ICT Supply Chain Risk Management

October 15-16, 2012

Conference Agenda

Final Agenda

Monday, October 15

8:00-8:30 am **Registration**

Plenary	Green Auditorium

8:30-8:45 am **Welcome and Opening Remarks**

Donna Dodson
Chief, Computer Security Division, IT Laboratory, NIST

8:45-9:00 am **Workshop Overview**

9:00-9:45 am **Supply Chain Risk: Stagnation or Transformation?**

Gary S. Lynch
Global Leader, Risk Intelligence and Supply Chain Risk, Marsh Risk Consulting & Author

Gary will offer his unique perspective on the current state of risk management across multiple risk topics, industries and geographies. As Author, Global Leader, Senior Research Fellow as well as former industry Research Director and Chief Information Security and Continuity Risk Officer, he has a unique perspective of the topic. He will provide a view on:

- How the risk decision has evolved/devolved through decades of business and technology transformation.
- Significant trends that are driving greater clustered and systemic risk.
- The upside potential offered by more advanced, unified strategies.

9:45-10:30 am **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

With the increasing sophistication of cyber threats and the need for great dependability in the supply chain, NIST has developed a series of security standards and guidelines to 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. The emerging security controls in NIST Special Publication 800-53, Revision 4, to be published later this year, include specific safeguards and countermeasures to help organizations protect all aspects of their supply chain, from development to delivery to implementation and operation.

10:30-11:00 am **Supply Chain Approaches in Industry**

Taylor Wilkerson
Program Manager, LMI's Research Institute

For many years, industry has been addressing 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, an industry association focused on SCRM, and the Supply Chain Council, Taylor will present leading practices that companies are using to manage risks, including supply chain definition, risk assessment methods, risk treatment approaches, response actions, and risk recovery. This discussion will include an overview of standards being used to facilitate SCRM. This session will provide a foundation of general SCRM practices that could be applied to cybersecurity risks.

11:00-11:15 am **Break**

11:15-12:30 pm **Panel - Bridging the Divide: A discussion of Federal Government and Industry's Thoughts and Vision for ICT Supply Chain Risk Management (see panelist below for link to presentations)**

Description: In this panel, representatives from government and industry will discuss their opinions on the current state of ICT supply chain risk management and how they believe the discipline needs to progress. Panelists will discuss, among other items: their programs and approaches; what they feel is critical for the success of ICT SCRM; what is, and is not, in the scope 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.

Moderator: **Jennifer Bisceglie**, Interos
Panelists: **Joe Jarzombek**, Department of Homeland Security
Craig Corbin, World Wide Technology
Wayne Meitzler, Pacific Northwest National Laboratory, Department of Energy
John Toomer, The Boeing Company

12:30-1:30 pm **Lunch** (boxed lunches provided)

1:30-2:00 pm **Program Protection Planning in a Global Supply Chain**

Mitchell Komaroff
Director, Trusted Mission Systems and Networks, DoD CIO

2:00-5:30 pm: Breakout Sessions Green Auditorium

Session A: Foundational Underpinnings **Lecture Room A**

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 will identify and evaluate existing terms and definitions used throughout industry, academia and government, in order to develop

an ICT supply chain lexicon and taxonomy that can act as the foundation for future ICT SCRM efforts.

Objectives:

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

Session B : Tools, Technologies, and Techniques **Lecture Room B**

Facilitator: **Dr. Sandor Boyson**, University of Maryland
Hart Rossman, 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. This session will seek to identify available and developing ICT SCRM tools, technologies, and techniques and evaluate their benefits and limitations. Areas throughout the system lifecycle where existing tools, technologies, and techniques are inadequate to reasonably mitigate ICT supply chain risks will be identified as potential areas of opportunity.

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.

ICT Supply Chain Risk Management

October 15-16, 2012

Conference Agenda

Final Agenda

Tuesday, October 16

9:00-12:30 pm **Breakout Sessions**

Session C : Practices and Standards **Lecture Room A**

Facilitator: **Don Davidson**, DOD
Nadya Bartol, ISO/IEC 27036 Editor

Overview: The 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).

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 will review the purpose, scope, effectiveness, and development approaches of various ICT SCRM standards and identify areas where additional standards or guidance is needed and how it should be developed.

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.

Session D: Research and Resources **Lecture Room B**

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. This session will identify recent and current research that seeks a further understanding of the ICT supply chain, helps mitigate risks, locates various resources that may be useful to both the research and implementation of ICT SCRM, and detects those areas where additional research or resources are needed.

ICT Supply Chain Risk Management
Final Agenda

Objectives:

- Identify recent and current research seeking to 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.

12:30-1:30 pm **Lunch** (boxed lunches provided)

1:30-2:00 pm **ICT Supply Chain Risk Management from the Utilities Perspective**

Connie Durcsak
President and CEO, Utilities Telecom Council

Connie will address the utilities sector perspective on ICT SCRM and its importance to keeping the national critical infrastructure secure. Utilities Telecom Council is the source and resource for information and communications technology (ICT) solutions, collaboration, and advocacy for utilities and other critical infrastructure industries. 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 smartgrid. Connie will discuss a paradox created by the fact that the systems running those critical functions are increasingly relying 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. The majority of ICT SCRM efforts to date focused on US government, defense sector, IT, and telecommunications. UTC believes that utilities are the next frontier of tailoring and applying ICT SCRM practices.

2:00-5:15 pm	Presentation of Findings	Green Auditorium

FINDINGS: Session A

Break

FINDINGS: Session B

FINDINGS: Session C

FINDINGS: Session D

5:15-5:30 pm **Closing Remarks**