FOURTH ANNUAL

Secure and Resilient Cyber Architectures Invitational
Moving Cyber Resilience into Practice

May 28-29, 2014, 8:00 a.m.-5:00 p.m.

There is an optional Cyber Resilience Tutorial planned for May 27, 1-5 p.m., at MITRE McLean. Space is limited.

Day 1: May 28

8:00 – 9:00	Booths, Registration and Continental Breakfast
9:00 – 9:15	**Workshop Overview** Bill Neugent, MITRE
9:15 – 9:45	**Welcome** Gary Gagnon, Senior Vice President and Chief Security Officer of The MITRE Corporation
9:45 – 10:30	**Enabling Secure and Resilient Infrastructures in the Public and Private Sectors** Brigadier General (retired) Gregory J. Touhill, DHS Deputy Assistant Secretary for Cyber Security Operations and Programs
10:30 – 10:45	Break and Commercial Booths
10:45 – 11:30	**Managing Cyber Resilience in Financial Market Infrastructures** Ken Buckley, Associate Director, Division of Reserve Bank Operations and Payment Systems, Board of Governors of the Federal Reserve System
11:30 – 12:15	**Running Cyber Tabletop Exercises and Lessons Learned for Resilience** David Dumas, Senior Network Security Engineer, Verizon Security Operations
12:15 – 1:00	Lunch and Commercial Booths
1:00 – 2:00	**Panel: Putting Cyber Resilience into Practice** Panel Moderator: Kevin Bingham, Technical Director, NSA IAD Mitigations Group
2:00 – 3:20	**Working Groups Initial Meeting and Commercial Booths** (details on back) • Track 1: Applying Cyber Resilience to Space (chaired by Dr. Roberta Ewart, SMC) • Track 2: Resilient Critical Infrastructures: Applying Cyber Resilience and Overcoming the Barriers to Acceptance (chaired by Dr. Nick Multari, PNNL) • Track 3: Cyber Resilience and Its Role in the Systems Engineering Life Cycle (chaired by Dr. Ron Ross, NIST) • Track 4: Designing a Cyber Resilience Challenge for Integration and Demonstration (chaired by Harriet Goldman, MITRE)
3:20 – 3:30	**Day 1 Wrap-Up** Bill Neugent
3:30 – 5:00	Commercial Booths and Optional Breakout Discussions
5:00 – 7:00	Networking and Social Hour, Commercial Booths

Day 2: May 29

7:30 – 8:30	Continental Breakfast
8:30 – 12:00	**Track Breakouts** (details on back) • Track 1: Applying Cyber Resilience to Space (chaired by Dr. Roberta Ewart, SMC) • Track 2: Resilient Critical Infrastructures: Applying Cyber Resilience and Overcoming the Barriers to Acceptance (chaired by Dr. Nick Multari, PNNL) • Track 3: Cyber Resilience and Its Role in the Systems Engineering Life Cycle (chaired by Dr. Ron Ross, NIST) • Track 4: Designing a Cyber Resilience Challenge for Integration and Demonstration (chaired by Harriet Goldman, MITRE)
10:25 – 10:40	Break
12:00 – 12:45	Lunch
12:45 – 3:00	**Track Breakouts Continue**
3:00 – 4:30	**Track Readouts and Way Forward**

Vendors include: *Blue Ridge Networks, Bromium, CrowdStrike, FireEye, ForeScout, GD Fidelis Cybersecurity Solutions, Ionic Security, Palo Alto Networks, SCIT Labs, Tibco Streambase, Unisys*

MITRE

FOURTH ANNUAL

Secure and Resilient Cyber Architectures Invitational
Moving Cyber Resilience into Practice

May 28-29, 2014, 8:00 a.m.-5:00 p.m.

There is an optional Cyber Resilience Tutorial planned for May 27, 1-5 p.m., at MITRE McLean. Space is limited.

Working Group abstracts

Track 1: **Applying Cyber Resilience to Space**
This track is intended to develop and produce community-derived and actionable results for applying cyber resilience to cyber-enhanced space operations and cyber security efforts for the space community. Topics to be discussed include coming up with a better understanding of critical needs based on the available science and technology options; sharing insights on the current state of practice; and identifying the development priorities driving user consideration. The working group will develop and document the community-vetted best practices and practical steps to assist in moving space cyber resilience from theory to practice.

Track 2: **Resilient Critical Infrastructures: Applying Cyber Resilience and Overcoming the Barriers to Acceptance**
This track examines the application of cyber resilience to critical infrastructures and barriers to acceptance by focusing on regulations, validation, privacy, transparency, and access control. We will discuss how these barriers can be overcome and a path for easing the concerns of decision makers.

Track 3: **Cyber Resilience and Its Role in the Systems Engineering Life Cycle**
This track focuses on the relationship between cyber resilience and the systems engineering life cycle. We will identify where and how to better incorporate cyber resilience into the systems engineering life cycle and recommend concrete actions that could be taken this year to achieve better outcomes.

Track 4: **Designing a Cyber Resilience Challenge for Integration and Demonstration**
The intended outcome of this track is to construct one or more problem scenarios, incorporating a set of threat vectors and resilient technologies/products that mitigate them. The problem scenarios will serve as a starting point for developing integrated demonstrations to prove or disprove the effectiveness of the selected technologies/products. The results of the demonstrations will be presented at the 2015 Invitational.

MITRE