Summary of the Workshop

On

Information and Communication Technologies Supply Chain Risk Management

National Institute of Standards and Technology

October 15-16, 2012

Background

Federal agency information systems are increasingly at risk of both intentional and unintentional supply chain compromise due to increasing reliance on Commercial off-the-shelf (COTS) products, the growing complexity of information and communications technologies (ICT), the mounting number of information systems, and growing speed and complexity of a distributed global supply chain. There is a great demand from federal departments and agencies for supply chain risk management (SCRM) guidance.

However, the ICT supply chain security discipline is in an early stage of development with diverse perspectives on foundational ICT supply definitions and scope, disparate bodies of knowledge, and fragmented standards and best practice efforts. Additionally, there is a need to identify available and needed tools, technologies, and research efforts related to ICT supply chain risk, and to better understand their benefits and limitations.

This document is a summary of a workshop held October 15-16, 2012 to broadly engage all stakeholders in an effort to set a foundation for NIST's future work on ICT SCRM. Approximately 130 representatives from industry, academia, and government attended the workshop. Links to presentation materials are included in this summary where possible.

Summary of Day 1 – October 15, 2012

- Opening Remarks; Donna Dodson; Chief, Computer Security Division, Information Technology Laboratory, NIST
  - **Description**: The SCRM issue is of rising importance in every aspect of our life. It impacts the defense and economic security of the nation; everybody is reliant on the same technology. We at NIST need to understand how technology can address the risk management needs and requirements of SCRM and what standards and best practices NIST can develop and incorporate from industry to tackle this issue.

- Overview of Workshop; Jon Boyens; ICT SCRM Project Lead, Computer Security Division, Information Technology Laboratory, NIST.
  - **Description**: Stemming from CNCI 11, NIST Interagency Report (IR) 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems,* was published just prior to the workshop in early October, 2012. Now, NIST is moving towards developing a Special Publication (SP) on SCRM. Supply chain risk is a very complex problem and NIST is committed to working closely with industry and government to identify and develop tools, technologies, and standards to help organizations manage it.

- Supply Chain Risk: Stagnation or Transformation? Gary S. Lynch; Global Leader, Risk Intelligence and Supply Chain Risk MARSH Risk Consulting & Author
  - **Description**: Gary offered his unique perspective on the current state of risk management across multiple risk topics, industries and geographies. One of his favorite quotes, "if you have seen one supply

chain, you've seen one supply chain", demonstrates the complexity of SCRM. He argued that uncertainty is fundamental to risk; without uncertainty, there is no risk. With each business trend, the exposure to uncertainty becomes greater.

Unification or taxonomies provide the ability to understand the supply chain. They provide a "market", with defined customers, products and services, and needs and wants. They provide the ability to understand who owns a problem and what their motivations are. Transparency and data allows for improved efficiency, risk transformation, and an opportunity for reducing underwriting costs.

Particular threats or threat events have moved to the backstage, meaning they are used as a mechanism to test the design of a supply chain, but no one can accurately predict the types of events that are going to occur. So, design takes on greater importance for assurance, and testing becomes the modeling activity. Liability / responsibility to others in most instances is not sufficiently understood and therefore, either not considered or measured. There is more of an association of who is trusted for a given good, or the desire to take over that portion of the supply chain themselves.

- Managing Supply Chain Risk: Using NIST's FISMA-Related Standards and Guidelines; Ron Ross; NIST Fellow & Project Leader, FISMA Implementation Project and Joint Task Force Transformation Initiative
  - **Description**: Ron discussed the increasing sophistication of cyber threats and the need for great dependability in the supply chain. He argued for a "change of course", requiring us to:
    - Simplify: reduce the complexity of IT through standardizing, optimizing, and consolidating IT assets
    - Specialize: customize security controls to the missions/business functions
    - Integrate: Implement security requirements into enterprise architecture, systems engineering, SDLC, and acquisition.

    It is important to build things right first, and then continuously monitor what you have built. Looking at Advanced Persistent Threats (APT) and conventional threats (e.g. hostile cyber attacks, natural disasters, and errors of omission and commission), no one wants to implement thousands of controls for a "sky is falling" situation. There needs to be credible risk assessments and top level decision makers need help to understand the actual mission risk. Security programs should be built using an "integrated project team" concept where every stakeholder is around the table and contributes critical information to senior leaders deciding whether a mission is a "go" or "no-go".

    NIST has developed a series of security standards and guidelines which can help effectively manage information security-related risks that emanate from the supply chain. The guidelines include a Risk Management Framework and a broad-based set of security controls that are targeted at specific supply chain issues including the development of trustworthy information system components and systems. Ron provided an overview of NIST Special Publication 800-53, Revision 4, to be published later this year, including specific safeguards and countermeasures to help organizations protect all aspects of their supply chain, from development to delivery to implementation and operation.

- Supply Chain Approaches in Industry; Taylor Wilkerson; Program Manager, LMI's Research Institute
  - **Description**: For many years, industry has addressed a wide variety of risks in their supply chains—natural disasters, financial disruptions, quality failures, counterfeits, and more. Based on his work with

the Supply Chain Risk Leadership Council (www.scrlc.com), an industry association focused on SCRM, and the Supply Chain Council (www.supply-chain.org), Taylor presented leading risk management practices that companies are now using to manage risks, including supply chain definitions, risk assessment methods, risk treatment approaches, response actions, and risk recovery.

Supply Chain Risks include financial, demand, quality, and cybersecurity risks and cover natural, accidental, man-made, and malicious disruptions. You need prioritization to deal with the real threat of risks and your SCRM program needs to cover recovery and monitoring in addition to risk assessment. There's not always a lot of data on risks – risk, by definition, is uncertainty – sometimes you rely on the subjective discussion of stakeholders in a room to identify the threats to your supply chain. It is impossible to mitigate every risk your supply chain faces, but you can develop a plan to respond when unmitigated risks occur. How you communicate with suppliers and customers is important since they control the security and resilience of your supply chain.

One of the most difficult challenges of SCRM is mapping your supply chain. Today's supply chains operate globally and are very dynamic with short product and technology life cycles. In many cases, companies don't even touch the products they make; it's direct shipped to the customer or retailer from the manufacturer, who is separate from the brand name company. Industry has spent the last two decades disaggregating supply chains, and with that, companies lose a lot of control. Approaches to the hard problems include visibility, multi-tier collaboration, and increased development and use of standards.

Taylor provided his views on the future, including:

- Future / Emerging Risks: cyber, regulatory, sustainability, social media
- Tools for Risk Management: visibility, simulation, monitoring

- Panel – Bridging the Divide: A discussion of Federal Government and Industry's Thoughts and Vision for ICT Supply Chain Risk Management
  - **Description**: In this panel, representatives from government and industry discussed their opinions on the current state of ICT supply chain risk management and how they believe the discipline needs to progress. Panelists discussed their programs and approaches, what they feel is critical for the success of ICT SCRM, what is, and is not, in the scope of ICT supply chain risk management, what is the "real" risk (versus "perceived" risk) of supply chain compromise, what constitutes "shared responsibility" and accountability, successes and challenges, and existing gaps and areas requiring future work.
    - **Joe Jarzombek**, Department of Homeland Security: Enterprise level risk is often inherited from supply chain development and acquisition decisions. Who makes risk decisions and who owns the risk? Often risk decisions are being made by those who do not own the resultant risk attributable to counterfeit and tainted products (those with malware, exploitable weaknesses and vulnerabilities). Who evaluates software and IT components as "fit for use" in the intended operational environment? Organizations need technology to help understand risks and develop mitigation strategies.
    - **Wayne Meitzler**, Pacific Northwest National Laboratory, Department of Energy: SCRM has two major elements: securityand logistics. Logistics have been addressed for decades; however, security has hardly been touched. Yet security – that is the integrity of electronic devices – is paramount as the nation depends increasingly on commodity devices obtained through global

markets. Without the assurance of integrity in commodity devices, critical systems in defense, infrastructure, and commerce could have catastrophic failures, or vital intellectual property lost to competitors. So, how will industry and the government create increased level of trust for these vital devices in an era of doing more with less?

    - **Craig Corbin**, World Wide Technology: Currently seeing large COTS purchases with nebulous requirements. Requirement to provide SCRM information, but award is not going to be awarded based on that information. Prove that you know how to mitigate risk of counterfeits. Is a plan for mitigation or actual mitigation more important?
    - **John Toomer**, The Boeing Company
    - (Moderator) **Jennifer Bisceglie**, Interos: Summarized the common points as (1) the need to focus on standardizing the business requirements to ensure the Government gets what they're asking for and (2) be familiar with the various options as to how to monitor and audit the technology in use to ensure supply chain risk mitigation.

  - **Question & Answer Discussion Points:**
    - *How real is the threat? What is it?* The real question should be "how real is the risk". Organizations have to recognize the likelihood of an event. It's a very sophisticated attacker that can use the supply chain as an attack venue. Counterfeits are a major problem and they are becoming very sophisticated. Also, it is not always about a threat actor, but unaware, well-meaning individuals in the supply chain. Organizations are attacked all the time, but what is important is the business case and when can the organization say 'we have spent enough'?
    - *Where do the responsibilities lie?* Acquirers and suppliers need a better understanding of SCRM so there can be a conversation with both sides. RFP's are a start, but are they the right / best thing? Are they articulated correctly according to organization values? The cost of mitigation varies with the methodology. Acquirers should work with suppliers to develop requirements as far as both can afford. There is a government responsibility to give suppliers clear requirements – what will be classified, what is required, etc. Also, there should be both a carrot and a stick from those who supply requirements.
    - *How important is SCRM ranked in you organizations?* SCRM is a great opportunity for an organization to differentiate itself from the rest of the pack. There is a lot of movement in SCRM, but it needs to be streamlined. Risk management is a human enterprise that crosses all areas of an organization's structure.
    - *There are a lot of standards, what is needed?* The government is a small amount of the worldwide business – international standards are needed, but they must meet Federal government needs. A challenge is that organizations only test against requirements, and not unintended or intended vulnerabilities. Better diagnostic capabilities are needed. Who touched a product should not be as important as does it work and is it secure.

- Program Protection Planning in a Global Supply Chain; Mitchell Komaroff; Director, Trusted Mission Systems and Networks (TMSN), Department of Defense (DoD) Chief Information Officer (CIO)
  - **Description**: Commercial IT products have penetrated every facet of the Department of Defense (DoD), including providing mission-critical functions. Mr. Komaroff talked about the strategy for Trusted Mission Systems and Networks in DoD (DoDI 5200.44):
        - Understand system criticality and prioritize resources

- Strengthen systems security engineering practices to identify and protect critical functions and components
- Use threat assessment to inform risk management strategies
- Manage risk to critical components through the acquisition lifecycle / acquisition program protection and SCRM.
- Partner with industry to drive security

Through the program protection planning, the DoD intends to manage risk to their system and capabilities. DoD-CIO (TMSN) cooperates with AT&L/CIO, NSA, IC, and CNSS on SCRM activities. He provided an overview of several initiatives that the DoD is involved with, including:

- DoD 5200.44 *Trusted Systems and Networks*: This document establishes policy and responsibilities for the identification and protection of critical functions through Program Protection.
- ISO/IEC 15026 *Systems and Software Assurance:* A four-part, international standard provides an "assurance case" linked to life-cycle processes.
- ISO/IEC 27036 *Information security for supplier relationships*: This international standard addresses the issue of how data is protected in a supplier/acquirer relationship.
- The International Council on Systems Engineering (INCOSE): A membership organization for systems engineering best practices.
- The Open Group: A membership organization currently working on developing a standard and accreditation program around maliciously tainted and counterfeit products.
- NIST SP 800-160: A planned publication to help Federal Agencies system security engineering.

- Session A: Foundational Underpinnings
  - **Facilitator**:
    - Don Davidson, DOD
    - Nadya Bartol, ISO/IEC 27036 Editor

  - **Overview**: Currently, there is no commonly accepted set of terms, definitions, and classifications for ICT supply chain risk management. The term "supply chain" currently has many definitions in the context of ICT, either defining the term broadly and all-encompassing or emphasizing specific aspects and characteristics, e.g. constituents, processes, functions, interactions, system/ network, objectives, etc. The lack of a common understanding between both individuals and organizations hampers efforts to develop standards and best practices as well as impedes an organizations ability to mitigate supply chain risks.

    This session took a systematic look at some key definitions and issues of concern for development of NIST SP 800-161. Topics for discussion were:

    - Scope of SCRM
    - Target audience
    - Definition and use of some specific terms, including SCRM, critical component, integrator, and visibility
    - Composite / underlying disciplines

- **Objectives:**
  - Identify key terms related to ICT SCRM.
  - Ascertain current and possible definitions.
  - Define what constitutes and characterizes the ICT supply chain.

- **Discussion Results:**
  - The NIST SP needs to provide practical, obtainable, and measurable baseline (not ceiling) guidance for Federal Information Processing Standard (FIPS) High-impact hardware, software and services, but it should not preclude moderate-impact or other tailoring. It should be risk-based, and allow for prioritizing of resources according to the mission / business case. The scope should be broad enough so that it does not quickly become obsolete and be very clear so that it can become the foundation for future work (e.g. potential contract language or regulations). Specific measurements / measures should *not* be listed, but the notion of good measurement practices should be mentioned and point to existing guidance where possible.
  - The NIST SP should tie in with the Unified Risk Management Framework (NIST SP 800-39, 800-37, 800-53, etc.) and contain a description of how this document fits in, builds, and compliments other standards. An overlay on top of existing standards (most likely NIST SP 800-53) would be useful.
  - The audience / stakeholders should be limited to the Federal Government, but extended to include federal developers, managers, and end users of systems. It should take into consideration the (possibly varying) perspectives from which the reader is coming. It would be useful to have contract terms in the document.
  - It should also include a threat frame of reference, model or reference to other document (e.g. NIST SP 800-30, Open Group Trusted Technology Forum (OTTF), Common Criteria), but not scenarios, in order to help industry and the government have a conversation and to prevent attempting to “boil the ocean” or “being afraid of the boogey man”. Counterfeits, unintentional and intentional vulnerabilities, and poor practices should all be included and Intellectual Property (data and metadata) should be specifically addressed. Risks both to and through the ICT Supply Chain should be included.
  - Definitions need to be clear and from the acquirer’s perspective. However, they must acknowledge that industry may have different definitions for the same terms. The differences between secure engineering, quality assurance, and SCRM need to be clarified. The terms should be generic and the document as a whole should speak in a “global” language which crosses industries and geographic borders. Some specific terms were discussed (Information Assurance, Information Security Risk, acquirer, critical component, visibility, transparency, customer, etc.).
  - Responsibility and accountability are important items to consider, especially with traceability, visibility, and authenticity. How much visibility a customer should have into supplier processes, and vice-verse, is questionable, but a two-way visibility system is necessary. Mission owners should know what their systems are made of at least.

- Session B: Tools, Technologies, and Techniques
  - **Facilitator:**

    - Dr. Sandor Boyson, University of Maryland

- **Overview**: Many tools, technologies and techniques have been developed to help mitigate supply chain risks, but they are unevenly distributed throughout the ICT supply chain. Often, they are limited to specific threats or vulnerabilities, designed for a specific implementation, lack useful metrics, or are considered unreasonable for widespread use.

  Lee Zeichner (ZRA) gave an overview of the Supply Chain Automated Risk Level Evaluation Tool (SCARLET) . He discussed the difficulties of quantifying the supply chain, focusing on differences between the private and government sectors and a lack of education on the subject. He stated that there are "pockets of capabilities", including the medical, aerospace, and financial communities, that do some aspect of SCRM relatively well and that there is a need to put all this existing experience together instead of trying to start from scratch or simply re-creating something that already exists.

  Christy Coffey (TM Forum) provided an overview of the Cyberops Metrics Project, launched in January 2012. The goal of the project was to provide metrics to improve the "contractability" of information security / SCRM. The five large best practice guides in the project are: Patching; Mobile Devices; Human Factors; DDos; Servers.

  The group was asked for feedback and then led through a "Delta Exercise" in which participants were asked to list any tools they thought were useful or needed in the SCRM space. Results are located in Appendix A.

- **Objectives:**
    - Evaluate the benefits and limitations of current and proposed tools and technologies for evaluating and mitigating supply chain risks.
    - Discuss the effectiveness of various techniques currently being used by both government and industry.
    - Identify areas where existing tools, technologies, and techniques are inadequate to reasonably mitigate ICT supply chain risk throughout the system lifecycle and provide potential areas of opportunity.

- **Discussion Results:**
    - SCRM metrics are vital for feedback, to hold organizations / people accountable, and because "you can't secure what you don't know". However, metrics can be subjective, company to company, which is an issue with NIST IR 7622 and other performance-based standards.
    - It is difficult to quantify qualitative metrics (e.g. decision-making skills) and there can be differences in how mitigating strategies are applied, which affects associated metrics. Studies on the effectiveness of SCRM controls need to be conducted.
    - The value of mapping the supply chain is unclear. Some claimed it vital while others didn't see the use. Arguments were that it provides accountability, knowledge and traceability, but is only a snapshot in time. While it doesn't make sense to map another's suppliers, if they map it and make that map available, that is good for the acquirer.
    - Delta Exercise results are located in Appendix A.

Summary of Day 2 – October 16, 2012

- Session C: Practices and Standards
  - **Facilitator**:
    - Don Davidson, DOD
    - Nadya Bartol, ISO/IEC 27036 Editor

  - **Overview**: The United States Government (USG) recognizes that broad use of recognized standards and practices best ensures the integrity of federal information systems dependent upon a global supply chain of increasingly sophisticated systems, components, software, and services. However, the ICT supply chain security discipline is in an early stage of development, with a plethora of standards and best practice efforts. Many of the efforts rely heavily on cybersecurity and system and software engineering standards and practices, and build on top of that traditional logistics-based supply chain practices. There is currently a question of how broadly or narrowly focused ICT SCRM practices should be in terms of scope (to include quality control/management?) and feasibility (aspirational versus commercially reasonable).

    This session started with a review of current ICT SCRM Standards activities:
    - *NIST IR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems*: NIST recently released the final version of this document after a four-year effort. It contains 10 descriptive practices covering the entire systems life cycle. It was originally intended for use in pilot programs, but now is a research document of potential mitigation strategies.
    - *NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations*: NIST released the first draft of this document in Spring, 2012. It includes the addition of SA-12 which is the principal SCRM control. Many of the control enhancements of SA-12 overlap with 7622. There are also controls for counterfeits, tamper resistance, and other supply chain-related concepts throughout the document.
    - *ISO / IEC 27036, Information security for supplier relationships*: This is a draft international standard in multiple parts. Currently, parts 1, 2, 3, and 5 are being developed. The standard addresses the issue of how data is protected in a supplier/acquirer relationship.
    - *Open Group*: The Open Group worked for over 18 months to collect best practices and turn them into a useable framework. Several documents were created. They recently finished a “snapshot standard”, and are currently half way through the accreditation program. They hope to have a pilot in the first quarter of 2013.
    - *SAE AS5553, Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition*: AS5553 was published in 2009 and primarily addresses the end user. The main point of the standard is if a manufactured part is important, an acquirer should purchase it from the authorized source. If the part does need to be bought from a secondary market, extra research is needed.
    - SAE AS6061, Counterfeit Electronic Parts for Distributors: AS6061 is related to AS5553, but is directed towards independent distributors.
    - Safecode: Safecode was established in 2007 to share best practices. Their goal was to write down the best practices in a readable, usable format. There are two papers available on their website on supply chain (*Framework for Software Supply Chain Integrity*, and *Overview of Software Integrity Controls*).
    - *Common Criteria*: The concept of criticality was the main focus of this effort. Some parts matter more to the system, and doing extra assurance affects the final cost to the buyer. The goal of

this effort was to create a method to evaluate criticality and make sure there were no short cuts to certification.

  - *ASIS*, *Supply Chain Risk Management Standard: a Compilation of Best Practices*: The standard development effort is focused on security and assurance and is being carried out in collaboration with the Supply Chain Risk Leadership Council. ASIS was previously focused on everything but the management of ICT, so they are working towards that goal through this standard.

    Department of Defense (DoD) Activities: The DoD is currently involved in several on-going efforts related to SCRM. Most notably, they co-chair Working Group 2 formed from the Comprehensive National Cybersecurity Initiative (CNCI) #11. Also, there is a Public-Private SCRM Ad-hoc working group where all US entities are allowed to participate in ISO standards development on SCRM. A Key Practices Guide currently used by NATO is being considered for an update. While there are numerous efforts in SCRM, the DoD is interested in ones that will be actionable in the next few years.

With the federal government's increasing reliance on COTS hardware and software, there is great demand for a consistent federal approach to ICT SCRM. In this session, attendees discussed the following issues related to the development of a government-wide SCRM Standard:

  - ICT SCRM vs. Basic Business Processes
  - Intentional vs. Unintentional Threats
  - The Development Approach of a Special Publication
  - Key Practices

- **Objectives:**
  - Discuss the merits and challenges associated with various ICT SCRM standards and related efforts – their purpose, scope, effectiveness, and plans for development.
  - Identify areas where additional standards and guidance are needed and how they should be developed.
  - Determine a balanced scope and approach that is sufficiently robust yet commercially reasonable.

- **Discussion Results:**
  - All Federal acquirers should be able to reference the Special Publication and it should help suppliers understand the business practices of Federal IT systems. It should give industry some idea of what to expect from federal agencies. The Special Publication should be framed so that it helps those who don't necessarily understand SCRM or who may not have FISMA requirements.
  - The Special Publication should drive harmonization and set the stage for SCRM. It must align with other NIST documents and global standards and provide insight into the various surrounding standards and how a customer might use them. Common language across disciplines / efforts is a problem (e.g. "defensive design" vs. "secure engineering"). Standards should use the language of the foundational documents they point to, and vice-verse, so there isn't a gap.
  - The Special Publication should be goal oriented / performance-based. While example best practices in standards is useful, the Special Publication should not be so prescriptive as to stifle innovation. Additionally, metrology has not yet been developed for many practices. It may be possible to develop separate, supplemental NIST Interagency Reports on specific techniques /

technologies which can be updated as necessary. However, there must not be too many documents or it can become difficult to manage.

- The scope of the document needs to be practical, obtainable, and focused on the government's responsibilities when acquiring technology. Intentional and unintentional threats should be addressed, but the practices associated with them are different. Unintentional consequences should be foundational with intentional-based practices applied on top. A certain level of product quality should be expected.
- The Special Publication should be developed as an overlay to NIST SP 800-53r4 with other publications bundled in. However, it should not be limited to one perspective or limited to 800-53 practices only. A clear tie-in with NIST SP 800-53 along with foundational practices is generally accepted as a good approach, but there is uncertainty as to how it will be done.
- Key practices should be worded from the acquirer's perspective. Although none had a majority of participants disagree, of the key practices in NIST IR 7622, only #4, "Share Information within Strict Limits" presented any significant concern (6 out of approximately 50). The main comment was that this practice was covered by general information assurance practices and may be covered by other requirements (the Federal Acquisition Regulation (FAR) was mentioned, though unconfirmed). The SP should talk about information sharing, but then reference other sources for specifics.
- Of the 12 OTTF practices, numbers 1 and 2 (Risk Management and Physical Security, respectively) were determined to be foundational to a supply chain overlay. There was no real objection to any of the practices.

NIST IR 7622 Key Practices
1. Uniquely Identify Supply Chain Elements, Processes, and Actors
2. Limit Access and Exposure within the Supply Chain
3. Establish and Maintain the Provenance of Elements, Processes, Tools, and Data
4. Share Information within Strict Limits
5. Perform Supply Chain Risk Management Awareness and Training
6. Use Defensive Design for Systems, Elements, and Processes
7. Perform Continuous Integrator Review
8. Strengthen Delivery Mechanisms
9. Assure Sustainment Activities and Processes
10. Manage Disposal and Final Disposition Activities throughout the System or Element Life Cycle

OTTF Practices
1. Risk Management
2. Physical Security
3. Access Controls
4. Employee and Supplier Security
5. Business Partner Security
6. Supply Security Training
7. Information Systems Security
8. Trusted Technology Components
9. Secure Transmission and Handling
10. Open Source Handling
11. Counterfeit Mitigation
12. Malware Detection

- Session D: Research and Resources
  - **Facilitator:**
    - Dr. Sandor Boyson, University of Maryland
    - Hart Rossman, University of Maryland
  - **Overview**: Research and bodies of knowledge in ICT SCRM are often detached and isolated. There is a need to identify and link current ICT SCRM research activities and available resources in order to promote development in this field.

    Holly Mann, Hart Hanson, and Christy Coffey provided an overview of the UMD SCRM Prototype Web Portal. The portal contained the following major sections:
    - Assessment tool: A strategic readiness survey based on NIST IR 7622. Results allow peer benchmarking and the ability to determine an organization's maturity level
    - Mapping tool: Allows organizations to geographically display their supply chain, including vital information and "CVSS-like" scores for various nodes and transactions.
    - Initiatives Database: Searchable repository of SCRM standards and initiatives to enable organizations to find specific guidance or control information.
    - Library: Searchable database of relevant SCRM documents which allows users to upload their own documents.
    - Forum and News: Not available yet, but will allow real-time collaboration and transfer of information.
    - A detailed report on the portal can be found at: http://csrc.nist.gov/scrm/documents/umd_ict_scrm_portal_report3.pdf

    The group was then led through a delta exercise in which participants were asked to describe areas where they would like to see some research done. Results are included in Appendix B.
  - **Objectives**:
    - Identify recent and current research seeking further understanding of the ICT supply chain and help mitigate supply chain risks.
    - Ascertain various resources useful to either the research or implementation of ICT SCRM.
    - Detect those areas where additional research or resources are needed in this field.
  - **Discussion Results:**
    - Security and anonymity of data (especially survey results) is paramount. False survey answers could become a problem if the information is used for rating, but right now it is completely confidential, so there is no pressure to do that. Falsifying answers would make the survey useless. Because the survey does take a significant amount of knowledge of business practices to complete, organizations may have to find information; it takes a lot of effort to complete. However, organizations who completed the survey found it valuable.
    - The usefulness of the map was debated, with a general agreement that it was useful, but would be much better if it allowed for real-time information feeds. Arguments included that knowing what your assets are and where they are is a basic thing for other disciplines / tools. The map helps visualize threats and vulnerabilities. The map focuses on interrelationships, bridges cyber and physical networks, and provides a means for analyzing the strategic level of SCRM. Several

specific suggestions for improving the map were provided, including the ability to visualize the importance of nodes, trustworthiness, and to add layers.

        - There is a strong desire for an “answer” – recommendations or guidance on how to improve based on survey results or map vulnerabilities.
        - The lack of effectiveness studies was brought up as a major concern. SCRM was compared to “Green” initiatives, suggesting that organizations need to be able to show metrics for how they do “good” instead of just highlighting when something bad happens. It was suggested that perhaps organizations don’t recognize the “good” because there is no data collected or documented. The reason given was that organizations are “too busy”.
        - Delta exercise results are located in Appendix B.

- ICT Supply Chain Risk Management from the Utilities Perspective; Connie Durcsak; President and CEO, Utilities Telecom Council
    - **Description**: Utilities Telecom Council (UTC) is the source and resource for information and communications technology (ICT) solutions, collaboration, and advocacy for utilities and other critical infrastructure industries. Connie addressed the utilities sector perspective on ICT SCRM and its importance to keeping the national critical infrastructure secure.

      Connie discussed a paradox created by the fact that the systems running critical utilities functions are increasingly reliant on telecommunications networks and ICT components. Utilities rely on telecommunications to run operations, but telecommunications rely on utilities to provide electric power. The telecommunications sector and the energy sectors are not just interdependent, they are co-dependent. Water and power systems’ success will ultimately succeed or fail based on the strength of our telecommunications network.

      Cybersecurity is one of UTC’s top concerns. ICT SCRM is an emerging challenge for the utilities, caused by an increased use of increasingly sophisticated technologies and platforms that are connecting to the Internet, such as the smartgrid. Threats to the utilities industry are not just hackers, but nation states, etc. These threats are not abstract and not in the future.

      This underscores the need for strong guidance from government on SCRM for the critical infrastructure. ICT SCRM is being addressed publically and privately and that creates a positive environment for collaboration. This collaboration supports increased awareness of potential solutions throughout the community. The majority of ICT SCRM efforts to date focused on US government, defense sector, IT, and telecommunications. Guidance needs to be useful, concise, and strike a practical balance (not too specific or general). UTC believes that utilities are the next frontier of tailoring and applying ICT SCRM practices.

Conclusion and Way Forward

There is a need for ICT SCRM solutions. A NIST Special Publication on supply chain risk management will be valuable for providing the U.S. Government and other organizations internationally a common foundation of terms and definitions, as well as offering agencies practical guidance on how to manage their supply chain risk. There is also a need for more long-term research efforts to develop tools to help organizations identify and effectively manage risks to their supply chains. Effectiveness studies are currently missing from current ICT Supply Chain research and this is necessary in order to determine what really works and what doesn't.

NIST has documented the suggestions made during this workshop and will incorporate them into a NIST Special Publication on ICT SCRM. As the document is developed, further discussions with smaller stakeholder groups will be conducted to ensure the document contains understandable, useful, and practical guidance for U.S. Federal Government departments and agencies.

In addition, NIST will collaborate with various organizations and groups to help develop research activities that were identified during this workshop as most critical. Avenues for discussing and suggesting new research and tools will be considered.

Appendix A: Tools / Technologies / Techniques Delta Exercise

Participants were separated into groups of 5 people. Each group was given a stack of 3x5 notecards and instructed to identify as many tools, technologies, and techniques as they could and write a description in the format shown in the table below. For each tool/technology/technique, users were asked to write:

(a) Which of the 10 given ICT Supply Chain Elements they believed it fell under,

(b) A name or description of the technology, tool, or technique,

(c) An example of the tool / technology / technique in use,

(d) Whether it is internally developed or commercially available,

(e) How technically complex the tool/technology/technique is (Technology Readiness Level), and

(f) Whether the tool/technology/technique is unique, emergent, or common (Diffusion level).

(a) ICT Supply Chain Element	**(b) Technology/Tool/ Techniques**	**(c) Exemplars (Companies/Projects/Use Cases)**	**(d) Internal Vs. COTS**	**(e) Technology Readiness Level (TRL) [1-9]**	**(f) Diffusion Level (Unique, emergent, common)**
1.Predict					
2.Protect (passive)					
3.Detect	[Example: Nano-pico Gamma sensor array]	[Example: Detect side channel attacks using cosmic radiation against embedded firmware]	[Example: Internal]	[Example: 7]	[Example: Unique]
4.Defend (active)					
5.Respond					
6.Recover					
7. GRC (governance, risk, compliance)					
8. Provenance & Pedigree*					
9. Anti-Counterfeit*					
10.Collaboration & Orchestration					

The following is collection of the responses received.

Category	Name	Description	TRL	Diffusion
Anti-Counterfeit	Mass Serialization	Technique of mass serialization. Examples include SEMI - T20 and ISO TC 247	6	emergent
Anti-Counterfeit	Digitally signed software	Only accept software (or patches to it) if the software is signed & signer is trusted. If not (yet) trusted, then evaluate.	9	common
Anti-Counterfeit	RFID Tags	RFID tagging. COTS	9	common
Anti-Counterfeit	Anti-Counterfeit	Visual inspection, x-rays, acoustic, labeling (RFD, DNA), acoustic microscopy, oscillators	7 to 9	common
anti-Counterfeit	DNA Marking	DNA marking. ex: validate authenticity	9	emergent
Collaboration & Orchestration	Collaboration Orgs	2 examples: ERAI database (www.erai.com), member of standards org: best of breed best practices for supply chain, ex: OTTF		emergent
Defend	Defensive Design	Design a system (software/hardware) to prevent/limit damage that could be caused by other components	9	common
Defend	Input Validation	Verify & limit to system and major components to valid values/ranges. Related to defensive design. Software: Correct data types, whitelisting, correct data range. Hardware: voltage limit	9	common
Defend	Anti-virus	Anti-virus (ex: Norton)	9	common
Detect	Diverse Double-Compiling (DDC)	Compilers are vulnerable to the "trusting trust" attack as noted by Ken Thompson & others. DDC can detect if the compilers source & executable correspond, thus countering subverted compilers	6	emergent
Detect	Open Source Software/Mass Peer Review	Reveal source code to all, this transparency enables widespread mass peer review to detect unintentional or intentional vulnerabilities	9	common
Detect	Software Vulnerability Scanner	Examine software for common vulnerabilities and report them	9	common
Detect	Software static analysis	HP Fortify as an example	9	common
Detect	Intrusion Detection System	Intrusion Detection Systems. Ex: tripwire, Symantec, etc.	9	common
GRC	Adjust sourcing agreements	Adjust sourcing agreements. Everyone does it.	9	common
GRC	FISMA, CoBIT, Frameworks	FISMA, CoBIT, Frameworks, etc. Sets a framework to implement risk guidance based on executive level and a flexible response based on project needs. Requires measurements & sets compliance requirements	9	common
GRC	Change Control Management	Documentation of changes and a formal process to approve the change. Many companies' projects use them.	9	common
GRC	SCARLET	Assesses Risk.	UNK	Unique
GRC or Provenance & Pedigree	Business Intelligence Tools or Database	Investigate companies	9	Common

Category	Name	Description	TRL	Diffusion
Predict	Supply Chain Threat Forecast Models	Weather, geopolitical, labor, economic, etc.	9	common
Predict	IPS Systems	IPS systems	9	common
Predict	Tool to predict social events	Tool to predict social events. In-Q-Tel investment	1 or 2	Unique
Protect	Encryption	Digital signatures, Kerberos, RSA tokens, etc.	9	common
Protect	Physical Access Control	Physical access control, wrapping, technology access control, firewall.	9	common
Protect	Segregate Manufacturing	Segregate manufacturing of components within plant. Ex: prevent tampering	9	Unique
Protect	Test scenarios & cases based on requirements	Companies & projects use/share test cases for known requirements. COTS products test case lifecycle manager	9	common
Protect	Separation of Duties	Enforce separation of duties. Widely used in IT and accounting fields.	9	common
Protect	EMI/Cabling shielding	EMI/Cabling Shielding. ARC Technologies (arc-tech.com). Eliminates unwanted interference from EMI (electro-magnetic interference)	9	Unique
Provenance & Pedigree	Examine Developers	Examine who key developers of components to determine the likelihood that they'd insert vulnerabilities (intentional or not)	9	common
Provenance & Pedigree	Provenance	Where has the part been? Chain of custody required by most purchasing contract	2	common
Provenance & Pedigree	Software Library/Component Tagging	Include information in software libraries/components so can easily determine what they are, version, and if that version is vulnerable. Otherwise end-users can't determine if software they receive has vulnerable components in it	6	
Provenance & Pedigree or Anti-Counterfeit	DNA on Microchip	DNA on microchip cannot be altered without destroying DNA. DARPA project	2	Unique
Recover	Product Redundancy	Multiple suppliers	9	common
Recover	Recovery Tool	Tool and documentation for recovering. Examples: Olson Captop allows recovery	7	common
Respond	CERT	Response teams at every level	9	common
Respond	Notification to systems and people	Examples: anti-virus, internal MRB system (e.g. quarantine)	8	common
Respond or Detect	T3	Technique- Tool. Incident response recognition of supply chain causal factor(s).Ex: Checklist provided to 1st & 2nd tier responders to help interpret when reported events may have SC source	3	proof of concept phase

Appendix B: Research Needed Delta Exercise

Participants were separated into groups of 5 people. Each group was given a stack of 3x5 notecards and instructed to think of what research they would like to see conducted and write a description in the format shown in the table below. For each tool/technology/technique, users were asked to write:

(a) Which of the 10 given ICT Supply Chain Elements they believed it fell under,

(b) A name or short description research concept,

(c) The objective of or purpose for the research,

(d) Who (industry, academia, or government) would be the best choice for conducting the research,

(e) An estimate of how long the research would take, and

(f) What priority the user would give the research.

(a) ICT Supply Chain Element	**(b) Research Concept**	**(c) Objective** **(Use Case, Goal, Problem)**	**(d) Conducted by:** **Industry,** **Academia,** **Government**	**(e) Est. Time Required** **1-3 years** **3-5 years** **Hard Problem**	**(f) Priority** **1= Low** **2= Medium** **3= High** **4= Urgent**
1.Predict	[Example: Real-time neurologic assessment of software developers]	[Example: We can't currently anticipate when a developer is about to write a line of vulnerable code]	[Example: Academia]	[Example: Hard Problem]	[Example: Urgent]
2.Protect (passive)					
3.Detect					
4.Defend (active)					
5.Respond					
6.Recover					
7. GRC (governance, risk, compliance)					
8. Provenance & Pedigree*					
9. Anti-Counterfeit*					
10.Collaboration & Orchestration					

* 8 & 9 are potentially subsets of other ICT SC Assurance categories. However, they have been called out due to their overwhelming applicability to the SCRM domain.

The following is collection of the responses received.

Category	Research Concept	Objective/ Description	Conducted By:	Estimated Time	Priority
Anti-Counterfeit	Detect unauthorized inserted logic.	As technology node advances (e.g. 120nm-45nm), more difficult to detect additional logic.	academia	Hard problem	High
Collaboration & Orchestration	Defensive Design.	Determine criticality of mission systems and collaborate w/interagency partners to be on the same page.			
Collaboration & Orchestration	Review law & policy to allow companies to share information weaknesses without liability.	Allow organizations within supply chains to identify vulnerabilities.	academia, government	Hard problem	Medium
Collaboration & Orchestration	Assessment & prioritization of IT change activities.	Determine efficient, effective mechanism to minimize disruption to supply chain & operational business functions. Low maturity capabilities already exist.	academia, industry	1-3yrs	Medium
Collaboration & Orchestration	Government and others have an anonymous "Angie's List" forum to discuss their suppliers and lessons learned.	Collaboration forum.	industry, government	1-3yrs	High
Collaboration & Orchestration	How to motivate companies/suppliers.	To perform in-depth analysis of their own supply chains rather than the buyer finding the vulnerable software or counterfeit part.	industry, government	Hard problem	High
Collaboration & Orchestration	Government contractors "Angie's List" to vet vendors, give ratings.	Members comment on reliability, performance of vendors. Think of ways that this does not become a black list. Provenance & pedigree is recorded.	academia	3-5yrs	High
Defend	Red teaming to determine supply chain weak points.	Research likely points of attack on a supply chain by thinking like the adversary.	academia, government	1-3yrs	Medium
Defend	Screen software/hardware/firmware for unwanted activity/capability.	Know the product does only desired activity.	academia, industry	1-3yrs	High
Detect	Easily & economically detect malware on government/industry extensively installed legacy software base.	Identify malware on legacy infrastructure.	all	3-5yrs	High
Espionage	Does a way exist to take back the loss of IP or other sensitive data to the use of a supplier and/or their	Quantify the impact of safe/trusted suppliers in terms of sensitive data.	academia, industry	3-5yrs	Medium

Category	Research Concept	Objective/ Description	Conducted By:	Estimated Time	Priority
	activity?				
GRC	Develop effectiveness measures, performance metrics of countermeasures.	We can't measure ROI on supply chain risk mitigations.	industry, academia, government	1-3yrs	Urgent
GRC	Certification requirement standard that standardizes new supplier provides (legal or otherwise)	Reduce threats to our networks and threats to supply chain fulfillment.	industry	1-3yrs	Medium
GRC	Ensure contractual & pre-contractual documents are reflecting supply chain requirements effectively.	Many contractual documents such as specification documents et. al. may not set supply chain requirements in terms that can be enforced or audited.	government, industry	1-3yrs	High
GRC	What does a government entity need to know about the product or company prior to making a product or service acquisition?	Scale differs with large systems to low cost efforts. Focus government on right questions to ask on SCRM.	academia, government	1-3yrs	Urgent
Predict	Connection between foreign suppliers and foreign intelligence agencies.	Probability that products contain malware or are otherwise tainted.	government, industry	1-3yrs	High
Predict	Utilize existing models (e.g. hurricane, earthquake) to determine likely scenarios & facilitate contingency planning.	Avoid operational surprise.	industry		Medium
Predict	Systems are built from components and depend on risk from each component.	Provide a formalism for capturing risk in each component so that risk of the system can be derived.	academia, industry	3-5yrs	Medium
Predict	Mergers & acquisitions, joint venture, partnerships, investments by or of suppliers	Changes in suppliers change user risk posture.	industry	Hard problem	High
Protect	Effectiveness of Software development practices.	We have too many potential practices to choose from. How does a company or a project determine which ones should be executed?	academia, government	1-3yrs	Urgent
Protect	Due Diligence.	Companies do not know their sub-suppliers.	industry	1-3yrs	High
Protect	Contracting language.	To identify sub-suppliers and aggregate risks.	industry	1-3yrs	High

Category	Research Concept	Objective/ Description	Conducted By:	Estimated Time	Priority
Protect	Forensic research software.	Need to screen software to discover malware, botnets, etc.	academia	Hard problem	High
Protect	Detailed supply chain modeling.	Create ability to create a detailed supply chain description rapidly. Simply describing a supply chain is a crucial challenge that is not well addressed at present. Assessments often fail for not understanding the underlying structure & behavior of the system being assessed.	academia, government	1-3yrs	High
Protect or GRC	How do we motivate suppliers to become trusted suppliers- what incentives do they need?	Create a broader base of trusted suppliers.	all	3-5yrs	High
Provenance & Pedigree	On interfaces where data is converted between electrical & optical bits, ensure nothing causes change.	There is no protection currently on such interfaces.	academia, government	Hard problem	High
Provenance & Pedigree	Need to develop models of supply chain lifecycles for ICT products.	Aim would be to gain clearer idea of what parts of supply chain are more vulnerable to subversion by malicious actors. This would assist decision makers in allocating resources to improve integrity of supply chains for various types of products.	industry	1-3yrs	High
Provenance & Pedigree	Look at supply chain sub tiers.	Establish ability to explore into sub tiers of a given supply chain. Transparency beyond 1st tier is lacking.	industry, government	3-5yrs	Urgent
recover, provenance, ant-counterfeit	3D printing for SCRM, additive manufacturing.	Being able to replace bad equipment or produce additional under critical circumstances.	academia	Hard problem	High
Respond	Cost of alternatives.	Being able to change suppliers quickly.	industry	1-3yrs	Low
Response	Following a real world event (e.g. earthquake, company bankruptcy) - map the effects on a organization's supply chain.	Determine impact on supply chain.	government	3-5yrs	Medium

Appendix C: List of Acronyms

APT - Advanced Persistent Threats

CIO - Chief Information Officer

CNCI - Comprehensive National Cybersecurity Initiative

COTS - Commercial off-the-shelf

DDC - Diverse Double-Compiling

DoD - Department of Defense

FAR - Federal Acquisition Regulation

ICT - information and communications technologies

IR - Interagency Report

NIST – National Institute of Standards and Technology

OTTF - Open Group Trusted Technology Forum

RFP - Request for Proposal

SCRM - supply chain risk management

SDLC - Software Development Life Cycle

SP - Special Publication

TRL - Technology Readiness Level

USG - United States Government

UTC - Utilities Telecom Council