Cybersecurity Framework Workshop
Florida Center for Cybersecurity at the University of South Florida (USF)

Marshall Student Center, Oval Theater, 4103 USF Cedar Circle, Tampa, FL 33620
October 29-30, 2014

Workshop Purpose: To discuss initial experiences with the Framework for Improving Critical Infrastructure Cybersecurity (the Framework), with a focus on resources to help organizations use the Framework more effectively and efficiently.

Workshop Input: The Framework for Improving Critical Infrastructure Cybersecurity; the National Institute of Standards and Technology (NIST) Roadmap for Improving Critical Infrastructure Cybersecurity (the Roadmap); public Request for Information (RFI) responses; and working session objectives.

Final Agenda
Wednesday, October 29, 2014

7:00 AM   **Registration - Oval Theater**

8:00 AM   **Welcome Plenaries**
Sri Sridharan, Managing Director, Florida Center for Cybersecurity, USF
Ari Schwartz, National Security Council (NSC), Executive Office of the President
Giles Smith, Deputy Director Cyber Security and Resilience, Department for Business, Innovation and Skills (BIS), UK Government

8:30 AM   **Use of the Framework**
The objective of this panel is to share lessons learned from organizations that leveraging the Framework in their organizations.
 Moderator: Matt Scholl, NIST
 Panelists: Tim Casey, Intel Corporation
     Jefferson England, Silverstar Communications
     Kenny Mesker, Chevron

10:00 AM   **Break**

10:15 AM   **Sector Guidance for the Framework**
The objective of panel is to update participants on evolving sector needs, the utility of the Framework for these needs, and discuss some of the sector-specific priorities and challenges.
 Moderator: Thad Odderstol, Department of Homeland Security
 Panelists: Chris Boyers, AT&T
     Tamara Lance, Atmos Energy
     Karl Schimmeck, Securities Industry and Financial Markets Association (SIFMA)

11:15 AM   **Supporting Framework Implementation**

This panel will examine tools, products, standards, and services that have been developed to assist in organization's cybersecurity risk management practices.

Moderator: Dr. Robert Bishop, Dean of Engineering, University of South Florida

Panelists: Ken Gonzalez, AXELOS

Chris Halterman, Ernst & Young

Leo Staples, on behalf of Automation Federation

Rob Stroud, CA Technologies, on behalf of ISACA

Simon White, Liberty International Underwriters

12:15 PM **Rules of Engagement**

1:00 PM **Lunch**

2:00 PM **Working Sessions** – Assigned Groups and Locations on Campus
The objective of this working session is to obtain feedback on the Cybersecurity Framework itself learned through implementation. Working session objectives and discussion questions will be used to guide the discussion.

Group #	Location
1	Room 2707
2	Room 2708
3	Room 2709
4	Room 3705
5	Room 3707
6	Room 3709

5:00 PM **Adjourn Day 1**

8:00 AM   **Registration**

9:00 AM   **Topic-Specific Working Sessions 1**

Topic	Location
Authentication	Room 2707
Objective: This session will focus on authentication capabilities that can be used today and tomorrow in both IT and Industrial Control Systems (ICS). As part of the discussion, we will ask participants to describe challenges and threats posed by weak authentication mechanisms, discuss the state of the market for strong authentication solutions, examine barriers to the deployment of multi-factor authentication (MFA) in legacy systems, and identify gaps in requirements and standards that need to be addressed.	
Automated Indicator Sharing	Room 2709
Objective: This session will focus on identification of key practices - including trust models, standards, services, and tools - for sharing threat data through actionable common indicators. The session will examine use cases to frame the discussion on the benefits, challenges, and barriers for sharing cyber threat data, and how to leverage that data within an enterprise-wide cybersecurity program.	
Supply Chain and Conformity Assessment	Room 2708
Objective: This session will discuss supply chain risk management and conformity assessment in relation to the use of the Cybersecurity Framework, including future work and opportunities for engagement.	
Cybersecurity Workforce	Room 3711
Objective: This session will discuss the current and future critical infrastructure cybersecurity workforce needs, and consider strategies, practices, tools, and research needed to expand and fill the workforce pipeline.	
Standards Supporting the Framework	Room 3709
Objective: This session will discuss initial experiences in leveraging standards – both cross-sector and sector-specific – to use the Framework and consider strategies to identify and fill gaps in order to facilitate more effective and efficient implementation of cybersecurity programs.	
Privacy Methodology	Room 3705
Objective: This session will discuss and enable participants to share any best practices or challenges in using the privacy and civil liberties methodology to integrate privacy risk mitigation within the Framework.	

10:15 AM   **Break**

10:30 AM   **Topic-Specific Working Sessions 2 –** Same selection of topics as shown above

12:00 PM   **Lunch**

1:00 PM   **Plenary**
Chuck Romine, Director, Information Technology Laboratory, NIST

1:15 PM   **The View of Policy Makers**
The objective of this panel is to discuss current cybersecurity policy initiatives, including national, international, and regional. It will highlight not only how these organizations view the Framework, but their related policies and initiatives.

      Moderator: Norma Krayem, Squire Patton Boggs
      Panelists: Miles Keogh, National Association of Regulatory Utility Commissioners (NARUC)
                   Jeanette Manfra, NSC, Executive Office of the President
                   Jamia McDonald, Rhode Island Emergency Management Agency
                   Nestor Ramirez, US Patent and Trademark Office
                   James Snook, Office of Cyber Security and Information Assurance (OCSIA), UK Government
                   Aristotelis Tzafalias, European Commission

2:15 PM   **Updates from NIST**
This Panel will discuss current priorities and trends around Authentication, Cyber-Physical Systems, Privacy, and Applied Cybersecurity and their relation to the Framework and Roadmap areas.

      Moderator: Donna Dodson, NIST
      Panelists: Jeremy Grant, NIST
                   Naomi Lefkovitz, NIST
                   Nate Lesser, NIST
                   Vicky Pillitteri, NIST

3:00 PM   **Summary of Workshop and Discussion of Next Steps**
This Panel will present an initial analysis of the RFI responses and the workshop, and discuss next steps.

3:30 PM   **Adjourn Workshop**