Cybersecurity Framework Workshop 2017
National Institute of Standards and Technology, Gaithersburg MD

May 16-17, 2017

Workshop Purpose: The purpose of this workshop is to provide attendees with the following:

1) An opportunity to provide comments and discuss the Framework Draft V1.1,
2) A forum for participants to learn from each other's experiences with the Framework, and
3) An update on Framework-related policy issues and the progress of technical work that may shape future enhancements.

Sharing will take place through panels of experts and working sessions as well as networking.

Agenda

Tuesday, May 16, 2017

7:30 AM	**Registrant Check-In –** NIST cafeteria available to attendees
8:30 AM	**Welcome to NIST**– Red Auditorium
8:45 AM	**User Experiences with the Framework (Panel)** – Red Auditorium
9:45 AM	**Recent International Use (Panel)** – Red Auditorium
10:30 AM	**Break –** NIST cafeteria available to attendees
10:45 AM	**Introduction to Draft Framework V1.1 –** Red Auditorium
11:15 AM	**Evolving the Framework through Experience (Panel)** – Red Auditorium
12:15 PM	**Breakout Session Intro and Rules of Engagement** – Red Auditorium
12:30 PM	**Lunch –** NIST cafeteria available to attendees; Many off-site options available
1:45 PM	**Working Sessions I – Draft Framework V1.1 (concurrent sessions)**
	- NCCoE Profile Development Presentation– Red Auditorium
	- V1.1: Threat Intelligence – Green Auditorium
	- V1.1: Measurement – Heritage Room
	- V1.1: Supply Chain Risk Management – West Square
	- V1.1: Identity – Lecture Room A
	- V1.1: Implementation Tiers – Lecture Room B
	- V1.1: General – Lecture Room C
	- V1.1: General – Lecture Room D
3:15 PM	**Break** – NIST cafeteria available to attendees
3:30 PM	**Working Sessions II – Special Topics (concurrent sessions)**
	- Baldrige Cybersecurity Excellence Builder Presentation – Red Auditorium
	- Coordinated Vulnerability Disclosure – Green Auditorium
	- Policy and Law – Heritage Room
	- Confidence Mechanisms – West Square
	- Future of Informative References – Lecture Room A
	- Federal Use – Lecture Room B
	- Innovations in the Framework – Lecture Room C
	- Cybersecurity Insurance and the Framework – Lecture Room D
5:00 PM	**Adjourn**

Wednesday, May 17, 2017

8:00 AM **Registrant Check-In –** NIST cafeteria available to attendees

9:00 AM **Working Sessions III – Deep Dive Topics (concurrent sessions)**

- International Alignment – Red Auditorium
- The Sector Customization Process – The Communications Sector – Heritage Room
- The Sector Customization Process – The Financial Sector – West Square
- Cyber Meets the Physical World– Lecture Room A
- Small and Medium Businesses and Cybersecurity – Lecture Room B
- Cybersecurity Governance and the Board – Lecture Room D

10:30 AM **Break** – NIST cafeteria available to attendees

11:00 AM **Continuation of Working Sessions III (concurrent sessions)**
Deep dive topics continue in their respective rooms with further discussion of topics introduced during the morning working sessions.

12:30 PM **Lunch –** NIST cafeteria available to attendees; Many off-site options available

1:30 PM **Readout of Panels**

2:30 PM **Readout of Workshop Findings and Next Steps**

3:30 PM **Adjourn**

Tuesday Afternoon Working Sessions (more topics may be added)

Proposed Version 1.1: These sessions will cover the proposed updates to the Framework. Some sessions will begin with a particular update topic (SCRM, Identity, Tiers, Threat Intelligence, Measurement) and then move on to other topics in v1.1.

Policy and Law: The Framework allows organizations to tie their regulatory and legal requirements to cybersecurity risk management. This session will highlight how to effectively use the Framework within the legal and policy arenas to effectively identity, assess, and manage cybersecurity risk.

Confidence Mechanisms: This session will use presentations and facilitated discussion to explore the different types of mechanisms used by organizations to develop/increase confidence in their ability to manage cybersecurity risk. Each of the presenters will walk through key aspects of their approach that provide value to stakeholders/customers and leverage the Framework. The facilitated discussion will include the presenters and the audience to explore topics related to considerations in the development, use, and adoption of their unique approaches; the depth/breadth of the approach, the use of measures and scale (quantitative or qualitative), translational value, and organizational focus (C-suite to cyber control implementation to user).

Federal Use: This session is for discussing ways that the Framework can provide value to the risk management programs and practices in federal agencies. This will include ways that Framework complements federal Risk Management Framework practices.

Innovations in the Framework: The Framework has been adopted by many users in industry. Some users have incorporated pieces of the Framework into their entire cybersecurity program. This session is for advanced users of the Framework to discuss challenges in deep implementations and how they tailored the Framework to fit their unique cybersecurity risk environment.

Cybersecurity Insurance and the Framework: This session will discuss the benefits to an evolving and growing insurance market of a widely used and consistent approach to understanding and communicating cyber risks. Participants will provide their experience with using the Cybersecurity Framework for developing and analyzing data and using the data for underwriting cyber risks. Additionally, the session seeks comments about how the Framework might be helpful in communicating cybersecurity outcomes in the insurance market.

Future of Informative References: The informative references began as the most cited industry standards and practices to help organizations manage cybersecurity risk. These references have since been updated and changed. This session will discuss how the Framework should be updated to handle a changing and growing standards landscape.

Coordinated Vulnerability Disclosure: There is always a risk of vulnerabilities in the software, systems, and infrastructure we rely on. These flaws are often found by external parties such as security researchers, rather than by the organization responsible for development and maintenance. Vulnerability disclosure policies and processes help organizations work with these external parties, and serve as a mechanism to receive information and mitigate vulnerabilities. Consensus is emerging on the importance of these policies and processes, and how they must reflect the diverse needs and capabilities of the organization. This session will discuss whether and how this issue could fit into the Framework, how disclosure relates to organizational risk, references, and approaches to maturity.

Wednesday Morning Working Sessions on Deep Dive Topics (more topics may be added)

International Alignment: The Framework is used increasingly by international organizations and nations to manage cybersecurity risk. More work needs to be done to help align cybersecurity strategies globally to better combat an international threat. This breakout will discuss current thinking on the topic as well as set the stage for later discussion.

Small and Medium Sized Businesses and Cybersecurity: Cybersecurity affects all organizations; small and Medium Sized Businesses (SMBs) are no exception. While the Framework was designed for organizations of all sizes, SMBs may experience challenges customizing and applying the Framework to their unique business environments. This breakout will highlight ways that SMBs are currently using the Cybersecurity Framework as well as how it can be made more usable to SMBs. Discussion will also touch on additional cybersecurity resources that would assist SMBs.

The Sector Customization Process - The Financial Services Sector: The Cybersecurity Framework lends itself to be tailored to the specific needs of each sector. This breakout will focus on how to effectively tailor the Framework in the financial services sector; it also will include discussion of the process of developing a sector profile. Participants in sectors other than financial services will find value in witnessing the process for future discussion in their sector. The discussion that follows will continue on the topic.

Cyber Meets the Physical World: The diverse use and rapid proliferation of connected devices – typically captured by the "Internet of Things (IoT)" – creates enormous value for industry, consumers, and broader society. At the same time, emerging threats, such as last year's Mirai DDoS attacks, highlight the critical need to develop and apply guidance to maintain the cybersecurity of devices and the ecosystems into which they are deployed. NIST is seeking feedback on how the Framework may be applied to the IoT, both in terms of the devices themselves, as well as their integration into broader enterprise and network environments. Topics in this breakout may include: existing IoT definitions and taxonomies and their consistency with the Framework; IoT specific threats and constraints; sector-specific considerations for IoT security; and the integration of IoT-specific threats into the Framework model.

Cybersecurity Governance and the Board: Boards of Directors are becoming much more aware of – and involved with – cybersecurity risk management policies and decisions as part of their broader enterprise risk management responsibilities. The Cybersecurity Framework has helped boards to tackle these issues. Many challenges remain about how risk management decisions affect and are affected by resource allocation, public disclosures, and risk committees. This breakout will advance the discussion and focus on how the Framework is helping and can be better utilized.

The Sector Customization Process – The Communications Sector: Within the Communications Sector, a number of organizations have developed their own methods to measure the effectiveness of NIST Cybersecurity Framework adoption. While this may be beneficial for individual organizations, it does not provide a sector-level approach to measuring Framework effectiveness. This panel will discuss potential approaches to measurement across the sector, including recent studies by sector working groups on issues related to cybersecurity, risk management, and best practices.