Cybersecurity Framework Workshop

Carnegie Mellon University

May 29-31, 2013

Cybersecurity Framework Workshop Objectives:

Create the initial body of standards, guidelines, best practices, tools and procedures for cybersecurity management of traditional information technology (IT) and industrial control systems (ICS) that will be used for the initial Draft Framework.

Jointly develop cross-sector principles, common points and themes and identify initial gaps.

AGENDA-Wednesday, May 29, 2013

9:00 AM Welcome Patrick Gallagher, Director, NIST

9:20 AM Overview of Workshop Logistics

9:45 AM Overview of NIST Approach to Developing the Framework

10:15 AM Break

10:35 AM NIST Preliminary Analysis of Comments

11:45 AM Rules of Engagement for Workshop Tracks and Participation

12:00 PM Lunch

1:15 PM Track Working Sessions - All attendees will cycle through all tracks during the workshop. The Principles, Common Points and Initial Gaps that were identified in the initial analysis of the RFI responses were used to create to the Tracks. Attendees should be prepared to discuss specific standards, guidelines, and practices identified in the RFI responses. Track Session details are below full agenda.

Workshop Track 1: Business of Cyber Risk

Workshop Track 2: Threat Management

Workshop Track 3: Cybersecurity Dependencies and Resiliency

Workshop Track 4: Cybersecurity Progression and Maturity: From Basics to Advanced Cybersecurity

4:30 PM Adjourn

AGENDA-Thursday, May 30, 2013

9:00 AM Opening Plenary
Jared L. Cohon, President, Carnegie Mellon University
Bruce McConnell, Acting Deputy Under Secretary, DHS

9:45 AM Track Working Sessions

Workshop Track 1: Business of Cyber Risk

Workshop Track 2: Threat Management

Workshop Track 3: Cybersecurity Dependencies and Resiliency

Workshop Track 4: Cybersecurity Progression and Maturity: From Basics to Advanced Cybersecurity

12:30 PM Lunch

1:45 PM Track Working Sessions

Workshop Track 1: Business of Cyber Risk

Workshop Track 2: Threat Management

Workshop Track 3: Cybersecurity Dependencies and Resiliency

Workshop Track 4: Cybersecurity Progression and Maturity: From Basics to Advanced Cybersecurity

4:30 PM Adjourn

AGENDA - Friday, May 31, 2013

9:00 AM Track Working Sessions

Workshop Track 1: Business of Cyber Risk

Workshop Track 2: Threat Management

Workshop Track 3: Cybersecurity Dependencies and Resiliency

Workshop Track 4: Cybersecurity Progression and Maturity: From Basics to Advanced Cybersecurity

11:30 AM Plenary - Discussion of Next Steps

12:30 PM Adjourn

Workshop Track 1: Business of Cyber Risk

Track Context: Cybersecurity is one component of the overall business risk environment and should feed into an organization's risk considerations. Cybersecurity risk, as with all risks, cannot be completely eliminated, but instead must be managed through informed decision-making processes and matched with organization's overall business needs.

Track Goals: Ensure standards, guidelines, best practices, tools and procedures critical infrastructure owners and operators use to frame, assess, respond, and monitor cybersecurity and privacy risk in the context of their business/enterprise operations are included in the RFI response data. Address governance and risk management.

Inputs: (From RFI Response) List of laws, regulations, standards, best practices

Output:

- Validated/updated list of relevant policy drivers for identifying, addressing, managing, and responding to cyber and privacy risk
- Successful implementation strategies
- Useful metrics

Workshop Track 2: Threat Management

Track Context: The current threat landscape is constantly changing. The attackers are continuously innovating and changing how they gain access to critical systems. As such, critical infrastructure needs to understand, analyze, and adapt to the variety of threats.

Track Goals: Ensure standards, guidelines, best practices, tools and procedures, and information sources to identify threats are identified and included as well as threat response actions. Identify any privacy and civil liberties concerns. Examine best practices in cybersecurity and technology that can enhance privacy and civil liberties.

Inputs: (From RFI Response) List of current threats and threat related information sharing capabilities/needs/gaps.

Outputs:

- Validated/updated list of relevant threats, threat management, threat information sources
- Implementation of threat remediation strategies along with associated risk for privacy and civil liberties.
- Metrics and best practices

Workshop Track 3: Cybersecurity Dependencies and Resiliency

Track Context: Cybersecurity cannot operate in isolation; it must be considered and incorporated into the business missions and business operations of the critical infrastructure. Owners/operators of critical infrastructure depend on safe, reliable, and resilient delivery of critical services and functions that are enabled by information systems.

Track Goals: Identify the critical services which are dependent on IT/ICS for delivery and operations. Identify how these critical services are protected. Identify best practices around resiliency. Clearly understand and capture the connections between business mission needs and IT/ICS security requirements. Identify the privacy and civil liberties concerns. Understand how privacy and civil liberty considerations impact decisions. Examine best practices in cybersecurity and technology that can enhance privacy and civil liberties in the critical infrastructure.

Inputs: List of current resiliency best practices from the RFI responses.

Output:

- Validated list of resiliency best practices along with associated risk for privacy and civil liberties.
- Map the intersection of cyber and other threat protections.

Workshop Track 4: Cybersecurity Progression and Maturity: From Basics to Advanced Cybersecurity

Track Context: Cybersecurity is not a one-size-fits-all endeavor. Each organization has different needs and resource levels. A broad range of activities can be utilized to increase the organization's cybersecurity posture, which can vary depending on sector and business needs.

Track Goal(s):
Identify of maturity models for inclusion into the initial data set. Identify IT/ICS "cybersecurity hygiene" activities (access control, cryptography, etc.) for inclusion into the data set. Identify risk of such activities to privacy and civil liberties.

Inputs: List of maturity models; List of current IT/ICS"cybersecurity hygiene" activities

Output:

- Validated list of maturity models.
- Validated list of IT/ICS "cybersecurity hygiene" activities along with associated risk for privacy and civil liberties.