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 that will be used to populate the initial Draft Cybersecurity Framework.

Achieve consensus on cross-sector principles, common points and themes and identify initial gaps.

AGENDA
Wednesday, May 29, 2013

8:00 AM Registration
Wean Commons, 1st Floor, University Center (UC)

Morning sessions will be at the McConomy Auditorium, 1st floor, UC

9:00 AM Welcome
Patrick Gallagher
Under Secretary of Commerce for Standards and Technology and
Director of the National Institute of Standards and Technology

9:35 AM Overview of NIST Approach to Developing the Framework
Adam Sedgewick, Senior Information Technology Advisor, NIST

10:05 AM Break

10:35 AM NIST Preliminary Analysis of Comments
Victoria Pillitteri, NIST
Jon Boyens, NIST
Matthew Scholl, NIST
Kevin Stine, NIST
Lisa Carnahan, NIST

11:30 AM Closing Morning Plenary
Ari Schwartz, Department of Commerce

11:45 AM Workshop Logistics and Rules of Engagement

12:00 PM Lunch (*Wiegand Gymnasium, 1st floor, UC)*

1:15 PM Track Working Sessions - All attendees will cycle through all tracks during the workshop. Details on the context and the goals of the Tracks are below.

Workshop Track 1: Business of Cyber Risk
Workshop Track 2: Threat Management
Workshop Track 3: Cybersecurity Dependencies and Resiliency
Workshop Track 4: Progressive Cybersecurity: From Basics to Advanced Cybersecurity

Note: Attendees have been sorted into groups for the working sessions. The back of your badge should have a sticker, which will correspond to the designation below. Group 8 badges do not have dots. The same groups will meet in the same room for all working sessions during the workshop.

Group #	Designation on Badge	Location for Group
Group 1	Large Green Dot	Rangos 1, 2nd floor, UC
Group 2	Red Dot	Rangos 2, 2nd floor, UC
Group 3	Yellow Dot	Rangos 3, 2nd floor, UC
Group 4	Green Dot with Star	Boardroom A, Posner Center
Group 5	Red Dot with Star	Boardroom B, Posner Center
Group 6	Blue Dot	Mellon Auditorium, Posner Hall
Group 7	Small Green Dot	Gregg Hall, Room 100, Porter Hall
Group 8	No Dot	INI Distributed Education Center (DEC), Robert Mehrabian Collaborative Innovation Center

4:30 PM Adjourn

Thursday, May 30, 2013

9:00 AM Opening Plenary
McConomy Auditorium, 1st floor, UC

Jared L. Cohon, President, Carnegie Mellon University
Bruce McConnell, Acting Deputy Under Secretary, DHS

9:45 AM Track Working Sessions

Workshop Track 1: The Business of Cyber Risk
Workshop Track 2: Threat Management
Workshop Track 3: Cybersecurity Dependencies and Resiliency
Workshop Track 4: Progressive Cybersecurity: From Basics to Advanced Cybersecurity

Note: Groups meet in the same rooms as on Wednesday afternoon

12:30 PM Lunch (*Wiegand Gymnasium, 1st floor, UC)*

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: Progressive Cybersecurity: From Basics to Advanced Cybersecurity

Note: Groups meet in the same rooms as the morning

4:30 PM Adjourn

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: Progressive Cybersecurity: From Basics to Advanced Cybersecurity

Note: Groups meet in the same rooms as on Thursday

11:30 AM Plenary - Discussion of Next Steps
McConomy Auditorium, 1st floor, UC

12:30 PM Adjourn

Workshop Track Descriptions

The Principles, Common Points and Initial Gaps identified in the initial analysis of the RFI responses were used to create the Tracks.

Workshop Track 1: The 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 an organization's overall business needs.

Track Goals: Ensure the standards, guidelines, best practices, tools and procedures used by critical infrastructure owners and operators to frame, assess, respond, and monitor cybersecurity and privacy risk are included in the RFI response data.

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

Outputs:

- Validated/updated list of relevant policy drivers for *identifying, assessing, and mitigating cyber 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. Therefore, 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.

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
- 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 reliant on underlying IT.

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

Inputs: (From RFI Response) List of current resiliency best practices

Outputs:

- Validated list of resiliency best practices
- Map the intersection of cyber and other threat protections

Workshop Track 4: Progressive Cybersecurity: 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 an organization's cybersecurity posture, which can vary depending on sector and business needs.

Track Goals: Identification of maturity models for inclusion into the initial data set. Identification of "cybersecurity hygiene" activities (access control, cryptography, etc.) for inclusion into the data set.

Inputs: (From RFI Response) List of maturity models; List of current "cybersecurity hygiene" activities.

Outputs:

- Validated list of maturity models
- Validated list of "cybersecurity hygiene" activities
- Progressive list of cybersecurity activities