CONFERENCE AGENDA

GOALS:

1. Share the current findings from NIST's research on industry best practices in Cyber Supply Chain Risk Management.
2. Validate the current findings and receive additional input from stakeholders.
3. Receive input to inform future versions of the Cybersecurity Framework and other cybersecurity and supply chain risk management initiatives.

THURSDAY, OCTOBER 1

7:45 AM – 8:45 AM **Registration**

PLENARY SESSION — **Red Auditorium**

8:45 AM – 9:00 AM **Welcome**

Donna Dodson
Chief Cybersecurity Advisor, Information Technology Laboratory, NIST

9:00 AM – 9:30 AM **Workshop Overview**

9:30 AM – 10:30 AM **Panel 1 - Cyber Supply Chain Risk**

Description: Many organizations are familiar with cybersecurity risks and well versed in supply chain risks. How these risks intersect is an unresolved and often bewildering topic for many. This panel will discuss different types of cybersecurity risks that affect the supply chain, and supply chain risks that affect cybersecurity – together called cyber supply chain risks. Panelists will present anecdotal evidence of how these risks can affect organizations and why organizational risk managers should care.

Moderator: **Michael Wagner**, Johnson & Johnson

Panalists: **Kevin Engfer**, Northrop Grumman
David Brown, Intel Corporation
Jim McConnell, Verizon

10:30 AM – 11:00 AM ***BREAK***

TIMES AND SCHEDULE SUBJECT TO CHANGE

CONFERENCE AGENDA

11:00 AM – 12:30 PM Panel 2 - Organizational Strategies

Description: Over the last several years, many organizations have launched strategies to mitigate and manage their cyber supply chain risks. This panel will provide a brief overview of some of the "best practices" organizations have established related to risk identification and management, supplier selection and management, as well as the tools, technologies, and processes they employ. Panelists will discuss how their organizations strategically address their cyber supply chain risks as part or alongside of their quality, supply chain resilience, physical security, and cybersecurity programs.

Moderator: **Dr. Sandor Boyson**, Supply Chain Management Center, University of Maryland

Panalists: **Edna Conway**, Cisco Systems
Robert (Bob) Smola and **Sharlin Barfield**, John Deere
Michael Wagner and **Tu Tran**, Johnson & Johnson
Phil Seward, Schweitzer Engineering Laboratories (SEL)

12:30 PM – 1:30 PM ***LUNCH***

1:30 PM – 4:30 PM BREAKOUT SESSIONS

Breakout Session A: Supply Chain Risk and Risk Management — Lecture Room A, Lecture Room B

Different risk groups across the company– procurement, supply chain continuity, quality assurance, physical security – have processes and tools that can help narrow cybersecurity risks to the supply chain. For example, supplier selection and management practices (typically the procurement or sourcing group), supply chain mapping tools (supply chain continuity group), track and trace tools (quality assurance group) are fundamental to supply chain cybersecurity as well. This session will explore and seek input to the best practices and tools used by different operational units that can do double duty in mitigating cybersecurity risks to the supply chain. It will also explore seek input on how best practices in cyber supply chain risk management can reinforce more traditional supply chain and enterprise risk management goals.

Breakout Session B: Organizational Strategies and Supplier Selection and Management — Lecture Room D, Heritage Room

Traditionally, when anyone mentions cyber supply chain security, everyone looks to the IT group. However, cybersecurity risks cut across different operational units. Cyber supply chain risks can emerge at any point and time in a product or service life cycle. This session seeks input on best practices to create better coordination and collaboration among different functional groups, supplier selection and management approaches and the business case for an enterprise-wide approach to supply chain risk management.

4:30 PM – 5:00 PM DAY'S SUMMARY AND TEXT POLL OF THE AUDIENCE — Red Auditorium

TIMES AND SCHEDULE SUBJECT TO CHANGE

CONFERENCE AGENDA

FRIDAY, OCTOBER 2

PLENARY SESSION	Red Auditorium

8:00 AM – 8:15 AM **Recap of the Previous Day and Direction for Today**

8:15 PM – 8:45 PM **Keynote Address**

Linda Conrad
Head of Strategic Business Risk, Zurich Insurance Group, Global Corporate in North America

Cyber Insecurity: better managing cyber risks
Technological defenses like firewalls, passwords and encryption are critical but cannot fully protect organizations against potential data loss and business interruptions that can result from cyber disruptions. Linda will discuss:

- The cyber-security landscape, global threats, and best practices.
- The potential impacts to third-party liability as well as first-party business interruption and property damage.
- The ways to identify and quantify the key exposures and steps to improve an organization's cyber risk profile by reviewing the potential for security losses and other breaches to itself or its suppliers.
- The development of an action plan to help stress test and improve an organization's overall information security and business resilience.

8:45 AM – 10:00 AM **Panel 3 - Standards and Best Practices**

Description: Several industry organizations in multiple critical infrastructure sectors have put forth standards, principles, and best practices targeting a variety of audiences. These cover a wide range of audiences in numerous industries and contexts that together provide a view into the entire ICT supply chain, including acquirers, and COTS providers and manufacturers. These documents range from formal standards coupled with conformance criteria, to practical guidelines for acquirers. This panel will include representatives of several such organizations who will provide an overview of their initiatives.

Moderator: **Jon Boyens**, Computer Security Division, NIST

Panalists: **Nadya Bartol**, Utilities Telecom Council (UTC)
Chris Eisenbrey, Edison Electric Institute (EEI)
Steve Griffith, National Electrical Manufacturers Association (NEMA)
Andras Szakal, The Open Group
Catherine Ortiz, DoD Trusted Foundry Program

10:00 AM – 10:30 AM ***BREAK***

CONFERENCE AGENDA

10:30 AM – 12:30 PM **Facilitated Discussion**

Standards mapping overview and feedback into the Cybersecurity Framework Core and potential gaps. There will be a discussion and audience input to follow the presentation.

12:30 PM – 12:45 PM **Workshop Summary / Closing Remarks**

What was discussed, what was discovered, what are the general impressions from the 2 days, poll results and next steps.

TIMES AND SCHEDULE SUBJECT TO CHANGE