific and state the operational context
- Training, Lessons learned, overall plan and chain of command for notification

19) How would you rate the importance of each of the following entities in responding to a serious threat to your IT supply chain?

	Unimportant	Of Little Importance	Moderately Important	Important	Very Important
Internal Security Organization	(4.1%)	(2.5%)	(18.0%)	(19.7%)	(55.7%)
FBI	(8.9%)	(15.4%)	(28.5%)	(26.8%)	(20.3%)
Local Police	(15.3%)	(29.0%)	(27.4%)	(16.1%)	(12.1%)
US CERT (Computer Emergency Response Team)	(8.1%)	(9.7%)	(24.2%)	(27.4%)	(30.6%)
DOD Computer Security Evaluation Center	(9.8%)	(15.4%)	(19.5%)	(29.3%)	(26.0%)
Department Of Commerce/Bureau Of Industry and Security	(12.9%)	(22.6%)	(26.6%)	(18.5%)	(19.4%)
Department Of Homeland Security	(10.5%)	(18.5%)	(26.6%)	(19.4%)	(25.0%)
Industrial Association/Organization	(17.1%)	(22.8%)	(27.6%)	(20.3%)	(12.2%)
Sector Coordinating Council, or similar public/private partnership	(17.1%)	(30.9%)	(24.4%)	(17.1%)	(10.6%)

Section IV:
Elements of a Vendor Code of Practice for IT Supply Chain Risk Management

20) **Please rate the attractiveness of each item below for potential inclusion into a Federal Code of Practice for IT Vendors that seeks to improve supply chain risk management?**

The attractiveness of each Code element must be based on both its *potential operational* and *cost effectiveness* for your company.

	Ineffective	Rarely Effective	Moderately Effective	Effective	Highly Effective
The IT Vendor must demonstrate an executive risk management mechanism, such as a risk board.	(12.2%)	(23.6%)	(31.7%)	(22.0%)	(10.6%)
The IT Vendor must submit a supply chain risk management plan with each bid to a federal acquiring party.	(14.6%)	(19.5%)	(30.9%)	(23.6%)	(11.4%)
The IT Vendor must disclose all IT risks to a federal acquiring party at contract inception and during the project cycle for itself and its suppliers.	(13.8%)	(13.0%)	(27.6%)	(30.1%)	(15.4%)
The IT Vendor must maintain an acceptable level of supply chain audits.	(10.5%)	(13.7%)	(27.4%)	(28.2%)	(20.2%)
The IT Vendor must track supply chain risks/mitigation actions in an online registry accessible both to the acquiring party and supply chain participants.	(15.6%)	(18.9%)	(31.1%)	(22.1%)	(12.3%)
The IT Vendor must develop, maintain and periodically test business continuity plans.	(10.5%)	(9.7%)	(25.0%)	(29.0%)	(25.8%)
The IT Vendor must guarantee authenticity of products.	(4.8%)	(8.1%)	(26.6%)	(29.0%)	(31.5%)
The Federal Acquiring Party must provide additional dedicated contractual resources to vendors for undertaking critical risk management improvements.	(12.3%)	(9.8%)	(25.4%)	(32.8%)	(19.7%)
The Federal Acquiring Party must incentivize vendors' critical risk management improvements by rewarding such investments with preferential vendor status.	(7.3%)	(7.3%)	(22.0%)	(30.9%)	(32.5%)
The Federal Acquiring Party must help companies to buffer exposure to liability and reduce corporate capital reserves set aside for future liability claims.	(10.9%)	(15.1%)	(16.8%)	(31.9%)	(25.2%)
The Federal Acquiring Party must simplify/eliminate acquisition procedures and regulations not pertinent to cost-effective corporate self-regulation of supply chain risk.	(5.0%)	(10.0%)	(16.7%)	(38.3%)	(30.0%)
The Federal Acquiring Party must incentivize vendors to identify and develop local U.S. based sources of supply as alternatives to overseas outsourcing.	(5.8%)	(7.5%)	(17.5%)	(30.8%)	(38.3%)

21) Please specify any <u>other</u> items that should be included in a Federal Code of Practice for IT Vendors that seeks to improve supply chain risk management:

The IT Vendor must:

- Be held to a higher standard
- Make a CEO-level commitment to a list of security practices in any software development project
- Not declare as proprietary the solution details and integration technology used to meet public requirements
- Establish protocols and operate with full visibility for control and accountability

- Demonstrative the effectiveness of products, and test results which are reasonable

- Be reasonably flexible to incorporate unforeseen contingency need into contracts.

- Comply with all applicable United States laws and regulations, and all country of origin laws and regulations

- Disclose a summary of the processes and mechanisms used to ensure the authenticity and integrity of products

- Get Common Criteria, FIPS and 508 Certified

- Be capable of maintaining a comprehensive assessment and reporting program utilizing resources available

- Provide training, support through the systems life cycle development

- Validate all pieces/parts of their product line and for software map the signatures to a centralized board

- Not fear compliance mandates and cooperate where warranted

The Federal Acquiring Party must:

- Understand what they're getting before they put it in the RFP. And allow proposals to be longer.

- Keep all venders on a level playing field

- Publish lessons learned and innovative solution details in appropriate industry journals

- Create and administer objective and measurable performance requirements that include consistent, uniform metrics

- Train their representative to ensure the quality of products delivered

- Take the professional and honest efforts of IT Vendor into consideration before reassigning the same
- Be deeply committed to conducting business according to the highest standards of honesty, ethics
- Provide special incentives and reduced demands on small business providers
- Collaborate with the vendor to assure unfettered communication and achievement of security objective
- Consider the way set up the IT standards and procedures
- Maintain records of the supply chain from acquisition through the end of life and disposal/sanitization
- Not be hostile to U.S. based industries; must not ignore the sub-supply chain associated with the pr

Follow-Up

22) Please indicate if you would agree to be contacted for further information (check one):

- Yes
- No

23) If yes, please provide your name, email address and telephone number.

First Name: _____

Last Name:_____

Email Address: _____

Telephone Number: _____

Thank You!

Thank you for taking our survey. Your response is very important to us.

Appendix 2:

Texas IT Code

(Texas Administrative Code, Title 1, Part 10, Chapter217, Subchapter B, Rule §217.12) became effective in December:

(a) Effective December 1, 2010, a contract for the purchase or lease of network hardware or network software entered into by a state agency, after compliance with Chapter 212 of this title (relating to Purchases of Commodity Items), is required to contain the following certification to be completed by vendors, including manufacturers and resellers: Vendor hereby certifies that the network hardware or software, as applicable, procured or leased under this contract, has undergone independent certification testing for known and relevant vulnerabilities in accordance with §2059.060, Texas Government Code.

(b) The required independent certification testing of network hardware or software for vulnerabilities must be conducted against established standards under maximum load conditions in accordance with published performance claims of a hardware or software manufacturer, as applicable. Testable performance claims are quantifiable metrics provided by the manufacturer that include, but are not limited to, maximum bandwidth, maximum processing speed, average response times, or number of simultaneous connections.

(c) At its discretion, a state agency may request supporting information from a vendor related to the independent certification testing for known and relevant vulnerabilities.

(d) A contract for the purchase or lease of network hardware or network software is exempt from the certification requirement in subsection (a) of this section if one of the following circumstances exists:

(1) No independent certification testing standards have been established for applicable network hardware or network software;

(2) An independent testing laboratory that is able to perform independent certification testing of applicable network hardware or software for vulnerabilities does not exist;

(3) The contract is the result of an emergency procurement as defined in §2155.137, Texas Government Code;

(4) A state agency head, or his or her designated representative(s), who determines that it is in the best interests of the state agency to proceed with a purchase or lease of network hardware or software, grants an exemption to the certification requirement in subsection (a) of this section.

Each exemption must provide a justification for the exemption, including relevant cost avoidance, reduction of undue burden, the intended usage or risk assessment of potential vulnerabilities.

In a separate article by Security Dark Reading:
http://www.darkreading.com/vulnerability-management/167901026/security/perimeter-security/229209866/ul-seal-of-approval-launched-for-resiliency-of-networking-security-products.html