T&E to Disrupt the Cyber Attack Life Cycle

PROGRAM GUIDE

March 15 - Pre-Workshop Tutorials
March 16-17 - Cyber Security Workshop Plenary and Technical Track Sessions

---

Residence Inn by Marriott ~ Arlington, VA
Hosted by the ITEA George Washington Chapter

CONTINUING EDUCATION UNITS (CEUs)

Each of the 4-hour Pre-Workshop Tutorials provide 4 contact hours of instruction (4 CEUs) that are directly applicable to your professional development program, including the Certified Test and Evaluation Professional Credential (CTEP).

In addition to the Pre-Workshop Tutorials, the Workshop provides 4 contact hours of instruction (4 CEUs) for each half-day, 8 contact hours of instruction (8 CEUs) for each full-day, that are directly applicable to your professional development program, including the Certified Test and Evaluation Professional Credential (CTEP).

THANK YOU TO OUR SPONSORS!

Platinum Level Sponsor

EWA Government Systems, Inc.

Enabling a more secure future

Gold Level Sponsors

AMERICAN™ SYSTEMS

wyle

Bronze Level Sponsor

ACQUIRED DATA SOLUTIONS

Workshop Program Committee

Program Chair

Jeff McNeil, PhD., Professor, Clemson University, and Principal Investigator, Test Capabilities Development, OUSD (AT&L)/TRMC

Technical Co-Chairs

Mr. Adam Tanverdi and Robert Tamburello, Ph.D.

Volunteers

Ms. Kyra Ball	**Ms. Ellen Byington**	**Ms. Morgan Broyles**
Ms. Alison Caughman	**Ms. Camellia Cupp**	**Paul Dailey, Ph.D.**
Mr. Tony Garces	**Mr. Jonathan Jones**	**Mr. Gerard Nelson**
Ms. Eileen Redd	**Mr. Steve Seiden**	**Adel Slamani, Ph.D.**
Mr. Geoffrey Wilson	**Ms. Krista Wilson**	

Welcome to the 2016 Cyber Security Workshop!

We appreciate you taking the time and effort to join us, and we hope that you find this year's Workshop personally and professional rewarding.

This year's program is focused on T&E support to achieving resilience through disrupting the cyber-attack lifecycle. The Program includes operational perspectives of defending DoD platforms, systems, and networks, and how T&E can set the conditions for success. The Program includes perspectives from community leaders, cyber range providers and emerging initiatives, and coalition, industry and academic partners. The program includes a half day of classified track sessions addressing Offensive Cyberspace Operations (OCO) capabilities, Threat Resources, and Cyber-EW convergence.

We also appreciate your support of the Association, and your personal commitment to the professional excellence embodied in advancing the test and evaluation industry. Please let us know what else we can be doing to assist your personal and professional success.

TUESDAY, MARCH 15TH

Pre-Workshop Tutorials (Separate fee required)

8:00 a.m. to Noon – Morning Tutorials

TENA and JMETC

Instructor: **Mr. Gene Hudgins** - Wyle

The Test and Training Enabling Architecture (TENA) was developed as a United States (US) Department of Defense (DoD) Central Test and Evaluation Investment Program (CTEIP) project to enable interoperability among ranges, facilities, and simulations in a timely and cost-efficient manner, as well as to foster reuse of range assets and future software systems. TENA provides for real-time software system interoperability, as well as interfaces to existing range assets, Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems, and simulations. TENA has also been selected for use in Joint Mission Environment Test Capability (JMETC) events, well-designed for its role in prototyping demonstrations and distributed testing.

JMETC is a distributed live, virtual, and constructive (LVC) testing capability developed to support the acquisition community during program development, developmental testing, operational testing, and interoperability certification, and to demonstrate Net-Ready Key Performance Parameters (KPP) requirements in a customer-specific Joint Mission Environment (JME).Through its persistent connectivity established on the Secure Defense Research Engineering Network (SDREN), a part of the Global Information Grid (GIG), JMETC provides readily available connectivity to the Services' distributed test capabilities and simulations, as well as industry test resources.

JMETC is also aligned with the Joint National Training Capability (JNTC) integration solutions to foster test, training, and experimental collaboration. TENA provides the architecture and software implementation and capabilities necessary to quickly and economically enable interoperability among range systems, facilities, and simulations. TENA also fosters range asset reuse for enhanced utilization and provides compos-ability to rapidly assemble, initialize, test, and execute a system from reusable, interoperable elements. Because of its field proven history and acceptance by the range community, TENA provides a technology already being deployed in the US Department of Defense, and being used by Coalition partners as well. This tutorial will inform the audience as to the current impact of TENA and JMETC on the Test, Training, and Evaluation community; and its expected future benefits to the range community and the warfighter.

Cybersecurity Test & Evaluation and the National Cyber Range

Instructors: **Mr. Pete Christensen**, TRMC/NCR, and **Ms. Lizann Messerschmidt** - The MITRE Corporation

This tutorial is intended for managers and practitioners who are required to conduct test and evaluation of systems operating in Cyberspace. The tutorial introduces key concepts associated with Cyberspace and Cyberspace Operations. The material will cover both Offensive Cyber Operations and key avenues of attack as well as Defensive Cyber Operations and strategies for defending against those attacks. With respect to the DOD 5000 Process, we will discuss approaches for developing and testing systems to ensure mission effectiveness in a contested Cyber Environment. Finally, we will overview available resources and ongoing initiatives to improve Cyberspace T&E.

Cyber DEF/TEMP/Test Plan Development

Instructors: **Suzanne Beers, Ph.D**., and **Ms. Jean Petty** - The MITRE Corporation

The Developmental Evaluation Framework (DEF) was created to provide a systematic and deliberate Developmental Test and Evaluation (DT&E) planning mechanism to inform acquisition, programmatic and technical decisions early and throughout the acquisition cycle. It includes cybersecurity T&E, using a process developed jointly by DASD(DT&E) and DOT&E. The DEF articulates the Test and Evaluation Master Plan's (TEMP) DT&E strategy by describing: (1) decisions to be informed and the essence of the decision-makers' information needs; (2) evaluation of the system's performance, interoperability, cybersecurity, and reliability; and (3) the test and modeling and simulation events that will generate the data for the evaluation to inform the decisions.

DASD(DT&E) has been assisting programs build their TEMP's DEF through an engagement with the program offices - the DEF Core Team. The DEF Core Team is a DASD(DT&E) facilitated discussion with the Program Manager, Chief Engineer, Chief Developmental Tester, and Lead Developmental Test Organization. At the end of the day, a draft DEF is developed for insertion into the program's TEMP. After the DEF lays the program's DT&E strategy foundation, DT&E plans focused on performance, interoperability, cybersecurity, and reliability can be fleshed out. DASD(DT&E) and DOT&E have developed a six-step process for cybersecurity T&E. The first four steps in the six-step process comprise the recommendation for Cybersecurity DT&E planning and execution and the last two steps encompass the cybersecurity OT&E activities. DASD(DT&E) and DOT&E developed detailed guidance to implement the process and it is covered in this tutorial.

This tutorial will provide the what, why, and how of constructing a DEF and cybersecurity DT&E plan.

1:00 p.m. – 5:00 p.m. – Afternoon Tutorials

Software Assurance

Instructor: **Mr. Bob Martin**, Senior Secure Software & Technology Principal Engineer - The MITRE Corporation

This tutorial will explore how the directed activities in the DoDI 5200.44, DoDI 8510.01-2014, and DoDI 8500.01-2014, and their Program Protection Plans, Developmental test and evaluation, Systems Engineering design & architecture reviews can be used to gain assurance about DOD Software and its resilience to attack.

Improving our assurance that the mission will not be circumvented, undermined, or unnecessarily put at risk through attacks on the software that provides critical mission capabilities requires a shift in focus and integration of many types of assessment activities across the acquisition life cycle.

This tutorial will also cover how the public vulnerability information, along with an understanding of the weaknesses in commercial and open source software puts the mission at risk. Publicly available about these weaknesses and the patterns of attacks they are susceptible to can be used to test GOTS and custom software so we have insight into how attackable DOD Software is and what can be done to address those risks.

SimSpace Demonstration

Instructors: **Mr. Lee Rossey** - SimSpace Corporation CTO and Co-Founder

In this tutorial we will demonstrate the ability to operate a fully-featured cyber range in the public cloud able to run an arbitrary number of complex network environments ranging from hundreds to thousands of hosts in a secure and accessible manner. The tutorial will cover the steps required to define an arbitrary network, customize and deploy the hosts in the cloud, run a sample test, execute a fully automated sophisticated attack scenario and visualize and analyze the results.

Components of the range demonstrated in this tutorial include the ability to rapidly define and build tailored network environments. Once defined one of the advantages of the cloud is the ability to quickly duplicate existing setups (blueprints) to provide unique and customized instances for each user or test and then deploy for execution. The nearly unlimited storage and compute capacity provides the ability to run networks on-demand for users to run at the time and place of their choosing avoiding the typical scheduling challenges. Once a network is started we will highlight the high fidelity user emulation capabilities to model realistic enterprise activity. We will also run sophisticated, automated attack scenarios able to evade existing defenses on a fully patched and defended network using our zero-day emulator. Using the automated red team capability (auto-OPFOR) the attacks will step through a kill chain from the reconnaissance phase to the exploitation and movement within the network to the compromise and ex-filtrate a large collection of sensitive documents. This automated attacker is well suited for individual and team based self-learning as well as product development and regression testing. As the attack progresses through the network it will be visualized on a network map to provide overall status and awareness. We will then use the mission impact tool to visually display the effect of the attacks or defender actions by mapping key IT systems to business functions. Finally, we will demonstrate is the tracker application used to record red (adversary), white (control cell) and blue (defender) actions and intent to provide overall control, status and quantitative measurements for training, exercises and assessments.

WEDNESDAY, MARCH 16TH

Workshop Opening Plenary Session

8:00 a.m. Welcome – **Mr. Gene Hudgins -** ITEA President

8:05 a.m. Opening Remarks – **Jeff McNeil, Ph.D. -** Workshop Chair

8:15 a.m. ***Congressional Interest Items and Opportunities*** – Mr. Arun Seraphin - SASC Professional Staff Member, and Mr. Kevin Gates - HASC Professional Staff Member

9:00 a.m. Welcome Speaker – **Representative Jackie Speier (D-CA)** - Permanent Select Committee on Intelligence

9:20 a.m. Featured Speaker – **Mr. Stephen P. Welby** - Assistant Secretary of Defense for Research and Engineering (ASD R&E)

9:45 a.m. **BREAK**

10:00 a.m. Guest Speaker – **Ms. Kate Charlet** - Office of the Secretary of Defense for Policy (OSDP), Cyber Policy

11:00 a.m. ***Cybersecurity Test and Evaluation Process Overview*** – Ms. Jean Petty (MITRE / DASD, DT&E), and Mr. Dave Aland (DOT&E)

NOON **LUNCH**

1:00 p.m. Opening Keynote – **J. Michael Gilmore, Ph.D. -**Director Operational Test and Evaluation (DOT&E), Office of the Secretary of Defense (OSD)

1:30 p.m. **Cyber OT&E and T&E of Fielded Systems Panel**

Moderator: **Mitch Crosswait, Ph.D.** - Deputy Director Net-Centric Systems and Missile Defense Systems, DOT&E

Panelists:
Mr. Dave Aland - Director Operational Test & Evaluation
Mr. Brad Horton - Threat Systems Management Office
RADM Jeffrey Penfield, USN - Operational Test and Evaluation Force Command
Mr. William 'Bud' Redmond - Air Force Operational T&E Command
Mr. Jamie Wells - Department of Homeland Security

3:15 p.m. **BREAK**

3:30 p.m. **Cyber T&E Capability and Capacity to DT&E Panel**

Moderator: **Brian Hall, Ph.D.** - Principal Deputy Director, Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD/DT&E)

Panelists:
Ms. Tanya Skeen - Deputy Director, Headquarters, Air Force Test and Evaluation
Mr. Stu Young - NAVAIR
Mr. David Jimenez - Executive Technical Director, Deputy to the Commander, U.S. Army Test and Evaluation Command
Mr. Scott St Pierre - NAVSEA (CIO)
Brig General Guy M. Walsh, USAF (Ret) - Technical Advisor to the Deputy Commander, USCYBERCOM

5:30 p.m. **NETWORKING RECEPTION**

THURSDAY – MARCH 17TH

Workshop Day 2 Plenary Session

8:00 a.m. Opening Remarks – **Jeff McNeil, Ph.D.** - Workshop Chair

8:05 a.m. **Overview of the ITEA George Washington Chapter Scholarship Program**

8:15 a.m. Day 2 Keynote – **C. David Brown, Ph.D. –** Deputy Assistant Secretary of Defense, Developmental Test and Evaluation (DT&E) / Director, Test Resource Management Center (TRMC)

8:45 a.m. **Service Cyber T&E Visions/Approaches Executive Panel**

Moderator: **C. David Brown, Ph.D.** - DASD/DT&E/TRMC

Panelists:
MG Jonathan A. Maddux, USA - Program Executive Officer, Simulation, Training and Instrumentation (PEOSTRI)
Mr. Jeff H. Stanley - Associate Deputy Assistant Secretary of the Air Force for Science, Technology and Engineering, Office of the Assistant Secretary of the Air Force (Acquisition)
John Zangardi, Ph.D. - Deputy Assistant Secretary of the Navy, C4I/Space

10:15 a.m. **BREAK**

10:30 a.m. **Cyber Range Providers Panel**

Moderator: **Mr. Pete Christensen** - Director, National Cyber Range

Panelists:
Mr. Tim Bishop - Director, Threat Systems Management Office, Redstone
Mr. Bernard (Chip) Ferguson - Deputy Director, Interoperability, TRMC
Ms. Lori Pridmore - National Cyber Range Program Director, Lockheed Martin
Col Jenniffer F. Romero, USAF - Joint Chief, Cyber Space Environment Division (JIOR), Joint Staff J7 DDJT
Major George Van Osterom - USAF, 46th Test Squadron Det 2

NOON **LUNCH**

1:00 p.m. to 5:00 p.m. **TECHNICAL TRACK SESSIONS**

TRACK 1 - Cyber T&E Standards
Chair: Mr. George Wauer (SES, Ret.)

1:00 – 1:30 ***Cyber T&E Standards*** – Mr. George Wauer - TRMC

1:30 – 2:00 ***Test and Training Enabling Architecture (TENA)*** – Mr. Gene Hudgins - Wyle

2:00 – 2:30 ***Cyber Range Environment VV&A*** – Mr. Brad Seigler and Mr. Brian Kim - HU/APL

2:30 – 2:45 **BREAK**

2:45 – 3:15 ***DECRE Cyber Range Interface Specification*** – Mr. David Gerek

3:15 – 3:45 ***Cyber Range User's Guide*** – Col Burton Catledge - DASD (C3CB)

TRACK 2 - Cyber T&E Capability Development
Chair: Mr. Chris Paust, Central Test and Evaluation Investment Program (CTEIP) PM, TRMC

1:00 – 1:30 ***Central T&E Investment Program (CTEIP) Cyber Project Overview*** – Mr. Chris Paust - Central Test and Evaluation Investment Program (CTEIP) PM, TRMC

1:30 – 2:00 ***Cyber TASE (CTEIP)*** – Mr. Mike Winslow

2:00 – 2:30 ***T&E/S&T Cyberspace Test Technology Project Overview*** – Mr. Mark Ericksson

2:30 – 2:45 **BREAK**

2:45 – 3:15 ***DOT&E START Project Overview*** – Mr. Steve Gates - DOT&E

3:15 – 3:45 ***Spectral Environment Capture and Emulation*** – Acquired Data Solutions

3:45 – 4:15 ***SimSpace*** – Mr. Lee Rossey

TRACK 3 - Cyber T&E Workforce Development
Chair: Jeff McNeil, Ph.D., Professor Clemson University, Principal Investigator, Test Capabilities Development, OUSD (AT&L), TRMC

1:00 – 1:30 ***DoD Workforce Strategy/Framework Implementation and DoD Manual Development*** – Ms. Stephanie Keith - Chief, DoD CIO Cyber Workforce Strategy and Policy Division

1:30 – 2:00 ***T&E FIPT Cyber Key Leader Position Certification and Education*** – Mr. Tom Simms - DT&E

2:00 – 2:30 ***NCR Intern Program*** – Ms. Lori Pridmore - Lockheed Martin

2:30 – 2:45 **BREAK**

2:45 – 3:15 ***Wounded Warrior Cyber Combat Academy*** – Mr. Jim Wiggins - Executive Director, Federal IT Security Institute

3:15 – 3:45 ***NSA CAE Program*** – Ms. Heather Eikenberry - PM

TRACK 4 - Established Track Record: Cyber T&E Successes / Lessons Learned
Chair: Mr. Adam Tanverdi, National Cyber Range

1:00 – 1:30 ***NICS Testing on the NCR*** – Mr. Gene Anzano - DHS

1:30 – 2:00 ***Mission-Oriented Cybersecurity Requirements*** – Mr. Paul Kodzwa - IDA

2:00 – 2:30 ***AEC Evaluation Metrics Out-Brief*** – Mr. James Riordan - MIT LL

2:30 – 2:45 **BREAK**

2:45 – 3:15 ***Weapon Systems and Cyber Testing and Evaluation*** – Mr. Fred Wright - GTRI

3:15 – 3:45 ***Aircraft Cyber Threat Working Group Lessons Learned*** – Mr. Scott Jones

3:45 – 4:15 ***SoS Cybersecurity T&E*** – Ms. Paola Pringle - NAVAIR

TRACK 5 - Disrupting the Kill Chain
Chair: Robert Tamburello, Ph.D. - Deputy Director, National Cyber Range

1:00 – 1:30 ***All About the Baseline: An Essential Deliverable of Cyber Security T&E*** - Mr. John Schab - MITRE

1:30 – 2:00 ***Testing and Characterizing the Effectiveness Cyber Event Detection Capabilities: A Diagnostic Approach*** – Mr. Matthew Dinmore - JHU/APL

2:00 – 2:30 ***Hardware Trojan Detection in COTS Networking Devices*** – Mr. Peter Roy Ateshian - NPS

2:30 – 2:45 **BREAK**

2:45 – 3:15 ***Deceptive Disruption: Using Deception to Disrupt the Cyber Kill Chain*** – Mr. Duane Wilson - Sabre Systems, Inc.

3:15 – 3:45 ***Cyber4sight*** – Mr. Adam Perino and Ms. Danielle Meah - BAH

3:45 – 4:15 ***SAF A6/CIO TF Cyber Secure*** – Col Bill "Data" Bryant

---

TRACK 6 - Partnering with Industry and Academia Panel

1:00 – 5:00 Moderator: **Robin Poston, Ph.D. -** University of Memphis STEP

Panelists:
Dave Desjardins - Raytheon
Lee Rossey - SimSpace
Dipankar Dasgupta - University of Memphis STEP
George Hsieh, Ph.D. - Norfolk State University
Brig Gen Guy Walsh (USAF, ret.) - Technical Advisor to Deputy Commander, USCYBERCOM

NOW ONLINE at www.itea.org!

March 2016 issue of
The ITEA Journal of Test and Evaluation

Leveraging Training and Experimentation Infrastructure and Events for T&E

Past EXHIBITORS:

772 TS Benefield Anechoic Facility
Acquired Data Solutions, Inc.
ACROAMATICS Inc.
Advanced Systems Development, Inc.
Advanced Test Equipment Rentals
AEgis Technologies Group, Inc.
Agiltron
Air Academy Associates
Ampex Data Systems
Analytical Graphics, Inc.
Apogee Labs, Inc.
ARS
Astro Haven Enterprises
ATK
ATTI
Avionics Interface Technologies
Brand Design
CA Technologies
CALCULEX, Inc.
CDW-G
Charles Stark Draper Laboratory
CI Systems Inc.
Command Post Technologies
Compunetix, Inc.
Curtiss-Wright Controls Avionics & Electronics
Defense Acquisition University
Defense Threat Reduction Agency
Directed Energy Professional Society (DEPS)
DET S&T
DEWESoft, LLC
DEWETRON, Inc.
DRS Technologies
Dynetics, Inc.
Dytran Instruments, Inc.
Edge Consulting
Elotek Systems, Inc.
EMC Corporation
Emhiser Research
EMRTC New Mexico Tech
EWA Government Systems, Inc.
G.R.A.S. Sound & Vibration
GDP Space Systems
General Dynamics Mission Systems
Geodetics, Inc.
Georgia Tech Research Institute - GTRI
Glacier Technologies
HEL-JTO
IAI North America
IAI-ELTA
IDA Technology
Imprimis, Inc.
Innovative Defense Technologies
Integrated Network Enhanced Telemetry Project
International Institute for Software Testing
International Telemetering Conference
ITT Exelis
Ixia
Jacobs Technology
Joint Range Solutions
JT3 LLC
Keep it Simple
KRATOS Lancaster
Kratos Technology and Training Solutions
L-3 Telemetry & RF Products
Lockheed Martin Mission Systems
Malaysian Software Testing Board
ManTech International Corporation
Marvin Test Solutions, Inc.
Meggitt Sensing Systems
Miratek Corporation
NAVAIR
Naval Aviation Test & Evaluation University
NCSL International
NetAcquire Corporation
New Mexico Institute of Technology
NTSA
Olympus Industrial
OnTime Networks
PAE
Parasoft
PCB Piezotronics
Photo-Sonics, Inc.
Playas Training & Research Center
PMSC/AssetSmart
Precision Filters, Inc.
Raytheon Ktech
Rockwell Collins
Rotating Precision Mechanisms, Inc.
RoundTable Defense, LLC
RT Logic
Saalex Solutions, Inc.
SAIC
SAS Institute Inc.
Scientific Research Corporation (SRC)
SenQuest
SimIS Inc.
Smart Card Alliance
Smartronix Inc.
Spiral Technology, Inc.
STAR Dynamics, Inc.
SURVICE Engineering Company
SYMVIONICS Inc.
University of Memphis System Testing Excellence Program
Systems Application & Technologies (SA-Tech)
Systems Engineering & Management Company
TASC, Inc.
TDK-Lambda Americas
Technical Systems Integrators, Inc.
Tektronix, Inc.
Teletronics Technology Corporation
Telspan Data
TENA JMETC
Test Resource Management Center (TRMC)
The Boeing Company
The Johns Hopkins University Applied Physics Laboratory
THE SENTE GROUP, INC.
Tigua Enterprises, Inc.
TRAX International
TRIDEUM Corporation
U.S. Air Force Research Laboratory (AFRL)
U.S. Army Electronic Proving Ground - EPG
U.S. Army Virtual Targets Center
U.S. Army White Sands Missile Range - WSMR
Ulyssix Technologies, Inc.
Uniforce Sales and Engineering
Universal Switching Corporation
Weibel Scientific A/S
Wideband Systems, Inc.
Wyle
Zodiac Data Systems

Past SPONSORS:

Advanced Systems Development, Inc.
Alion Science and Technology
AMERICAN SYSTEMS
Applied Research Laboratory/Penn State University
Astro Haven Enterprises
Avion Solutions, Inc.
Booz Allen Hamilton, Inc.
CALCULEX, Inc.
Charles Stark Draper Laboratory
Command Post Technologies
EMRTC New Mexico Tech
Engility Corporation
Ernst & Young LLP
EWA Government Systems, Inc.
General Dynamics Mission Systems
Georgia Tech Research Institute - GTRI
IAI-ELTA
InDyne, Inc.
INQU, LLC
irig106.org
Jacobs Technology, Inc.
Joint Range Solutions
JT3 LLC
Kratos Technology and Training Solutions
Loch Harbour Group, Inc.
Lockheed Martin Mission Systems
ManTech International Corporation
Miratek Corporation
NetAcquire Corporation
PAE
Raytheon Ktech
Rockwell Collins
RoundTable Defense, LLC
Scientific Research Corporation
SimIS Inc.
SURVICE Engineering Company
Systems Application & Technologies (SA-Tech)
TASC, Inc.
The Boeing Company
TRAX International
TRIDEUM Corporation
Wyle

For information on exhibiting or sponsorships, contact John Bolino at symposium@itea.org

REGISTER AT: **www.itea.org/symposium**

ABSTRACTS

All About the Baseline: An Essential Deliverable of Cyber Security T&E
John Schab - MITRE Corporation

We've heard it before; it's just a matter of time before your system gets compromised. Recent SANS studies on malware, intrusion prevention and cyber threat intelligence agree that almost every organization, no matter how well prepared, is infected with malware to some degree and that many show signs of malicious activity. Yes, we have to do everything we can to prevent a breach, but it's even more important to quickly to detect, respond, and recover when a breach happens.

Finding evil is becoming more and more difficult as adversaries become stealthier and customize attacks for specific systems. Signature based detection is becoming less useful as advanced attackers customize their attacks for specific victims. The greatest opportunity for detection is knowing what's normal for your system and investigating anything that appears abnormal. Unfortunately, most defenders don't have a clear picture of what's normal for their system to begin with. According to the SANS 2015 Incident Response Survey, 37% of incident responders cite the inability to distinguish malicious events from non-events as an impediment to effective incident response.

How can cyber security T&E help? An important aspect of cyber security is knowing what is normal in order to identify what's not normal. This entails developing a highly accurate baseline of the system. A baseline needs to be developed in a realistic operational environment to ensure its accuracy. Additionally, the baseline should be developed before the system is placed on a real operational network since that network may already be compromised. If the system is baselined after being put into operation, there is a chance the baseline will contain existing adversarial activity. The result will allow adversarial activity to be considered normal activity, making a defender's job even more difficult. Therefore, an essential deliverable of cyber security T&E needs to be a complete baseline of the system gathered from an operational realistic test environment.

Cybersecurity Test and Evaluation Process Overview
Michael Said, Dave Aland and Jean Petty - DON T&E, DOT&E and DASD (DT&E)

We are vulnerable in this wired world. Today our reliance on the confidentially, availability and integrity of data stands in stark contrast to the inadequacy of our cybersecurity. DOD has established its Cyber Strategy and top level policies (i.e., DODI 5000.02 on Operation of the Defense Acquisition System, DODI 8500.01 on Cybersecurity, and DODI 8510.01 on Risk Management Framework). These have the focus on building capabilities for effective cybersecurity and cyber operation to defend DOD networks, systems and information against cyberattacks. But how does this translate into effective and efficient cybersecurity assessment efforts in support of acquisition programs? The Cybersecurity T&E Process has been established to close the gaps between policy, process and execution to begin supporting acquisition programs early in the life cycle. The Cybersecurity T&E Process provides:

- Support for cybersecurity assessments and authorization.
- Critical data and information for the program manager to enable root cause determinations and identify corrective actions on systems under development.
- Help ensure that cybersecurity risks are understood and appropriately mitigated.

This presentation will review the six phase Cybersecurity T&E Process (of which, four phases involve Developmental Testing and two phases involve Operational Testing). The process phases are iterative and executed as part of the acquisition continuum, from "Understand Cybersecurity Requirements" to "Adversarial Assessment" and subsequent test planning needs. Since both are involved in acquisition phases, the role of government and industry will also be covered. A Cyber Ranges overview will be provided as part of this presentation, with information on the various Cyber Ranges' mission, organization, functions and T&E capabilities.

Deceptive Disruption: Using deception to disrupt the cyber kill chain
Duane Wilson - Sabre Systems, Inc.

Military leaders need a way to actively defend their networks, host computers, or sensitive data to prevent an adversarial attempt to compromise these assets. The art of deception has commonly been used as a technique to lure attackers away from important data and learn about attackers that successfully compromise a network. It is believed that deception techniques, working in conjunction with traditional cyber defense methods, can alter the underlying attack process, making it more difficult, time consuming and cost prohibitive. Modern day military planners need a capability that goes beyond the current state-of-the-art in cyber deception to provide a system or systems that can be employed by a commander when needed to enable additional deception to be inserted into cyber operations. The primary goal will be to demonstrate the effectiveness of various deceptive techniques at each phase of the cyber kill chain. This effort will examine the typical attack steps of; reconnaissance (where the enemy researches, identifies and selects the target), scanning (where detailed information about the target is obtained allowing a specific attack to be crafted), gaining access (where the attack is carried out), and maintaining access (where the attack evidence is deleted and information is exfiltrated or altered/destroyed) to identify where and how deception technologies can be brought to bear to thwart the objectives of an attack. Lastly, we show the ability of our approach to adapt to various INFOCON levels to mirror a traditional information warfare setting. INFOCON (short for Information Operations Condition) is a threat level system in the United States based primarily on the status of information systems and is a method used by the military to defend against a computer network attack.

Hardware Trojan Detection in COTS Networking Devices
Peter Roy Ateshian - Naval Postgraduate School Computer Science Department

Hardware Trojans, in a device such as a networking interface card (NIC) can create a covert channel by leaking information through the networking interface. FPGA implementations, such as the RAM based FPGA board we used, are particularly susceptible as they can be reprogrammed remotely via a flash memory device after deployment or installation, simply as a RAM bit stream update. We detect such covert channel activity, not from the networking interface, or 64Gb bit stream, where it may be well hidden, but by analyzing device behavior from its electromagnetic (EM) power side channel radio frequency (RF) emissions. We show how non-standard operations can be detected after simple start-up EM characterization, by performing a normalized Differential Frequency Analysis (DFA) using an EM probe a few centimeters away from the FPGA board power pin. This was done using a standard commercial passive power side channel analysis tool. We first characterize normal device behavior using the power spectral components of the EM emanation. After that, we trigger certain anomalous behavior and are able to detect in the EM signal, a buffer overflow and also a packet buffer in RLDRAM being activated and used to potentially subvert delayed packets to an unauthorized third party listener. This research, funded by DARPA and performed by the Naval Postgraduate School CCW, shows the feasibility of an automated non-invasive black-box detection of anomalous behavior on a FPGA based device using differential frequency analysis (DFA).

Mission-Oriented Cybersecurity Requirements
Paul M. Kodzwa, Jr. - Institute for Defense Analyses

The lack of relevant mission-oriented, funded cybersecurity requirements was a recurring issue with acquisition program cybersecurity test and evaluation. Unlike more traditional requirements, cybersecurity requirements are described in Department directives and associated performance attributes and evaluated against compliance checklists. As a consequence, some have observed that cybersecurity is effectively disconnected from the system by which the military establishes requirements for combat capabilities, and cybersecurity test methods are disconnected from combat missions and associated tasks.

The most recent Joint Capabilities Integration and Development System Manual requires capability requirement sponsors to “incorporate or justify the absence of a System Survivability Key Performance Parameter (KPP)” in Capability Development Documents and Capability Production Documents. This KPP is in part intended to ensure the system maintains its critical capabilities under applicable cyber threat environments. In system-of-systems approaches, this KPP could also include resiliency attributes pertaining to the ability of the broader architecture to complete the mission. The Chairman, Joint Chiefs of Staff directs that sponsors include whether or not the system must be able to survive and operate in a cyber-contested environment. However, the JCIDS Manual also indicates that cybersecurity considerations in the System Survivability KPP should be based on applicable cybersecurity controls.

This briefing provides a distillation of previous findings from cyber events, workshops and interviews with cybersecurity T&E practitioners relevant to the cybersecurity requirement problem. We use this information to offer a potential approach to defining mission-oriented cybersecurity requirements.

NICS Testing on the NCR
CDR Gene Anzano, USCG - DHS S&T Office of Test and Evaluation

Last summer, in coordination with the Department of Homeland Security (DHS), the United States Coast Guard (USCG), and Massachusetts Institute of Technology (MIT) Lincoln Laboratories, the National Cyber Range (NCR) conducted cybersecurity testing and evaluation of the Next Generation Incident Command System (NICS) web-application. This was the first testing event of a DHS/CG application at the NCR, demonstrating the scheduling, preparation, and utility of red-team/penetration testing of a homeland security application at a cyber range for developmental and operational testing.

NICS is a web-based command and control application for small (local) to extreme (national) scale incidents that facilitates collaboration across Federal, Tribal, Military, State, County, and Local/Municipal levels of preparedness, planning, response, and recovery for all-risk/all-hazard events, such as Incidents of National Significance (IONS) (for example, the Deep Water Horizon oil spill of 2010 was an IONS and had an ICS response of over 50,000 personnel, 123 aircraft, 60 CG cutters, and 13,000 vessels in a period of 6 months). NICS was developed to make use of already available technology to first responders such as personal smart phones, tablets, and laptops and to facilitate situational awareness and response via the Internet. However, because it is web-based, NICS is open to malicious attacks and possible intrusion and data exfiltration. NCR evaluated the cyber security posture of the latest version of NICS and provided recommendations to the software developers/engineers to shore-up the identified vulnerabilities before its deployment for federal, nation-wide use.

Executive Summary:

- NCR was able to recreate the NICS operating environment and conduct all of the planned test cases
- 33 test cases resulted in 18 findings
- Results of architecture and source code review

The vulnerabilities identified were typical of applications that do not have security as a main feature: for example impersonating the Incident Commander can disrupt and deny command and control of incident responders if NICS were employed today, without testing. Cyber-testing web applications for homeland security missions is essential prior to deployment and fielding before it is employed and used by thousands of users, both government and private, in an IONS event.

PHY Layer Tools and Attacks in the Cyber-EW Domain
Ellen Byington and Sean Wallace - Acquired Data Solutions, Inc, I BD and Project Manager

The convergence of the Electronic Warfare and Cybersecurity domains implies moving down the protocol stack. As the community steadily improves resistance to attack on the logical layers, we must expect that attackers will start to move further down the stack and into the physical (PHY) layer.
Wireless PHY implementations are a particularly attractive target to adversaries. Join us as we discuss possible attacks on the wireless PHY layer and new instrumentation that may be used to defend, capture, replay and attack the PHY layer.

SAF A6/CIO TF Cyber Secure
William D. Bryant - SAF/CIO A6, Task Force Cyber Secure

The only way to effectively defend our weapons systems in cyberspace is through an active and maneuvering defense built on solid passive defenses. Currently, we primarily rely on static defense in depth for most of our mission and weapons systems, but that is not sufficient against a skilled and determined adversary.

It is useful to think of cyberspace assets in three broad categories: traditional IT, Operational Technology (OT), and platforms. IT based weapons systems are easier to actively defend than tanks and aircraft, but there are still hurdles preventing a complete active defense on many systems. For non-traditional IT weapons systems such as ships and aircraft the situation is far worse. They do not use well-known computer protocols such as TCP/IP and this will limit their ability to use commercial off the shelf solutions and require significant testing and integration of new tools.

To develop viable active defense across the Department of Defense (DoD) will require three elements; the first is a cadre of "boots on the ground" cyber warriors. The second major element of active defense is to build appropriate cyberspace command centers for mission and weapons systems in addition to the ones that already exist for traditional IT systems. The third and final necessary piece of active defense is significant change to acquisition authorities and procedures. These changes will certainly not be simple or easy. Congress will have to write major changes into law, through a process deliberately designed by the framers to be inefficient and difficult. Congress will have to be convinced to make the necessary changes that streamline the process, while still finding ways to keep sufficient oversight of a fast moving process.

Each of the Services needs to better defend its mission and weapons systems in cyberspace through instituting active defense. Cyberspace is a warfighting domain and the last ten years have shown static defensive approaches to be ineffective. For relatively unimportant systems such as a home computer, static defenses and firewalls may be sufficient, much like locking the doors and a basic alarm system meets most homeowner's needs. However, no major museum with a collection worth hundreds of millions of dollars would consider a static defense to be adequate. Instead they combine state of the art alarm and security systems with active patrols by guards that can react to intrusions and threats dynamically. Since cyberspace is a warfighting domain, we need to treat it as such by ensuring we have maneuver forces in cyberspace who can see and respond to enemies. Clausewitz viewed warfare as two wrestlers, each trying to throw the other while constantly adjusting and reacting to the most subtle of movements by their adversary. Right now, our defense of weapons and mission systems in cyberspace makes us akin to a deaf and blind wrestler with no sense of touch; we need to rapidly move toward regaining our ability to see and respond to a maneuvering enemy in cyberspace.

Testing and Characterizing the Effectiveness Cyber Event Detection Capabilities: A Diagnostic Approach
Matthew Dinmore, Ph.D. - Johns Hopkins University Applied Physics Laboratory

Detection of adversary activities in cyberspace is a critical enabling capability for cyberspace operations. Operators, analysts and commanders need to be aware of the efficacy of detection measures in defensive planning to assess mission effectiveness, residual risk and life cycle cost. In these ways, cyber detection capabilities are analogous to medical diagnostic tests: doctors and patients need to understand how effective a test is, what risks are associated with it, and whether the benefit justifies the cost. In this presentation, measures commonly used to evaluate medical diagnostic tests are applied to the test and evaluation of cyber detection capabilities. An approach to designing tests for characterizing detection capabilities is discussed, and analytic methods for evaluating the results detailed. Importantly, plain-language descriptions of the results are presented, as is an approach to comparing similar detection capabilities.

Weapon Systems and Cyber Testing and Evaluation
Mike Ruiz, Fred Wright, Dan Tabor, Douglas Woods, Ron Prado - Georgia Tech Research Institute

Based on recent DoD guidelines and instructions for cyber systems and T&E, there are new and additional requirements for dealing with cyber vulnerabilities for all types of systems. In many cases, program offices for weapons platforms are grappling with the meaning and utility of these requirements. This paper describes cyber test methodologies for platforms, such as aircraft or ground vehicles.

This paper will explore the difference between cyber security and vulnerabilities for enterprise IT systems and weapon systems platforms (e.g., vehicles). These differences inform how "cyber T&E" for weapons systems can be planned and conducted. In particular, risks and threat vectors to embedded systems in a combat environment are very different than internet facing IT systems. Also, tools for testing IT systems are also different from tools for weapons platforms.

An iterative risk assessment-test process is proposed based on recent weapon systems assessments. A key part of this process is leverage activities required by regulations (e.g., Risk Management Framework) to guide the T&E process. Test plans are focused not only on identified threat vectors and risks but also on building confidence and reducing uncertainty in the risk models.

Based on recent weapon system assessments, we will also identify gaps in test capabilities and lessons learned. Test tools for weapons systems vulnerability analyses, analogous to the tools used for IT enterprise penetration testing, will be described as potential approaches to fill gaps.

SPEAKER BIOGRAPHIES

Mr. Dave Aland is a Staff Assistant for the Director Operational Test and Evaluation on the staff of the Secretary of Defense, specializing in Cybersecurity. Hailing originally from Annapolis, Maryland, Mr. Aland is a graduate of the United States Naval Academy as well as the U. S. Naval War College in Newport, Rhode Island. He is a previous recipient of an Armed Forces Communications and Electronics "Arthur K. Cebrowski" award for C4I research, and retired in 2002, with the rank of Captain. Mr. Aland's nearly thirty years of military service was spent in large part at sea, on ship types ranging from frigates and destroyers to aircraft carriers and a hydrofoil, including two on which he served as Commanding Officer. He has deployed to the Pacific, Western Pacific, Indian Ocean, Arabian Gulf, Mediterranean, North Atlantic, and Caribbean waters, and participated in combat operations in the Arabian Gulf, Eastern Mediterranean, Adriatic, Caribbean, and Eastern Pacific. Mr. Aland's last two active duty postings were as the Director of Communications for the U. S. Sixth Fleet, and the deputy to the Navy Chief Information Officer. Since his military retirement, Mr. Aland worked briefly with Titan Corporation in support of the Defense Security Service office of the Chief Information Officer, and with Wyle Inc. as consultant supporting the Director of Operational Test and Evaluation. He returned to direct government service in 2011.Mr. Aland specifically manages a Congressionally-mandated initiative to improve and streamline assessments of Information Assurance at the Combatant Commands and provides technical direction for cybersecurity assessments of exercises as well as programs of record.

Suzanne Beers, Ph.D., is MITRE Corporation's OSD Test & Evaluation Portfolio Manager. Suzanne joined MITRE in Colorado Springs, Colorado after retiring from the USAF, as a colonel, in October 2008. Her final assignment was as the Commander, Air Force Operational Test and Evaluation Center's Detachment 4 at Peterson AFB responsible for OT&E of new space, missile, and missile defense systems. At MITRE, Suzanne has supported DOT&E, DT&E, and now leads Developmental Evaluation Framework implementation for DASD(DT&E). She holds a plethora of degrees (five) from a wide variety of institutions of higher learning…giving her plenty of cheering flexibility during college football season…including a Bachelor's of Science in Mechanical Engineering from The Ohio State University and a Ph.D. in Electrical Engineering from Georgia Tech. Suzanne recently caught the triathlon bug, so when she's not working or traveling for DEF implementations, she's swimming, biking, running, or talking triathlon with fellow addicts! She'd be happy to entertain any Ironman-related questions!!

Mr. Timothy F. Bishop is the Director of the U.S. Army Threat Systems Management Office (TSMO) in Redstone Arsenal, AL. As part of the Program Executive Office for Simulation Training and Instrumentation (PEO STRI), Program Manager for Instrumentation Targets and Threat Simulators (PMITTS), Mr. Bishop is responsible for the acquisition, operation, maintenance and sustainment of the Army Threat Simulator (ATS) Program. He recently served as the Technical Director for the Joint Forces Command (JFCOM) Information Operations Joint Management Office (IO JMO) where he oversaw a number of acquisition programs on behalf of the Office of the Under Secretary of Defense for Intelligence (OUSD(I)).

As a 2008 graduate of the U.S. Army War College, Mr. Bishop served as the Director of Operations for the U.S. Army Installation Management Command – Europe (IMCOM-Europe) in Heidelberg, Germany. He has served as a Department of Army civilian for 25 years and before attending the U.S. Army War College served in a wide variety of key positions as a government civilian in the United States and overseas. His job assignments include Director of Operations, U.S. Army Mi-17 Kabul Air Wing, Kabul, Afghanistan; Technical Director/Advisor, U.S. Army Threat Systems Management Office (TSMO), Redstone Arsenal, AL; Division Chief, TSMO World Wide Operations, Ft Bliss, TX; and he has held Team Leader Positions over Operations, Foreign Commercial Purchase and Software Simulations within the Program Manager for Instrumentation Targets and Threat Simulators.

Mr. Bishop is a graduate of the University of Alabama – Huntsville with a B.S. in Electrical and Computer Engineering and he holds a M.S. in Strategic Studies from the U.S. Army War College. He is a graduate of the U.S. Army Senior Service College and Defense Acquisition University Advance Program Management Course holding Defense Acquisition Workforce Level III certification in both Program Management and Systems Engineering and Level II certified in Test and Evaluation.

Mr. Bishop resides in Huntsville, AL. His hobbies include golfing, reading, watching/playing sports, and horses.

C. David Brown, Ph.D., CTEP, is the Deputy Assistant Secretary of Defense for Developmental Test & Evaluation (DASD(DT&E)) and Director, Test Resource Management Center (TRMC). As the DASD(DT&E), he serves as the principal advisor on developmental test and evaluation to the Secretary of Defense (SECDEF) and the Undersecretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)). Dr. Brown is responsible for DT&E policy and guidance in support of the acquisition of major Department of Defense (DoD) weapons systems, and providing advocacy, oversight, and guidance to the DT&E acquisition workforce.

In Dr. Brown's role as Director, TRMC he advises the SECDEF and USD(AT&L) on matters pertaining to the DoD's Major Range and Test Facility Base (MRTFB), the Nation's critical range infrastructure for conducting effective test and evaluation (T&E). Additionally, he reviews and certifies proposed T&E budgets of Military Departments and Defense Agencies, administers the Central Test and Evaluation Investment Program (CTEIP), and oversees the DoD program for T&E science and technology.

Prior to his appointment in September of 2013, Dr. Brown was a consulting engineer for the MITRE Corporation and the Institute for Defense Analyses in the areas of DoD program management, systems engineering, and test and evaluation. He was also an adjunct professor and still teaches graduate courses in program management and systems engineering for Johns Hopkins University. He previously served as the Director of the Combined Test Organization and Executive Director for Test for the Army Future Combat Systems (FCS) program where he was responsible for planning and overseeing the testing and evaluation for this multi-billion-dollar revolutionary development program. Before working on the FCS program, Dr. Brown was the Director for Test and Technology for the Army Developmental Test Command, where he oversaw the management of more than 1700 tests annually, technical operations at five of the DoD MRTFBs and six associated test sites, and an annual budget of over $450 million in investment in test support and test technology development. Dr. Brown was also the focal point for the Army's application of modeling and simulation techniques to technical test and evaluation, including the development of the Virtual Proving Ground, the Army's multi-million-dollar, multi-year virtual testing program.

He has also been a test instrumentation engineer, test director, test manager, and an active Army Signal Corps officer in various leadership positions. Dr. Brown became a member of the Senior Executive Service in 1999, holds two patents, and has authored numerous technical papers. He is a registered Professional Engineer, was a member of the Army Acquisition Corps, and is a retired Army Reserve Colonel. He has a PhD in electrical engineering from the University of Delaware, and a MS in National Resource Strategy from the National Defense University Industrial College of the Armed Forces. He is an active member of the International Council on Systems Engineering and the International Test and Evaluation Association.

Colonel William D. Bryant is the Deputy Director, Task Force Cyber Secure, Office of Information Dominance and Chief Information Officer, Secretary of the Air Force, Pentagon. In this capacity, he is responsible for the day to day operations of the Chief of Staff directed task force responsible for cyber security and improving mission assurance of the Air Force's five core missions in and through the cyberspace domain.

Colonel Bryant received his commission in 1993 through the United States Air Force Academy. During his career, Colonel Bryant has served as a commander, operations officer, strategist, and planner as well as an F 16 Mission Commander, evaluator, and instructor pilot. He is a veteran of Operations NORTHERN WATCH, SOUTHERN WATCH, IRAQI FREEDOM, NEW DAWN, and NOBLE EAGLE. He has done strategic and operational planning for USAFCENT, USCENTCOM, 7 AF, USFK, PACAF and an interagency study group. In addition, as the chief of the Warfighting Mission Area Integration Division under the SAF/CIO A6, he has worked integration and cybersecurity of warfighting IT across the USAF enterprise to include weapons system IT, data links, radios, SATCOM and C2 systems.

Colonel Bryant was also the commander of the 407th Expeditionary Operations Support Squadron, located at Ali Base, Iraq. He led a team of more than one hundred and fifty technical specialists drawn from fifteen career fields to provide 24/7/365 support to joint air operations securing air dominance and battlespace control of Iraq's southern region. Colonel Bryant maintained an airfield complex worth more than $300 million that spanned more than 1,800 acres, and he executed Senior Airfield Authority at Ali Base by directing Airfield Operations, Civil Engineering, and Security Forces support to the largest and most active military airfield in southern Iraq.

Colonel Bryant has a number of academic degrees in a wide range of fields including Aeronautical Engineering, Military Studies, Organizational Management, Space Systems, and Strategic Studies. The dissertation topic for his PhD in Military Strategy was cyberspace superiority.

Colonel Bryant is also a Command Pilot and combat mission commander with over 1,500 flying hours, including 150 combat hours in the F-16 in the skies over Southwest Asia.

Mitch Crosswait, Ph.D., Deputy Director, Net-centric, Space and Missile Defense Systems, Office of the Secretary of Defense-Director, Operational Test and Evaluation. Dr. Crosswait received a Bachelor of Science in Applied and Engineering Physics from Cornell University, and a Ph. D. in nuclear engineering from MIT. For the past 25 years, he has conducted analysis, evaluation, testing and integration of defense and homeland security systems. Commissioned as a naval officer in 1984, he was assigned to the Naval Reactors branch of Navy Sea Systems Command, where he designed naval nuclear propulsion plants. Following graduate school, he worked for TRW Corporation as a systems engineer designing systems to transport and dispose of spent nuclear fuel from civilian and naval nuclear plants. In 1996, he became a lead analyst for the Office of Program Analysis and Evaluation in the Office of the Secretary of Defense, where he led inter-service and inter-agency teams to develop programmatic alternatives to reduce program cost and improve capability.

Dr. Crosswait became a Professional Staff Member on the Senate Armed Services Committee in 2001, where he provided funding recommendations and drafted legislation to strengthen testing, oversight and accountability for missile defense and space programs. Following 9/11, Dr. Crosswait joined the newly-formed Department of Homeland Security where he created and served as the Director of the Strategy, Planning and Integration Division within the Science and Technology Directorate. Later he served as a Deputy Director in the Department of Homeland Security's Office of Policy, where he co-led and managed the development of products to help ensure the Department cost-effectively achieved its strategic priorities. In 2013, Dr. Crosswait returned to the Department of Defense as the lead analyst for Army tactical communication systems in the office of the Director, Operational Test and Evaluation (DOT&E). Dr. Crosswait became a member of the Senior Executive Service in 2014 upon his selection as the DOT&E Deputy Director for Net-centric, Space and Missile Defense Systems.

Dr. Crosswait received the Exceptional Civilian Service, Outstanding Performance and Special Service awards from the Department of Defense, and a Special Award from the Department of Homeland Security for his contributions to the first Quadrennial Homeland Security Review. He earned a nuclear engineering fellowship from the Department of Energy, and is a licensed private pilot. He is an avid keyboardist who plays regularly at his church.

Paul Dailey, Ph.D., Senior Staff, Johns Hopkins University Applied Physics Lab (JHU/APL) has more than 13 years' experiences in systems engineering and test and evaluation (T&E) supporting Defense, Homeland Security and commercial programs. He is a graduate of the U.S. Naval Postgraduate School with a Ph.D. in Software Engineering and a M.S. in Systems Engineering and a graduate of the University of Louisville with a B.S. in Electrical Engineering. Currently, he primarily supports multiple cyber-related T&E efforts at JHU/APL and teaches a course on cyber systems T&E in APL's Strategic Education program.

Ms. Heather Eikenberry - Program Manager for the National Security Agency/College of Cyber's Centers of Academic Excellence in Cyber Operations. Ms. Heather Eikenberry is the Program Manager for the National Security Agency's Centers of Academic Excellence in Cyber Operations (CAE-CO) Program. Ms. Eikenberry is administratively responsible for the CAE-CO program which reviews educational institution's deeply technical cyber operations programs for possible CAE-CO designation. To date, 14 schools have earned this prestigious recognition. In addition, Ms. Eikenberry assists with the management of the CAE-CO Summer Intern Program which enables college students to experience an exciting hands-on education covering key topics of national security interest combined with a mission relevant Capstone project.

Ms. Eikenberry's 15-year career within the NSA has included positions as a Technical Analyst within the Information Assurance Directorate (IAD), Executive Assistant to an IAD Deputy Director, and Branch Chief within US CYBERCOMMAND. As part of NSA's National Cryptologic School (NCS), Ms. Eikenberry is also a member of the GenCyber Program which is growing the next generation of cybersecurity experts for the Nation by sponsoring educational institutions to run summer camps focused on creating interest in K-12 students in cybersecurity. Ms. Eikenberry holds Master's degrees in Biostatistics, Information Systems and Network Security.

Mr. Mark S. Erickson is a Senior Engineer, assigned to the Command Section of the 46th Test Squadron at Eglin AFB, Florida. He is a retired Air Force officer with over 30 years of test and evaluation experience at Edwards AFB, California and Eglin AFB, Florida. The first half of his career was spent in aircraft flight test, primarily on fighter propulsion, performance, and flight controls programs. He later worked advanced development and testing for the E-8C Joint STARS and Global Air Traffic Management programs at Hanscom AFB, Massachusetts. In 1998, he transitioned to electronic systems testing including command & control, cyberspace, electronic warfare, and seeker/sensor systems. He has been supporting TRMC's T&E/S&T program as the Executing Agent for Cyberspace Test Technology since 2013. He received a BS in Aeronautical Engineering from the USAF Academy, earned his MS in Aerospace Engineering with distinction from the AF Institute of Technology, and was the top flight test engineer/ navigator graduate from the AF Test Pilot School. He holds acquisition professional certifications in Test & Evaluation, Program Management, and Systems Engineering.

Mr. Bernard "Chip" Ferguson is the Deputy Director, Interoperability and Cyber Test Capability, Test Resource Management Center and the Program Manager for TRMC's Joint Mission Environment Test Capability (JMETC) Program. Mr. Ferguson started his career as a Private in the Army in 1965. Upon graduation from flight school in 1966, he was promoted to Warrant Officer I. He served a tour in Viet Nam immediately thereafter. Upon returning to the States, he was assigned as an instructor pilot. After a year of teaching student pilots, CW2 Ferguson was returned to Viet Nam. He received a Direct Commission to First Lieutenant enroots to Viet Nam. Upon his return in 1970, he learned how to be an Artillery Officer and CPT Ferguson was assigned as a Battery Commander. In 1972 he returned to Viet Nam for what was to be his last combat assignment. After that third tour, CPT Ferguson received assignments as a student at the Artillery Officers Advanced Course, as a college student at Auburn University, as a Recruiting Area Commander, as a student at the Command and General Staff College, and as a graduate student at Kansas State University. Upon completion, MAJ Ferguson was assigned to the 3rd Armor Division in Hanau, Germany where he served as a Battalion S3, Aviation Company Commander, and Deputy Battalion Commander. Upon returning to the States in 1984, MAJ Ferguson was assigned to the Army's Operational Test and Evaluation Command where he began his career in Test and Evaluation. In 1986 LTC Ferguson was again assigned to Hanau, Germany where he served as Commander, 2nd Battalion, 227th Aviation Regiment and as Deputy Commander of the 3rd Armor Division's Aviation Brigade. LTC Ferguson returned to the States in 1989 to attend the Industrial College of the Armed Forces. Upon graduation, he was assigned to the Office of the Director, Test and Evaluation, Office of the Secretary of Defense. COL Ferguson retired in 1993 and joined Science Applications International Corporation where he was a Senior Analyst, Division Manager, and Operations Manager—all supporting test and evaluation in the DoD. During his time with SAIC, Mr. Ferguson recognized the need for a distributed test capability in the Department. In 2006 he became aware that the Director, TRMC and the Principal Deputy Director, TRMC were seeking a Program Manager for the Joint Mission Environment Test Capability (JMETC) Program. Mr. Ferguson sought that position and is very grateful for the opportunity to become part of the JMETC Team.

Mr. Kevin Gates joined the House Armed Services Committee as a Professional Staff Member in March, 2007 to be responsible for the Information Technology (IT) and cyber operations portfolio, as well as the Science and Technology (S&T) portfolio. Previously, he worked for 8 years at Strategic Analysis, Inc of Arlington, Virginia for a variety of clients within the DoD science & technology community (including DARPA, ONR and the Defense Science Board), as well as the Homeland Security Advanced Research Projects Agency within DHS(S&T) and the intelligence community. He graduated from the University of North Carolina at Chapel Hill with BAs in History and International Studies, and has a MA from Georgetown University's Security Studies Program. He is the co-author of a chapter on critical infrastructure protection in Volume III of *Homeland Security: Protecting America's Targets*, James Forest (ed.), 2006.

Mr. Dave Gerrek, Senior Network / Electrical Engineer, SPAWAR Atlantic, supporting Cyberspace Environment Division (CED) Joint Staff DJ7/ DDJT. Currently, leading the design effort for the Next Generation Joint Information Operations Range (JIOR) to include automation, Multi-Protocol Label Switching (MPLS), and service provider technology. Additionally, co-chairs the DECRE Technical Working Group. Previously, Chief Network Engineer for Joint Training Enterprise Network (JTEN). World-wide network for S/CC/A supporting Modeling and Simulation (M&S) for Joint Training.

The Honorable J. Michael Gilmore, Ph.D. - Dr. J. Michael Gilmore was sworn in as Director of Operational Test and Evaluation on September 23, 2009. A Presidential appointee confirmed by the United States Senate, he serves as the senior advisor to the Secretary of Defense on operational and live fire test and evaluation of Department of Defense weapon systems. Prior to his current appointment, Dr. Gilmore was the Assistant Director for National Security at the Congressional Budget Office (CBO). In this position, he was responsible for CBO's National Security Division, which performs analyses of major policy and program issues in national defense, international affairs, and veterans' affairs. Specific areas of investigation included the long-term implications of current defense policies and programs, the implications of transformation for equipping and operating U.S. military forces, the effectiveness and costs of alternative approaches to modernizing U.S. military forces, and the resource demands associated with operating and supporting U.S. military forces. Dr. Gilmore is a former Deputy Director of General Purpose Programs within the Office of the Secretary of Defense, Program Analysis and Evaluation (OSD (PA&E)). As the Deputy Director, he was responsible for developing, formulating, and implementing Secretary of Defense policies on all aspects of Department of Defense general purpose programs, including analyzing the operational effectiveness and costs of U.S. conventional military forces and supporting programs. Before serving as a Deputy Director, Dr. Gilmore served as the Division Director of Operations Analysis and Procurement Planning, within the Office of the Deputy Director, Resource Analysis and prior to that as an Analyst for Strategic Defensive and Space Programs Division, Office of the Deputy Director, Strategic and Space Programs. Dr. Gilmore's service with Program Analysis and Evaluation covered 11 years. Early in his career, Dr. Gilmore worked at the Lawrence Livermore National Laboratory, Livermore, California performing research in their magnetic fusion energy program. He has also worked as an Analyst with the Falcon Associates, McLean, VA, and the McDonnell Douglas Washington Studies and Analysis Group, where he became Manager, Electronic Systems Company Analysis. A native of Ohio and resident of Virginia, Dr. Gilmore is a graduate of The Massachusetts Institute of Technology, Cambridge, Massachusetts, where he earned a B.S. in Physics. He subsequently earned a M.S. and Ph.D. in Nuclear Engineering from the University of Wisconsin, Madison, Wisconsin.

Mr. Bradley R. Horton is the chief of a STRATCOM/NSA accredited Red Team focusing on acquisition systems within the US Army and DoD. Brad holds a B.S. in Commerce and Business administration from the University of Alabama and a M.S. in Information Systems from the University of Alabama - Huntsville. He has participated in or led the cyber assessment of hundreds of systems, organizations, and hardened targets within the DoD and commercial sector including assessments of physical/operational security. His expertise is in the effective portrayal of advanced cyber threats, and he currently holds CISSP-ISSMP, C|EH, and CISA professional certifications.

Mr. Ryan Kelly is a cybersecurity engineer in the Mission Systems Group at the Johns Hopkins University Applied Physics Lab. He is an 11-year veteran of the Marine Corps wherein he served as an officer and helicopter pilot. Prior to joining the Applied Physics Lab, Ryan taught courses in cybersecurity at the United States Naval Academy and consulted as a forensic electrical engineer. He earned a Bachelor of Science degree in Computer Science from the United States Naval Academy in Annapolis, Maryland, and a Master of Science degree in Electrical Engineering from the Naval Postgraduate School in Monterey, California. Ryan's current area of focus is incorporating cybersecurity into systems engineering processes.

Jeff McNeil, Ph.D., is a Professor within the Clemson University College of Business and Behavioral Sciences, presently dedicated to full-time research supporting Test Capability Development for the DoD Test Resource Management Center. After receiving a Bachelor's Degree in Physics from the University of Nebraska-Lincoln, Jeff has spent 22 years serving across government, industry, and academia. A US Marine Corps Reserve Colonel and career intelligence officer, his recent military billets include Intelligence Plans and Operations Officer for Marine Forces Pacific and Central Commands, Joint Concept Development and Experimentation Deputy Director for International Engagement, US Strategic Command Assessment Officer, and currently Cyberspace Plans officer for US Pacific Command. He also spent over 14 years as a Principal Investigator for Scientific Research Corporation in support of various T&E projects, to include Cyberspace Threat Analysis for the T&E Threat Resource Activity (TETRA).Since completing his PhD in International Studies with research focused on International Conflict and Cooperation in Cyberspace, Dr. McNeil has taught a variety of International Relations and US Foreign policy courses for the University of Nebraska prior to assuming his current position.

Ms. Jean Petty is a Department Head for the MITRE Corporation's Portfolio supporting the Office of the Secretary of Defense (OSD). Jean joined MITRE in 1985 and has worked on a variety of projects performing systems engineering, test and evaluation, and acquisition support for major government and defense systems. Over the past two years, Jean worked with DASD(DT&E) to develop the Cybersecurity Test and Evaluation Guidebook and performed cybersecurity evaluation analysis for major DoD information system acquisitions. In addition to systems engineering and cybersecurity analysis, Jean has performed Common Criteria evaluation and validation for security functionality in commercial network and operating system products and has performed cryptographic test and evaluation. Jean is the mother of four children, an avid gardener, and the owner of too many animals to count, including dogs, cats, chickens, fish, and parrots.

Ms. Lori Pfannenstein - Program Manager, NSA / DHS National Centers of Academic Excellence in Cyber Defense, College of Cyber, National Security Agency. Lori Pfannenstein is a Program Manager at the National Security Agency (NSA) for the NSA/DHS Centers of Academic Excellence in Cyber Defense (CAE-CD) Program within the College of Cyber. The National Security Agency (NSA) and Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Cyber-Defense (CAE-CD) program. This program seeks to improve the cybersecurity posture of our nation by cultivating the next generation of cybersecurity professionals through education and research. Schools entering the program must meet a criterion established by the CAE-CD community that demonstrates appropriate rigor, breadth, and scope regarding education, research, and outreach activities related to cybersecurity. The program is dynamic and evolving and boasts a membership of over a 190 universities, colleges, and community colleges nationwide.

Lori has a long history of working in the cybersecurity arena with many years in the Computer Network Operations area of the Signals Intelligence (SIGINT) Directorate at NSA. With over 33 years of NSA experience, Lori has held a number of Program Management, management, and technical positions through the years. Lori holds a Bachelor of Science in Information Systems Management, an Associates of Science in Computer Science, and is currently enrolled in the Cybersecurity Fundamentals Graduate Certificate Program at the Naval Postgraduate School.

Mr. Lee Rossey co-founded SimSpace in 2015 with a core team of developers and cyber professionals that had previously worked together alongside the other co-founders in a national defense capacity.

Since 2000, Lee served in increasingly more responsible roles at MIT's Lincoln Laboratory (MIT LL), including most recently as Group Leader for the Cyber System Assessments Group. In this capacity, Lee and his team developed tools and processes for conducting independent assessments of cyber systems and capabilities for the U.S. Government.

During his tenure at Lincoln Laboratory, Lee led the establishment and growth of the Cyber System Assessment Group to become a nationally-recognized center of excellence. The Cyber System Assessment Group earned a reputation for technical excellence in cyber range development, cyber test and evaluation, cyber red-teaming and cyber exploitation. Lee's expertise provides a solid foundation to lead the development of capabilities to rapidly create and host realistic network environments and network clones, model sophisticated nation-state adversaries and develop data collection and analysis capabilities.

In the area of cyber ranges, Lee led the creation, development and deployment of the LARIAT traffic generation tool and related capabilities, which are currently used and operated at the major DoD cyber ranges and numerous other government and contractor laboratories. He has extensive experience in building and leading the development teams ensuring they meet the features, fidelity and priorities for the tests and programs being evaluated.

Lee holds dual degrees as a Bachelor of Science in Electrical Engineering as well as Computer Engineering from the State University of New York (Buffalo) and a Master of Science in Electrical and Computer Engineering from the University of Florida.

Lt Col Jenniffer F. Romero is the Joint Staff J7 Cyberspace Environment Division Chief managing all aspects of the Joint Information Operations Range (JIOR) operations to meet JIOR program requirements in support of CCMDs, Services, Agencies and the Test Community across the DoD. She coordinates with users and stakeholders to design, develop, and employ a cyberspace training, testing, and development environment. Her division ties complex cyberspace and information operations non-kinetic effects into testing and training environments spread through locations in multiple countries.

Additionally, she leads her division's participation in studies and collaborates with CCMDs, JS, OSD and Service Headquarters to analyze operational requirements, feedback, and lessons learned from operational assessments, training events, and from stakeholders and makes recommendations on policy changes. And finally, she oversees the integration of Information Operations and Cyberspace capabilities into the CCMD and Service training programs as specified in CJCS training guidance. Lt Col Romero is a 1993 graduate of Texas Christian University, where she was commissioned through Air Force ROTC.

Prior to her Joint Staff assignments, Lt Col Romero was the Deputy Group Commander, 435th Air and Space Communications Operations Group, Ramstein AB, Germany. During that assignment, she was also the Chief, Afghan Cyber Defense Cell for all of Afghanistan. She has been a squadron commander both in-garrison and deployed and is married to Major Michael Romero, USAF. They have two children, Thomas and Liam. She has been promoted to the rank of Colonel and will pin on the rank 1 April 2015.

Mr. John B. Schab is currently a Systems Engineering Lead for the MITRE Corporation where he supports the Director, Operational Test and Evaluation (DOT&E) and the Deputy Assistant Secretary of Defense for Developmental Test & Evaluation (DASD DT&E). He currently holds the following certifications: Certified Information Systems Security Professional (CISSP), GIAC Certified Enterprise Defender (GCED), GIAC Security Essentials Certification (GSEC), and CompTIA Security+.

Mr. Schab was formally the Director of the Aberdeen Field Office for the Georgia Tech Research Institute (GTRI). Prior to joining GTRI, Mr. Schab worked as a program manager for Trideum Corporation. His work assisted in developing new methods and procedures for testing and evaluating intelligent unmanned systems as well as planning and managing range improvement projects. Mr. Schab designed the Small Unmanned Ground Vehicle Test Course that was built at the Aberdeen Test Center in 2009.

Mr. Schab began his career as a project engineer with General Motors Corporation gaining experience in various departments including research & development, design, analysis, testing, and manufacturing. As a test engineer at GM, he was assigned safety and crashworthiness responsibilities for mid-sized sport utility vehicles. Mr. Schab and a co-worker earned GM's highest recognition for an innovative fuel tank design. He was also awarded multiple People Make Quality Happen awards through the use of statistical engineering methods combined with his test & evaluation experience. Upon his departure from GM, Mr. Schab served as a structural expert for the small car division of DaimlerChrysler Corporation.

Mr. Schab graduated from Cornell University with a Bachelor of Science Degree in Mechanical Engineering along with a Bachelor of Arts Degree in Physics from Ithaca College. In addition, he holds a Master of Science Degree in Engineering (MSE) from Purdue University along with a Master of Business Administration (MBA) and a Master of Science in Finance (MSF) from the Indiana University Kelley School of Business. He also holds a certificate in Defense Radar Systems from the Georgia Institute of Technology. Currently, Mr. Schab is pursuing a Master of Science in Information Security Engineering (MSISE) from the SANS Technology Institute where he is specializing in penetration testing and digital forensics.

Mr. Schab is a recognized expert in the T&E community. He currently serves on the Board of Directors for the International Test and Evaluation Association (ITEA) and served as technical track chairs for numerous T&E conferences. He previously served as the President for the Francis Scott Key Chapter of ITEA.

Ms. Tanya M. Skeen, a member of the Senior Executive Service, is Deputy Director of Test and Evaluation, Headquarters U.S. Air Force, Washington, D.C. She is responsible for policy, resources and oversight of developmental and operational testing, and is a focal point for foreign materiel acquisition and exploitation. She assists the Director in overseeing a $4 billion Air Force test infrastructure and the programming and execution of the Air Force test portfolio, with an annual budget of $1.9 billion.

Ms. Skeen is from Kent, Ohio, and was commissioned in the U.S. Navy in 1990 following graduation with highest distinction from Purdue University in Aeronautical and Astronautical Engineering. In the Navy, she served as a Technical Instructor and Assistant Director at the Nuclear Power Training Command and also received her Master of Science in Mechanical Engineering from the University of Central Florida in 1994. After leaving the Navy, she joined the private sector developing the next generation X-35 Joint Strike Fighter followed by several positions in flight test where she was responsible for test planning, execution and data analysis for nearly every aircraft in the current Air Force inventory including B-2, F-117, F-15, F-16 and F-22.

Additionally, Ms. Skeen was responsible for significant test range infrastructure upgrades for Red Flag testing as well as multiple programs that directly improved test range productivity. Following her private sector positions in flight test and other development programs, she returned to federal service in 2009 as the Program Executive Officer Chief Engineer at the Air Force Rapid Capabilities Office, Office of the Administrative Assistant to the Secretary of the Air Force, Washington, D.C. Her responsibilities at the AFRCO included technical oversight of a multi-billion-dollar portfolio and serving as the Program Director for programs including the Common Mission Control Center for multiple simultaneous mixed aircraft command and control.

Brigadier General Guy Walsh (USAF, Ret.), Strategic Initiatives, United States Cyber Command, serves as a technical advisor to the Deputy Commander, U.S. Cyber Command, Fort Meade, MD. In addition to directing joint cyber test efforts with the Office of Secretary of Defense (OSD) and Army Test and Evaluation Command (ATEC), he serves as the command's senior manager for the National Guard and Reserve Directorate working with OSD, military service components, and the National Guard Bureau (NGB) to develop strategy and policy for Reserve Component support to U.S. Cyber Command. Mr. Walsh also serves as a deputy director and senior mentor for U.S. Cyber Command's two Tier 1 Joint and Combined exercises, CYBER FLAG and CYBER GUARD. Prior to assuming his current role, Mr. Walsh served as the CYBERCOM J-3 lead for Strategic Initiatives. In this role, he was the principal advisor to the CYBERCOM Director of Operations on readiness, training and the development of Reserve Component cyber capability.

Mr. Walsh is U.S. Cyber Command's lead advocate for advancing policy and law regarding use of Title 32 authorities to protect and defend U.S. critical infrastructure. He has developed and initiated engagements and training programs between U.S. Cyber Command, Assistant Secretary of Defense for Homeland Defense (ASD-HD), FBI, DHS, State and local governments and private sector.

General Walsh had a distinguished career of 31 years of military service in the United States Air Force and the Air National Guard, commanding at the squadron, group and wing levels. He served as the Commander, 175th Wing, Maryland Air National Guard from 2002 thru 2009. In 2009-2010, Brigadier General Walsh commanded the 451st Air Expeditionary Wing in Kandahar, Afghanistan, becoming the first Air National Guard general officer to command an active duty air expeditionary wing in combat. Brigadier General Walsh is a command pilot having flown numerous tactical aircraft including the A-10 Thunderbolt II, F-4 Phantom, and C-130J Super Hercules. He retired in November 2010 having flown 4,200 hours and more than 100 combat missions including 79 A-10C Close Air Support missions supporting U.S. and NATO ground forces in Afghanistan.

General Walsh earned a Bachelor of Science degree in 1979 at the United States Air Force Academy and a Master's degree in International Relations and Strategic Studies from the University of Southern California. He attended Harvard University's Kennedy School of Government executive program for Homeland Security, and is a former National Defense Fellow, serving at the Institute for National Security Studies (INSS), Colorado Springs, CO. In 1990, he won the Anthony C. Shine award as the top fighter pilot in the United States Air Force. He received the Air Force Association Gil Robb Wilson Award for Arts and Literature in 2001 for work as co-editor of Spacepower for a New Millenium (McGraw-Hill, 2001). General Walsh's military decorations include the Legion of Merit, Bronze Star, Air Medal, Aerial Achievement Medal, the Maryland Distinguished Service Cross and numerous campaign medals.

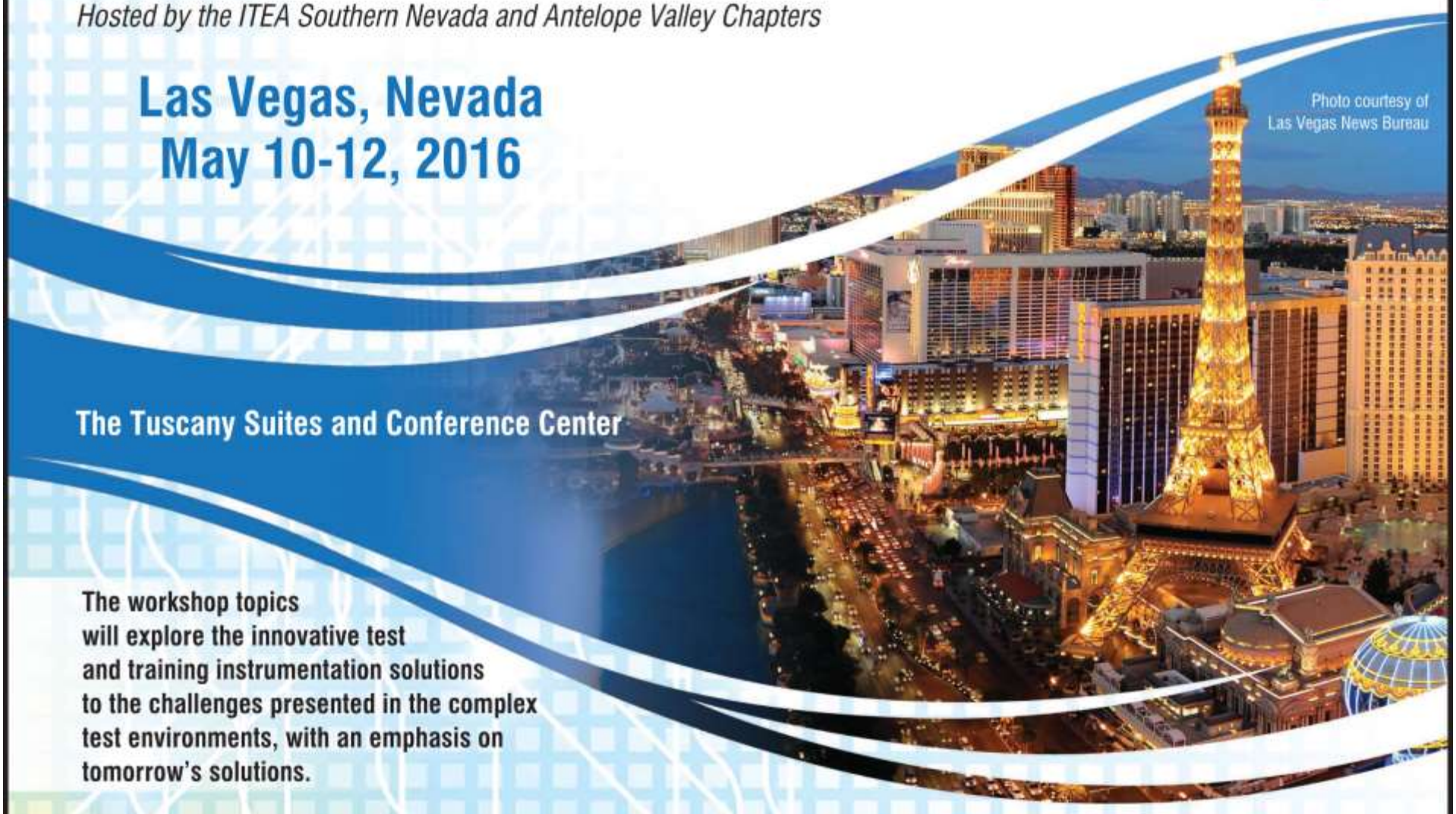
Mr. Michael Winslow is the Head of the Naval Network Analysis Branch at SPAWAR Systems Center Pacific and the Joint Program Manager for the Cyber TASE (Test Analysis and Simulation Environment) Centralized Test and Evaluation Investment Program (CTEIP) Project. Mr. Winslow has been working for the Government for 8 years running studies and evaluations for OPNAV N8, the Intelligence Community, SPAWAR CHENG, and various other DoD customers. Mr. Winslow supported the CANES Program Office as the Deputy Lead System Engineer up to the Program's Critical Design Review (CDR). Prior to working for the Government, Mr. Winslow worked for industry. Mr. Winslow holds two Bachelors of Science Degrees in Electrical Engineering and Mathematics from the University of California, San Diego.

George A. (Fred) Wright, Ph.D., is a Principal Research Engineer and Chief Engineer of the Cyber Technology and Information Security Laboratory at the Georgia Tech Research Institute. In 1987, Dr. Wright joined the Georgia Tech Research Institute where he has worked in network-centric and intelligence systems development and testing. The focus of his work is on technology support for novel paradigms distributed control systems. He has developed secure network-centric test and evaluation concepts and systems for all of the services and is currently supporting testing for the Marine Corp, Army, and Air National Guard. In addition, he currently works within the Cyber Security development and Cyber Commands for the Navy and Air Force. He received his Ph.D. in Electrical Engineering in 1996 from Georgia Institute of Technology.

20th ITEA Test Instrumentation Workshop

Hosted by the ITEA Southern Nevada and Antelope Valley Chapters

Las Vegas, Nevada
May 10-12, 2016



The Tuscany Suites and Conference Center

The workshop topics will explore the innovative test and training instrumentation solutions to the challenges presented in the complex test environments, with an emphasis on tomorrow's solutions.

Previous SPONSORS Include:

AMERICAN SYSTEMS
Engility Corporation
EWA Government Systems, Inc.
INQU, LLC
irig106.org
Jacobs - Teims
Joint Range Solutions
JT3 LLC
NetAcquire Corporation
PAE
TRAX International

For information on exhibiting or sponsorships, contact James Gaidry, 703-631-6220 or jgaidry@itea.org

REGISTER ONLINE:
www.itea.org

Previous EXHIBITORS Include:

ACROAMATICS Inc.
Advanced Test Equipment Rentals
AEgis Technologies Group, Inc.
Air Academy Associates
Ampex Data Systems
Apogee Labs, Inc.
Astro Haven Enterprises
Avionics Interface Technologies
CALCULEX, Inc.
CDW-G
CI Systems Inc.
Compunetix, Inc.
Curtiss-Wright Controls Avionics & Electronics
DEPS
DEWESoft, LLC
DEWETRON, Inc.
Dynetics, Inc.
Dytran Instruments, Inc.
Edge Consulting
Elotek Systems, Inc.
EMC Corporation
Emhiser Research
EWA Government Systems, Inc.
G.R.A.S. Sound & Vibration
GDP Space Systems
Geodetics, Inc.
Georgia Tech Research Institute - GTRI
IAI North America
Integrated Network Enhanced Telemetry Project
International Telemetering Conference
International Test and Evaluation Association (ITEA)
Jacobs - Teims
Joint Range Solutions
JT3 LLC
KRATOS Lancaster
L-3 Telemetry & RF Products
Lockheed Martin
Lockheed Martin Mission Systems
Meggitt Sensing Systems
NAVAIR
NAVAIR Weapons Div.
NetAcquire Corporation
OnTime Networks
PAE
PCB Piezotronics
Photo-Sonics, Inc.
PMSC/AssetSmart
Precision Filters, Inc.
Rotating Precision Mechanisms, Inc.
RT Logic
Saalex Solutions, Inc.
Smartronix Inc.
Spiral Technology, Inc.
SYMVIONICS Inc.
Systems Engineering & Management Company
Tektronix, Inc
Teletronics Technology Corporation
Telspan Data
TENA JMETC
TRAX International Corporation
Ulyssix Technologies, Inc.
Uniforce Sales and Engineering
Universal Switching Corporation
Wideband Systems, Inc.
Wyle
Zodiac Data Systems

Join us in Las Vegas – Register TODAY!

THANK YOU TO OUR SPONSORS!

Platinum Level Sponsor

EWA Government Systems, Inc.

Enabling a more secure future

Gold Level Sponsors

AMERICAN SYSTEMS™

wyle

Bronze Level Sponsor

ACQUIRED DATA SOLUTIONS