6th Cyber Security Workshop

"From Requirements to Test & Evaluation"

Program Guide

March 6-8, 2018

Ramada Plaza Beach Resort ~ Fort Walton Beach, FL

Hosted by the Emerald Coast Chapter

THANK YOU TO OUR SPONSORS!

Platinum Sponsor

ZODIAC DATA SYSTEMS

ZODIAC AEROSPACE

Gold Sponsors

AMERICAN SYSTEMS

CCAT CLEAR CREEK APPLIED TECHNOLOGIES

Georgia Tech Research Institute

KBRwyle We Deliver

Gold Sponsor

EWA Government Systems, Inc. Enabling a more secure future

Bronze Sponsor

CAPABILITY ANALYSIS CAMO LLC MEASUREMENT

ITEA is a 501(c)(3) professional education association dedicated to the education and advancement of the test and evaluation profession. Registration fees, membership dues, and sponsorships are tax deductible.

Sponsorship dollars defer the cost of the workshop and support the ITEA scholarship fund, which assists deserving students in their pursuit of academic disciplines related to the test and evaluation profession.

Program Committee

PROGRAM CHAIR

Mr. Jason Vosatka - 47th Cyberspace Test Squadron

PROGRAM TECHNICAL CHAIRS

Ms. Min Kim - AFLCMC, Armament Directorate
Mr. John Rafferty – 53rd EWG/F-35 PSC
Mr. Pete Crump – GTRI
Mr. Gene Hudgins - KBRWyle

WORKSHOP DESCRIPTION

Cybersecurity is in the forefront of the DoD acquisition community. It is particularly challenging for the non-Information Technology (IT) community to understand, capture, and interpret cybersecurity requirements. The Test & Evaluation (T&E) community needs to develop strategies for "bolting-on" and "baking-in" cybersecurity into legacy systems and new acquisition programs; all while executing T&E activities of non-IT systems. This workshop provides the opportunity to share experiences, lessons learned, and generate new ideas on cybersecurity from "Requirements to Test & Evaluation" amongst experienced T&E professionals.

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, or 20 contact hours of instruction (20 CEUs) for attending the full Workshop, that are directly applicable to your professional development program, including the Certified Test and Evaluation Professional Credential (CTEP).

Please send your request for a Certificate of Attendance to certification@itea.org

---

INDEX

2018 Test and Training Instrumentation Workshop

Hosted by the ITEA Southern Nevada and Antelope Valley Chapters

Supporting the Warfighter from Test to Training —Understanding the 3rd Offset

Las Vegas, Nevada • May 15-17, 2018

Photo courtesy of Las Vegas News Bureau

The Tuscany Suites and Conference Center

This year's goal is to identify and address those instrumentation and data collection issues and challenges faced by the test and training communities to support current and next generation weapon system testing and training missions.

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 Lena Moran, 951-219-4817 or Lmoran@traxintl.com

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!

Tuesday, March 6th

8:00 a.m. – Noon Morning Pre-Workshop Tutorials (Separate fee required)

Cybersecurity Test & Evaluation (Empire Ballroom)

Instructor: **Mr. Pete Christensen – Director, Cyber Support to OSD Programs, The MITRE Corporation**

Now more than ever, Program Managers (PM) must ensure that cybersecurity be given careful consideration throughout the system lifecycle. Specifically, this includes identifying cybersecurity requirements early in the acquisition and systems engineering lifecycle. Initiating a focus on cybersecurity earlier will provide PMs the opportunity to give careful consideration, upfront, to related cybersecurity testing activities that can be integrated into the engineering planning and design phases. Results of informal cybersecurity testing can then be applied to influence design and development efforts and to posture programs for success in Developmental Test (DT) and Operational Test (OT). The Deputy Assistant Secretary of Defense (DASD) Developmental Test and Engineering (DT&E) has collaborated with key systems engineering stakeholders to develop disciplined processes that will assist Program Managers (PM) in implementing an incremental and iterative phased approach to develop cyber secure systems. The National Cyber Range (NCR), under the purview of the Test Resource Management Center (TRMC), is a resource that can be leveraged by PMs to support cybersecurity testing. This presentation will provide an overview of the cybersecurity test and evaluation phased approach and the NCR.

How to Use Data Mining Methods to Better Detect Cyber Attack (Ambassador)

Instructor: **Thomas A. Donnelly, PhD, CAP, SAS Institute, Inc.**

This tutorial will primarily focus on learning how to effectively apply various data mining methods to existing internet traffic data with known cyber-attacks to build scoring models to monitor new traffic to flag potential attacks. Data mining methods to be discussed include decision trees, logistic regression, penalized regression, and neural networks. Model averaging, and the building of ensemble models will be shown to improve prediction over individual models. Effective methods to prevent overfitting models to data will be presented. The data mining methods taught can effectively be used with any large data sets in the T&E community such as databases of sensor data.

Planning and Executing Cyber Table Tops, Facilitator Training (Forum)

Instructor: **Ms. Sarah Standard, Cybersecurity/Interoperability Technical Director, DASD DT&E**

The primary objective of the Cyber Table Top (CTT) Facilitator Training Workshop is to build the knowledge, skills and abilities that will allow trainees to successfully construct, coordinate, organize, and execute a Cyber Table Top (CTT) exercise. The primary audience for this training are those personnel who will facilitate and moderate CTT's for their program, command. The training will include tips, tools, and resources for CTT facilitators as well as a practical example of the process and outputs.

1:00 PM – 5:00 PM Afternoon Pre-Workshop Tutorials (Separate fee required)

Identifying Requirements and Vulnerabilities for Cybersecurity, and the Fundamentals of Distributive Testing (Empire Ballroom)

Instructors: **Michael Lilienthal, PhD, CTEP, Director of Cyber and Navy Programs, Electric Warfare Associates, and Mr. Patrick Lardieri, Lockheed Martin Corporation**

Many Service acquisition, System Engineering (SE), and Test and Evaluation (T&E) teams are starting to move their programs from "checklist information assurance or compliance" cyber security approach to a proactive, iterative risk management process with the goal of ensuring personnel can still carry out their duties in a cyber contested environment. Many people are struggling to formulate a practical and effective approach to develop requirements and a plan to incorporate cyber security into their SE and T&E activities using the recent spate of cybersecurity policies and guidelines released by the Office of the Secretary of Defense (OSD). This tutorial will step using the Navy's Cyber Table Top (CTT) Wargaming Process and the National Cyber Range's cyber security evaluation testing process as an approach to gain actionable cyber threat understanding. The tutorial will also show how the use of the CTT and the NCR support execution of DOT&E's Six Phase Cybersecurity T&E process. The CTT (which has been adopted by the Navy) is a rigorous, intellectually intensive and interactive data collection and analysis process that introduces and explores the potential effects of cyber offensive operations on the capability of a system to carry out its designed functions. It produces a prioritized list of actionable recommendations to support more informed decisions and tradeoffs in a fiscally constrained environment.

Personnel using the process are better able to identify threat vectors, understand the vulnerabilities and mission risks of their system under development, and understand cyber threat consequences categorized by their impact and their likelihood of successful attacks. This helps scope the cyber security testing done at the NCR and other places. The tutorial will also show how the use of the cyber wargaming process in conjunction with the NCR will inform systems engineers on tradeoffs and potential workarounds to prevent or minimize cyber effects. The tutorial is based on the lessons learned from using the process and the NCR to support NAVAIR and SPAWAR acquisition programs. It is intended for use by Acquisition Program Management Offices, Systems Engineers, Chief Developmental Testers, and Lead Developmental Test and Evaluation (DT&E) Organizations.

Mission Threat Analysis and Cybersecurity (Ambassador)

Instructors: **Mr. James Wells, Deputy Director for Cyberspace and Homeland Security Enterprise Systems, Office of Test and Evaluation, Science and Technology Directorate, Department of Homeland Security, and Mr. Alex Hoover, Deputy Director for Cybersecurity Engineering, Office of Systems Engineering, Science and Technology Directorate, Department of Homeland Security**

For cybersecurity to not be a "bolt-on" to the development effort, it must be considered as part of the holistic security requirements process. This tutorial will walk through an integrated threat analysis process that treats cyber capabilities as a combined-arms part of threats' overall capabilities to subvert and exploit government missions supported by information technology. Specific points to be addressed and discussed are:

- Starting with the operational compromise baseline vice a historical list of cyber events
- Characterizing the potential mission impacts of all the threat's capabilities
- Identifying which portions of the threat's intent are likely to be carried out in cyberspace
- Mapping the relevant potions of the threat's intent to the technical and data architecture
- Using the attack surface as the basis for adversarial
- Defining the evaluation boundaries in terms of initial conditions for adversary TTP
- Designing cyber events into the performance space for effectiveness and suitability evaluation
- Scoping an appropriate Rules of Engagement for the adversarial team
- Integrating live, virtual, and constructive adversarial analysis into a composite cyber evaluation

The threat analysis topics will be discussed from a government leadership and management perspective, focusing on what to get done rather to what to do at an implementation level.

Fundamentals of Hardware Security and Assurance (Forum)

Instructors: **Mr. Jason Vosatka -** 47th Cyberspace Test Squadron

The world of Cybersecurity is rapidly evolving with emerging threats and new vulnerabilities being exploited every day. The traditional Computer Science perspective of Cybersecurity focuses on software and networking and relies on an inherent trust of the underlying hardware. However, the argument that hardware is inherently trustworthy is no longer accurate. Over the past decade, there has been a dramatic shift in the business models of design companies as they move from organic in-house capabilities towards an outsourced global marketplace. Companies are now being forced to rely on untrusted foundries and vendors to supply hardware, intellectual property, and other components that are integrated into electronic systems. These trends and dependencies are creating unprecedented attack surfaces for adversaries; therefore, resulting in new risks to the hardware comprising all electronic systems.

In this tutorial, we focus on learning the fundamental concepts of Hardware Security and Assurance of Microelectronics. This tutorial provides an insight into Counterfeit Integrated Circuits affecting supply chains, Hardware Trojan attacks and countermeasures, and Side-Channel Analysis techniques regarding extraction of sensitive information. We will also cover intrinsic hardware security primitives such as Physically Unclonable Functions, offensive physical attacks such as Reverse Engineering of ICs and Printed Circuit Boards, as well as defensive techniques of Hardware Metering and Split-Manufacturing. We also touch on other topics including basics of cybersecurity, applied cryptography, cross-layered systems security.

If you are curious about the following questions, this course is for you:

- How do we test and evaluate the hardware components and chipsets (e.g., ASIC, FPGA, SoC, MPU/MCU, PCB) that are installed into electronic systems to determine if they are genuine or counterfeit?
- How can malicious modifications, tampering, and backdoors in hardware jeopardize the security of trusted platforms?
- How do we research and analyze electronic systems for leakage (e.g., power, timing, EMI/RF) of sensitive information?

The goal of this tutorial is for students to gain an introductory education of this emerging hardware-centric domain of Cybersecurity. It will be taught from the Electrical & Computer Engineering perspective, which is a novel departure from the conventional Computer Science viewpoint. This tutorial will span several topics and dive into specific aspects offering both academic theory and real-world examples; all without the rigorous mathematics. It will not cover policies and procedures, but the topics covered will better educate the Test & Evaluation community.

Wednesday, March 7th

Workshop Opening Plenary Session (Ambassador)

8:00 a.m. Welcome - **Mr. Pete Crump**, ITEA Vice President, GTRI

8:15 a.m. Opening Remarks – **Mr. Jason Vosatka**, Workshop Chair, 47th Cyberspace Test Squadron

8:30 a.m. Opening Keynote - **Joseph Nichols, PhD**, Technical Advisor for Flight Test and Evaluation, AFTC

9:00 a.m. Featured Speaker – **Mr. James D. Tuttle,** Chief Systems Engineer, Science and Technology Directorate, DHS

9:30 a.m. Guest Speaker – **Ms. Sarah Standard**, Cybersecurity/Interoperability Technical Director, DASD DT&E

10:00 a.m. Break (Ambassador Forum)

10:30 a.m. Technical Track Sessions

TECHNICAL SESSION I: Vulnerability Identification				
Ambassador Room				
CHAIR: Paul Waters, PhD				
10:30 AM	***Reversing Cyber Risk Assessments for High-Value Returns***	Brian Mork, PhD	Plans and Programs	AFRL/XPZ, Wright Patterson AFB
11:00 AM	***A Cyber Table Top for Equipment Vendors***	Mr. Bob Baggerman	Senior Field Applications Engineer	Zodiac Data Systems
11:30 AM	***Lessons Learned and Recommendations for Conducting a Cyber Table Top in T&E***	Mr. Tristan Gilbert		WSMR
TECHNICAL SESSION II: Workforce Development				
Forum Room				
CHAIR: Mr. John Rafferty				
10:30 AM	***Acquisition Workforce Cyber Education & Training***	Mr. Steve Rajotte	Cyber Workforce Development Division Chief	Cyber Resiliency Office for Weapons Systems (CROWS), AFLCMC/EN
11:00 AM	***Building a Cyber Workforce of Security Testers Through Training and Certification Beyond Penetration Testing***	Mr. Randall Rice		American Software Testing Qualifications Board (ASTQB)
11:30 AM	tba			

Noon Lunch (Ambassador Foyer)

1:00 p.m. **Technical Track Sessions**

TECHNICAL SESSION III: Cybersecurity Requirements				
Ambassador Room				
CHAIR: Mr. Marshall Bronston				
1:00 PM	***Leveraging Secure Systems Analysis to Generate Testable Cyber Security Requirements***	Col William Young, Jr, USAF, PhD	Commander	53d Electronic Warfare Group
1:30 PM	***Cyber Requirements Engineering***	Mr. Al Morris CISSP, CEH, CHFI		People Tec
2:00 PM	***Identifying Requirements and Vulnerabilities for Cybersecurity; Or How I Learned to Stop Worrying and Love the Six-Phase Cybersecurity T&E Process***	CAPT Michael Lilienthal, PhD (USN Ret)	Director of Navy and Cyber Programs	EWA
TECHNICAL SESSION IV-A: Risk Assessment				
Forum Room				
CHAIR: Mr. Jason Vosatka				
1:00 PM	***Leveraging Machine-assisted Technologies for Platform Security Assessments***	Mr. Elbert Michael Ruiz	Senior Research Engineer	Georgia Technology Research Institute
1:30 PM	***Hardware Assurance Lifecycle Ecosystem: "Distributed Transition Environment"***	Matt Casto, PhD		AFRL/RYDP
2:00 PM	***Trusted and Assured Microelectronics Hardware Assurance Evaluation and Test Capabilities***	Jeremy Muldavin, PhD		ODASD(SE)
TECHNICAL SESSION V: Shift Left				
Empire Ballroom				
CHAIR: Mr. Gene Hudgins				
1:00 PM	***Cybersecurity Policy and Resiliency***	Mr. Edward Adkins	Professor of Engineering, Test and Cybersecurity	Defense Acquisition University
1:30 PM	***SHIFT LEFT: Army T&E Efforts to Address Cybersecurity Earlier in the Acquisition Cycle***	Mr. Patrick A. Thompson	Technical Director, Survivability Evaluation Directorate	U.S. Army Evaluation Center, Army Test and Evaluation Command
2:00 PM	***Using Modern SE Methods for Cyber Design & Test***	Mr. Frank Alvidrez	Senior Bomber Test Analyst	Spectrum Inc

2:30 p.m. **Break (Ambassador Foyer)**

3:00 p.m. Technical Track Sessions

TECHNICAL SESSION VI: Next Generation Cyber Resilience				
Ambassador Room				
CHAIR: Mr. Dave Brown				
3:00 PM	***Defining Resiliency***	Ms. Dawn Williamson	Resiliency and Security Engineering Lead	Northrop Grumman Aerospace Systems
3:30 PM	***A Program Framework for Cyber Resilience***	Ms. Rose Daley		John Hopkins University APL
4:00 PM	***Self-Cleaning Intrusion Tolerance (SCIT): A new approach to reduce the impact of data breaches***	Arun Sood, PhD		George Mason University and SCIT Labs
TECHNICAL SESSION IV-B: Risk Assessment				
Forum Room				
CHAIR: Mr. Bob Baggerman				
3:00 PM	***Quantifiable Cybersecurity Risk Assessments of Weapon Systems during Developmental Test***	Mr. Steve Klynsma	Principal Engineer	Army Program Directorate MITRE
3:30 PM	***Applying Quantifying Methods to Improve Cyber Security Risk Mitigation Selections for Aircraft***	Mr. Roger Beard		CAMO LLC
4:00 PM	***Hardware Exploits: Can You Trust Your Devices?***	Ms. Christina Witt	JT3 Information assurance and Validation Support Lead	Edwards AFB

4:30 p.m. Networking Reception (Beach Patio)

JOIN US IN OXNARD, CA

SAVE THE DATE

Dec. 11-14, 2018

35TH ANNUAL INTERNATIONAL

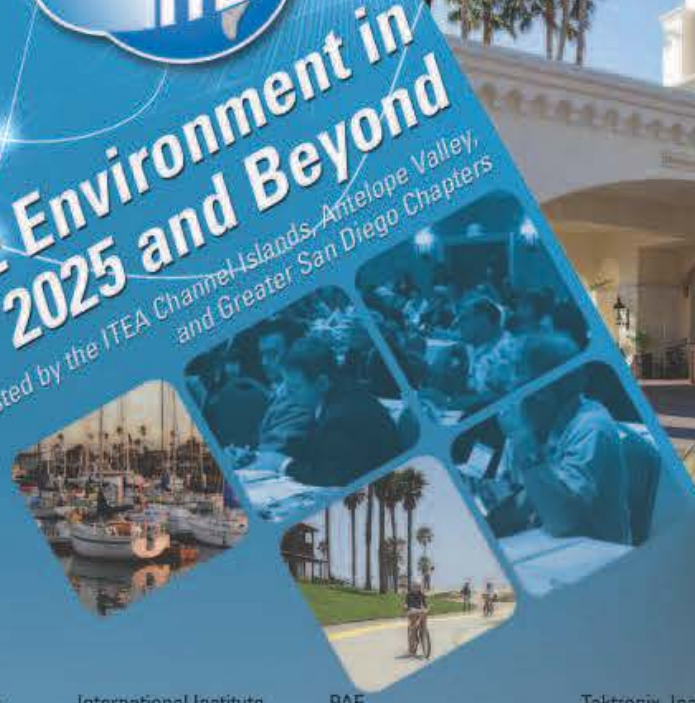
Test and Evaluation

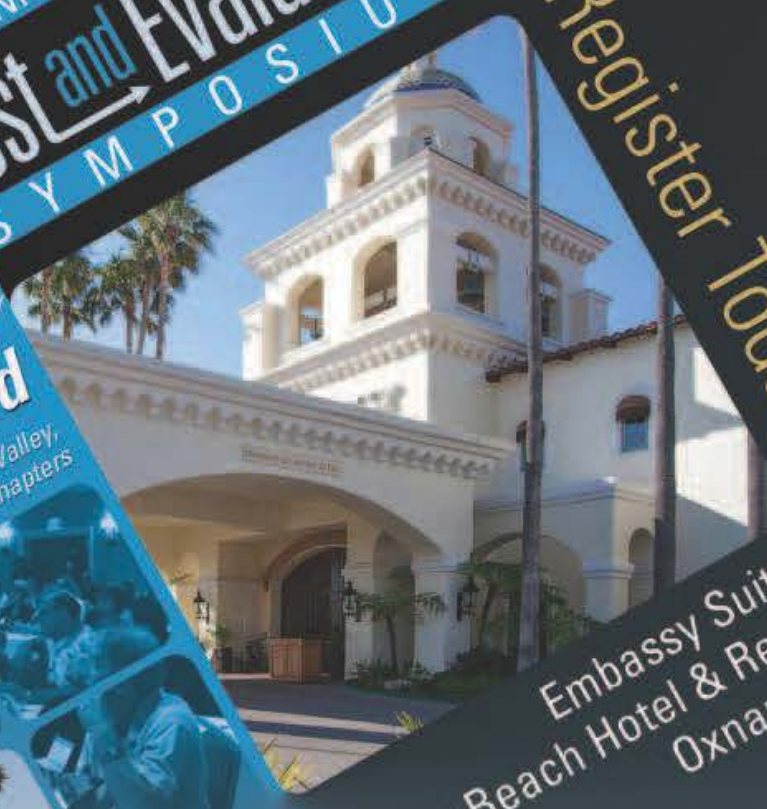
SYMPOSIUM

Register Today!

Global T&E Environment in 2025 and Beyond

Jointly Hosted by the ITEA Channel Islands, Antelope Valley, and Greater San Diego Chapters





Embassy Suites
Mandalay Beach Hotel & Resort
Oxnard, CA

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
DET S&T
DEWESoft, LLC
DEWETRON, Inc.
Directed Energy Professional Society (DEPS)
DRS Technologies
Dynetics, Inc.
Dytran Instruments, Inc.
Edge Consulting
Elotek Systems, Inc.
EMC Corporation
Emhiser Research
EMRTC New Mexico Tech
EWA Government Systems, Inc.
GDP Space Systems
General Dynamics Mission Systems
Geodetics, Inc.
Georgia Tech Research Institute - GTRI
Glacier Technologies
G.R.A.S. Sound & Vibration
HEL-JTO
IAI-ELTA
IAI North America
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)
SemQuest
SimIS Inc.
Smart Card Alliance
Smartronix Inc.
Spiral Technology, Inc.
STAR Dynamics, Inc.
SURVICE Engineering Company
SYMVIONICS Inc.
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
University of Memphis System Testing Excellence Program
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

Program Chair - Terry Clark, EWA GSI
Program Technical Chair - Gil Torres, Naval Air Systems Command
Exhibits and Sponsorships Chair – Eileen Redd, EWA GSI
Tutorial Chair – Vacant
International Panel Chair – Gloria Deane, DOT&E
Awards Committee Chair - Stephanie Clewer, PAE

Host Chapter Presidents
Antelope Valley Chapter: Christopher Klug, Edwards AFB
Emerald Coast Chapter: Joyce Matias, Naval Air Systems Command
Greater San Diego Chapter : Dan Phelan, Boarhog LLC

For information on exhibiting or sponsorships contact Eileen Redd at eredd@ewa.com

REGISTER ONLINE AT: **www.itea.org**

Thursday – March 8th

Workshop Plenary Session (Ambassador)

8:00 a.m. Day 2 Remarks – **Ms. Min Kim,** Technical Program Co-Chair, AFLCMC, Armament Directorate

8:05 a.m. Keynote Address - **Mr. William (Bud) Redmond**, Executive Director, AFOTEC

8:35 a.m. Featured Speaker – **Mitch Crosswait, PhD**, Deputy Director, Net-centric, Space and Missile Systems, DOT&E

9:05 a.m. **Town Hall on Cyber Resilience** - Mr. Dave Brown, Director of Cyber Programs, EWA

10:00 a.m. Break (Ambassador Foyer)

10:30 a.m. Technical Track Sessions

TECHNICAL SESSION VIII: Test and Evaluation				
Ambassador Room				
CHAIR: Mr. Chip Ferguson				
10:15 AM	***The Test Resource Management Center's Vision for Developing Cyber Test Range Capabilities***	Mr. Bernard B. (Chip) Ferguson		TRMC
10:45 AM	***Challenges and Opportunities of Autonomy Vulnerability T&E***	Mr. Don Strausberger	Principal Engineer	Aerospace, Transportation, and Advanced Systems Laboratory, GTRI
11:15 AM	***Applying Statistical Test Optimization Techniques to Cyber Testing***	Ms. Tonja Rogers Ms. Mary Kim Mr. Peter Kraus Mr. Neal Mackertich		CODE Center, Raytheon
TECHNICAL SESSION VII: Systems Security Engineering				
Empire Ballroom				
CHAIR: Mr. John Rafferty				
10:15 AM	***Test Case Design via Model Based Systems Engineering***	Mr. Marshall Bronston	Professional Research Engineer	Georgia Tech Research Institute
10:45 AM	***Institutionalizing a Proactive Cybersecurity Posture***	Mr. Gregory Jaeger	Senior Program Manager	Advanced Technology International
11:15 AM	***Cybersecurity Vs Cyber Survivability: Implementing a Paradigm Shift in T&E***	Mr. Michael Landolt		Army Test and Evaluation Command

TECHNICAL SESSION IX-A: Cybersecurity Research			
Forum Room			
CHAIR: Mr. Jason Vosatka			
10:15 AM	***Hardware for Cyber (H4C): A Suite of Electronic System Protections from Nato to System Levels***	Domenic Forte, PhD	University of Florida
10:45 AM	***Cybersecurity: From Test & Evaluation to Requirements***	Lok Yan, PhD	AFRL/RIGA
11:15 AM	TBA		

11:45 AM Lunch (Ambassador Foyer)

12:45 p.m. Technical Track Sessions

TECHNICAL SESSION X: T&E and Authorization				
Ambassador Room				
CHAIR: Mr. Bob Baggerman				
12:45 PM	***TENA and JMETC for Distributed and Cyber Test and Training***	Mr. Gene Hudgins		TENA/JMETC
1:15 PM	***TRMC Authorizing Official and RMF Processes***	Ms. Robin Deiulio	TWS ISSM	TRMC
1:45 PM	***Range Commander's Council Cyber Security Group***	Paul Waters, PhD		Edwards AFB
TECHNICAL SESSION XI: HW/SW Assurance				
Forum Room				
CHAIR: Mr. Pete Crump				
12:45 PM	***Cyber T&E of Weapon Platforms and Systems***	Mr. Ron Prado	Principal Research Engineer	Georgia Tech Research Institute
1:15 PM	***Stop looking under the (Cyber) lamp-post***	Mr. Arch Owen Mr. Mike Aucoin Mr. Neil Brock		Draper
1:45 PM	***Covering Arrays: Evaluating coverage and diversity in the presence of disallowed combinations***	Thomas Donnelly, PhD	JMP Senior Systems Engineer	SAS Federal LLC

2:15 p.m. Break (Ambassador Foyer)

2:30 p.m. **Technical Track Sessions**

TECHNICAL SESSION VI-B Next Generation Cyber Resilience				
Ambassador Room				
CHAIR: Mr. Dave Brown				
2:30 PM	***Cyber Security Test and Methodologies for Improving Mission Cyber Resiliency***	Mr. Daniel Nguyen Mr. Ralph Galetti Mr. Adonis Williams	Cyber Test Engineer	Boeing Test and Evaluation
3:00 PM	***Avoiding Elicitation***	Ms. Christina Witt, CISSP, CAP		JT#, Edwards AFB
3:30 PM	***Next Generation Cyber Test***	Mr. Steven Newton		47th Cyberspace Test Squadron
TECHNICAL SESSION IX-B: Cybersecurity Research				
Forum Room				
CHAIR: Mr. Kevin Burns				
2:30 PM	***System of Systems in a Cyber Range Environment***	Mr. Roderick Hallum		Joint Staff J6
3:00 PM	***Are Password Resets Using Emails Secure?***	Mr. Caleb Routh		University of North Florida
3:30 PM	***Assessing the Growing Threat to AI Applications***	James Cannady, PhD		Georgia Tech Research Institute

Workshop Closing Plenary Session (Ambassador)

4:00 p.m. Closing Keynote Address - **Mr. George Rumford -** Deputy, Director, Major Initiatives and Technical Analyses, TRMC

ABSTRACTS

A Cyber Table Top for Equipment Vendors

By Mr. Bob Baggerman - Zodiac Data Systems

Cyber security begins with a realistic risk assessment. NIST SP 800-131 provides general guidelines for a cyber risk assessment. Various risk assessment methods have been developed tailored to specific industries. The Cyber Table Top (CTT) risk assessment methodology is popular within the DoD for executing a cyber risk assessment. A CTT is a "thought" exercise pitting a red team against a blue team in simulated attack scenarios. A comprehensive CTT takes considerable people and time resources, often beyond the means of small product manufacturer. This paper presents the results of a small CTT exercise performed with flight test instrumentation developers. The preplanning methodology and attack scenarios are described, as well as the results and limitations of the exercise itself.

A Program Framework for Cyber Resilience

By Ms. Rose Daley - JHU/APL

Cyber-enabled technology and services are rapidly changing—more than any previous technology surges that drastically impacted society including transportation, power, and telephony—and will consistently evolve at alarming rates as the demand continues to escalate. Cyber-enabled technology and services will also become even more pervasive as functions that cannot be performed by human capital alone evolve. Many critical systems and platforms will be, by definition, exposed to an adverse cyber environment with an intelligent adversary that will use every capability necessary to achieve desired effects—for material gain (cybercrime) or for nation-state objectives. Strong cyber defenses can deter attacks from all but very well-provisioned, patient, and sophisticated adversaries willing to apply substantial resources to breach them, but while strong defenses are important, it is equally, if not more important to build systems, and their associated acquisition programs, that are resilient to cyber-attacks. In cyberspace, it is impossible to produce a fully resilient system when an adversary can know virtually everything about it well in advance of its deployment and may even be able to access or influence critical components and milestones. The path to developing an effective cyber resilience capability requires not only technology development, but also requires a balanced engineered system and associated development program that address technology, people and processes over the entire lifetime of the operational system. We introduce a resilient program framework that builds a holistic support structure to develop effective systems meeting operational requirements throughout the lifecycle, producing capabilities that remain resilient until the system is removed from service. The framework considers both system and adversary evolution—acknowledged but unknown current and future threats and cyber effects that could impact the operational performance—within the context of system development, test, evaluation, operational deployment and future improvement.

Acquisition Workforce Cyber Education & Training

By Mr. Steve Rajotte - USAF, Air Force Life Cycle Management Center

As the acquisition community continues to address cyber security in aircraft, armament and other embedded weapon systems, one of the key enablers is a trained and educated technical workforce. Each member of this workforce should have expertise, or at least working knowledge, in three distinct areas: acquisition policy/program management; system and sub-system subject matter expertise; and cyber security and resiliency principles. Unfortunately, much of the training that is currently available does not quite hit the mark. Some training continues to focus on why cyber security and resiliency are important but does not describe how to implement them. Existing classes on embedded system standards such as Link-16 or MIL-STD-1553 teach functionality, but not necessarily from a cyber perspective. Industry cyber security courses and certifications are heavily influenced by the traditional information technology environment which may not be particularly relevant to weapon systems cyber security. The Air Force Cyber Resiliency Office for Weapon Systems is building a notional training framework to fill this gap. This curriculum will leverage National Initiative for Cybersecurity Education domains and work roles under the National Institute of Standards and Technology, and work with Defense Acquisition University, Air Force Institute of Technology and industry partners to build or maintain courses tailored to meet training requirements. These training needs will evolve as operators and acquirers better understand how to incorporate cyber security and
resiliency as part of broader capability requirements, and as program offices and test squadrons integrate cyber into existing unit training and certification programs.

Applying Quantifying Methods to Improve Cyber Security Risk Mitigation Selections for Aircraft

By Mr. Roger Beard - CAMO LLC

This presentation outlines an application of modeling and simulation, threat modeling, and situation awareness methods to guide cyber risk tolerance selection, guide risk assessments, and assess effectiveness of proposed risk mitigations of aircraft systems. These methods are applied towards understanding complex system behavior, understanding defender and adversarial work factors, and the validation of mitigation effectiveness. Understanding complex system behavior underpins the setting of risk tolerances for a system as applied in operation, what risks exists, and whether proposed mitigations afford intended protections against risk caused by unexpected complex system behavior. Understanding complex system behavior also helps with developing or refining the metrics needed to set risk tolerance levels within an operational viewpoint. Identifying effective mitigations to aircraft cyber security risks is a challenging problem. Resources may be spent on mitigations with little efficacy to the problem at hand. Risk tolerances are needed to determine whether mitigations are necessary or whether mitigations effectively bring risk below risk tolerance or, at least, bring risk closer to an acceptable level of risk tolerance. Understanding the behavior of complex systems and the adversarial nature of the risk is essential to determine cyber risk, guide the selection of risk tolerance, and guide mitigation assessments that are critical to making mitigation resource commitments. Ideally, assessments of risk and mitigation effectiveness would match that which will happen in the real world. However, diverse issues contribute uncertainty into risk tolerance, risk, and mitigation assessments. Primary issues include: The multi-disciplinary nature of the problem; A shortage of Subject Matter Experts (SMEs); The difficulty of

validating mitigation effectiveness; Inconsistent risk assessment results caused by exclusive use of subjective assessment methods; Assessments done in absence of risk tolerances; and, The adversarial nature of the problem. One approach to better identify or augment effective mitigation selection is to combine available expertise with validated assessment methods to guide and provide answers within contexts set by SMEs. This approach reduces the role of subjectivity in assessments, increases the consistency of assessments resulting in an increased understanding of complex system behavior that, in turn, provides an increased understanding of the efficacy of proposed mitigations.

While not a guarantee to create assessments that will exactly match future real-world events, a better understanding of both complex system behavior and effects of mitigations increases the chances that assessments will represent future real world cyber security events and mitigation efforts have intended effects. A deeper understanding of complex system behavior is the core activity for identifying effective mitigations. Collaboration among the various SMEs (cyber, operations, system of system engineers, etc.) captures the multi-disciplinary factors involved and will likely be a major mission of the National Cyber Range and the Air Force Cyber Range. Integrating these factors using well-established system of systems processes and procedures – to include integration of multiple models and simulations – will inform the aircraft cyber risk assessment with operationally credible insight to significantly improve the overall cyber security risk assessments for aircraft systems, as well as other C4ISR systems.

Applying Statistical Test Optimization Techniques to Cyber Testing

By Ms. Tonja Rogers, Ms. Mary Kim, Mr. Peter Kraus, and Mr. Neal Mackertich - Raytheon

Statistical Test Optimization (STO) techniques have been successfully applied to system level testing of complex DoD systems, reducing the overall number of tests required to satisfy the technical requirements. Using STO ensures that a balanced set of tests are recommended that provide maximum coverage of the 'test space'. This paper is taking that methodology and applying the same STO techniques to Cyber Assessments to provide for consistent, thorough, and efficient test recommendations. Cyber Assessments today are a necessary component to ensuring that the system or systems are resilient to Cyber-attacks. However, there is often a disparity in the understanding between what types of Cyber Assessments should be conducted and the details associated with the different types of Cyber tests. Having the ability to take information about a system and generate an initial test plan will help bridge the gap between the test team and the program by providing an understanding of what types of Cyber Security Assessments (CSA) would be applicable, the initial set of relevant test cases by CSA type, and the applicable test tools that could be used to complete the engagement. In order to apply STO techniques to Cyber tests, the team would gather relevant factors that would be used to develop a test plan. Based on these factors and the constraints built for the project, a test plan would be generated using STO logic and processes. The test team supporting this effort will describe the process of developing a generic STO plan based on the types of CSA(s) such as Software Assurance; System and Network Vulnerability Assessments; Physical Assessments; Cyber Forensics and Reverse Engineering. The Cyber STO plan will allow any tester to customize the parameters to develop the best test plan for the pertinent CSA(s).

Are Password Resets Using Emails Secure?

By Mr. Caleb Routh - University of North Florida

In this work, we examine the vulnerabilities in using an e-mail as a self-service password reset point by exploiting vulnerabilities in e-mail server forgotten password reset paths. We will perform hacks of a personal Email account using a variety of tools such as; public knowledge attainable through social media or public records to answer security questions, password sniffers to obtain saved passwords on the computer, 'remember me' function of a service, exploiting weaknesses in mobile coding, and cracking the encryption used on the password recovery email itself.

Assessing the Growing Threat to AI Applications

By James Cannady, PhD - Georgia Tech Research Institute

In the past several years a series of major technological advances in the field of artificial intelligence (AI) have begun to revolutionize all aspects of information technology. Over $39 billion was spent on AI applications in 2016 and the worldwide growth in AI-enabled applications exceeded 135% in 2017. These new applications range from enhanced web search engines to AI-enabled applications that manage critical national security and industrial control systems. However, while AI offers significant enhancements to these applications it also has resulted in the development of a new series of threats and vulnerabilities. With the growth of machine learning in a range of technology applications the potential has arisen for a dedicated attacker to identify and manipulate the logic used by the AI. As the potential vulnerability of these algorithms increases the acceptance of the benefits of machine learning, especially in critical applications, is in doubt. A new area of research, known as Adversarial Learning, is focused on understanding these new threats to AI systems and in developing new methods of ensuring the reliability of security of AI-based applications. In this talk I will discuss Adversarial Learning, including the emerging threats to AI applications and the new approaches that are being designed to facilitate the evaluation of the specific threats posed to these applications. Additionally, new defensive measures that are being developed to protect AI-enabled applications from these emerging threats will also be discussed, with particular focus on methods to evaluate the effectiveness of these new security techniques.

Avoiding Elicitation – Elicitation is painless

By Christina Witt, CISSP, CAP - JT3

Elicitation is painless. The target is unaware it is happening, the target likes the adversary, and the target will thank the adversary for taking the information. This is because elicitors take into consideration the human factors of elicitation such as the natural tendency to discuss things that are not their direct concern, tendency to correct others, tendency to gossip, exploiting natural curiosity, and the desire for recognition. Learn the various elicitation tools used to obtain controlled unclassified or classified information, why they are effective, what red flags to look for, and tactics to thwart the tools used by an elicitor.

Building a Cyber Workforce of Security Testers Through Training and Certification Beyond Penetration Testing

By Mr. Randall Rice - American Software Testing Qualifications Board (ASTQB)

When asking senior-level executives or security administrators about the adequacy of their organizations' information security defenses, most people will list things such as encryption, firewalls, malware protection, and so forth. When asked, "How effective are your defenses?" most people can't give a definitive answer because the defenses have not been tested in a continuous and holistic way. Many people believe the status quo position that penetration testing is all that is needed to find security vulnerabilities. To help meet the need of training software testers and others in how to perform security testing as a specialty practice, the International Software Testing Qualifications Board (ISTQB) has developed an Advanced Level Security Tester syllabus and exam which leads to the CTAL-SEC designation. The American Software Testing Qualifications Board (ASTQB) administers this certification in the United States. The goal is help build a cyber workforce of security testers at an advanced level. This syllabus is freely available and draws from sources such as NIST, CERT and OWASP to describe the in-depth knowledge needed to test the security of systems and applications of all types. This syllabus and certification covers the topic of penetration testing but goes beyond penetration testing to test internal controls and procedures, identify vulnerabilities at the code level, perform security risk assessments, understand the tools available for security testing and how to design and conduct effective security tests. In this presentation, ASTQB board member Randall Rice, leader of the ISTQB Working Party that developed the syllabus, will present: An overview of the ISTQB Advanced Security Tester syllabus topics; How the certification works; How this certification differs from other security certifications; How the certification builds upon work done in other organizations, such as NIST, CERT and OWASP; The intended audience for the training and certification; and, The value of the ISTQB Advanced Security Tester certifications to testers and to organizations.

Challenges and Opportunities of Autonomy Vulnerability T&E

By Mr. Don Strausberger - Georgia Tech Research Institute

Test and Evaluation (T&E) of Autonomous Systems: Challenges and Opportunities of Autonomy Vulnerability T&E
This presentation explores the need for, and challenges with the T&E of vulnerability of autonomous cyber-physical systems. Today's warfighter system evaluation includes well established vulnerability assessment domains and T&E techniques for the hardware, sensors (i.e. optical, RF, etc.), communications/networks, and software (cyber). Autonomous systems will span and require these established vulnerability assessment domains to be addressed, but also introduce new, increasingly nefarious, and potentially more impactful avenues for exploitation than the highly complex (but automated) cyber-physical systems of today. This is a result of autonomy's perception, comprehension, and projection components potential vulnerability to being deceived, mislead, and exploited which will negatively impact decision-making. Perception, comprehension, and projection constitute new attack surfaces that are distinctly different from existing sensor and cyber-attack surfaces. While vulnerability T&E of sensors (Electronic Protection, etc.) is well established, and vulnerability T&E of cyber-physical systems is maturing, neither of these vulnerability T&E disciplines (and their according T&E infrastructure) address this need. The resulting T&E gap results in unmitigated risk management of the vulnerability and potential exploitation of the autonomous behaviors which will prevent its operational deployment. Understanding and evaluating newly introduced vulnerabilities of increasingly autonomous cyber-physical systems constitutes a fundamental and unique challenge that must be addressed by test and evaluation.

Covering Arrays: Evaluating Coverage and Diversity in the Presence of Disallowed Combinations

By Mr. Thomas A. Donnelly, PhD, CAP - SAS Institute Inc.

Test engineers are often faced with the challenge of selecting test cases that maximize the chance of discovering faults while working with a limited budget. Combinatorial testing is an effective test case selection strategy to address this challenge. The basic idea is to select test cases that ensure that all possible combinations of settings from two (or more) inputs are accounted for, regardless of which subset of two (or more) inputs are selected. Currently, combinatorial testing usually implies a covering array as the underlying mathematical construct. Amongst the challenges that practitioners sometimes encounter is: a) The challenge of accommodating constraints on allowed combinations of settings for some subset of inputs [1] when specifying the covering array to be used for combinatorial testing. b) The challenge of assessing the coverage and diversity properties [2] of the resulting covering array. In this talk we will address both of these challenges, but we will focus on a particular subclass of constraints, namely "disallowed combinations". We will motivate the discussion by working through a case study and, in the process, we will propose a new class of covering arrays, that we will refer to as "unsatisfiable constrained covering arrays", as well as extensions to the metrics proposed in [2] to accommodate this new class of covering arrays. References 1. Cohen, M., Dwyer, M., & Shi, J., "Constructing interaction test suites for highly-configurable systems in the presence of constraints: A greedy approach," IEEE Transactions on Software Engineering, 34(5), 2008, pp. 633-650. 2. Dalal, S., & Mallows, C., "Factor-covering designs for testing software," Technometrics, 40(3), 1998, pp. 234-243.

Cyber Requirements Engineering

By Mr. Al Morris - PeopleTec

Everyone has heard about protecting the Confidentiality, Integrity and Availability for information being processed by a system or application. What capabilities are really needed, and what information is important to being protected? Prevent, Mitigate and Recover from cybersecurity incidents are the primary goals of cybersecurity control applied to systems and applications in varying degrees of strictness that may or may not be appropriate for everyone. The primary goals of cybersecurity controls have implied secondary goals that cannot be overlooked. I.E. you can't recover from a cybersecurity incident if you can't detect one. What speed and level of recovery is required for a system or application will depend on the function is provides. If it's something like a medical device, an automobile, or aircraft that could affect someone's life, limb or eyesight both factors will be different than something that provides supply or logistics data. What may be more important to a system or application processing that data may be just the Integrity, in which case you want to Prevent data from being manipulated by authenticating the source and destination, and/or encrypting the data at rest and in transit which would fulfill the protection of the Confidentiality and Integrity of the information. Only if the data was required to perform a critical function of the system or application would you need to be concerned with the Availability.

If the data supports a critical function of a system or application that could affect someone's life, limb or eyesight additional design consideration need to be made. Is the function critical enough that it would require hardware redundancy, or to the extreme of supplier diversity and redundancy to prevent a hardware or embedded software cybersecurity incident from affecting the critical functions? This criticality analysis effort could lead to further Supply Chain Risk Management and Software and Firmware Assurance design, contracting and testing requirements. Where a firmware and hardware company may be contracted separately to provide a function that will be integrated by a more trusted supplier as an additional contract action. System of System design considerations and requirements need to be developed with the highest level of assembly in mind. A low likelihood, low impact, low probability vulnerability in one non-critical component of a system or application can be exploited and bring down critical functions if systems are designed and thrown together in stove pipes that will be tested only when the entire project is complete. All these functions, protections and requirements can substantially drive the cost of the development of an application or system. Cybersecurity? Safety? Airworthiness? DO-178? FACE? VICTORY. Some cost savings can be realized by crossing these related disciplines and designing out requirements that overlap in the contracts. Changes in DoD Acquisition and DoD Agency regulations are pushing ultimate responsibility down to the Project Officer level. Changes to DFARS regulations are supporting the Project Offices in leveraging requirements that ensure vendors of all hardware and software at all levels are performing their due diligence.

Cyber Security Test and Methodologies for Improving Mission Cyber Resiliency

By Mr. Daniel Nguyen, Mr. Ralph Galetti, and Mr. Adonis Williams - Boeing Test and Evaluation

Evaluating a system's cyber resiliency is typically an unstructured and ad-hoc T&E activity. Compounding the problem, ever-increasing system functionality, connectivity, and a growing list of potential cyber security threats significantly and dynamically alter the cyber-attack surface throughout a system's development lifecycle. To address these gaps and the unique challenges in cyber security testing, the specialized capability of Cyber Test and Evaluation (CT&E) has evolved from the broad foundation of T&E discipline. The CT&E framework is designed to enhance the cybersecurity posture of test platforms by focusing on threat scenarios that are critical to mission success. The methodology is platform agnostic and provides a repeatable process to inform and improve the overall cyber resilience of a system or a system of systems. This paper introduces a CT&E lifecycle solution and its application across a typical system development environment.

Cyber T&E of Weapon Platforms and Systems

By Mr. Ronald J. Prado - Georgia Tech Research Institute

It's been three years since release of the Cyber T&E Guidebook and two years since NDAA Section 1647 mandated cyber vulnerability evaluations of weapon systems. In that time, all services of the DoD have been methodically working through what that means for a weapons platform (as compared to an IT system) and have started the process of evaluation on their weapon platforms and subsystems. However, there are a large number of platforms that need to be evaluated, limited resources to test them, debate on what constitutes a comprehensive evaluation, and questions on if an evaluation is ever really complete (e.g., there are many subsystems to consider and there are always system updates in play). This presentation will explore these issues. Amongst the DoD services, there are varying methodologies that have been established to formally address cyber T&E of their platforms. They have attempted to work within their timing and funding constraints by prioritizing platform evaluations and by limiting the scope of the evaluations, at least initially, until long-term initiatives, methodologies, and processes can be matured. Based on recent DoD service initiatives to provide long-term methodologies and recent weapon system and subsystem assessment efforts, we will explore the issues and suggested strategies to provide a robust and efficient cyber T&E process. We will also discuss current capability needs and lessons learned that could be applied to the process.

Cybersecurity: From Test & Evaluation to Requirements

By Lok Yan, PhD - Air Force Research Laboratory, Information Directorate

The systems development lifecycle is often presented as a circle with one-directional arrows in between the Requirements, Design, Implementation, Test & Evaluation, Deployment, Maintenance, and Disposal lifecycle stages. This depicts a serial nature of systems development where there are "gates" through which the system passes from one stage to the next. This is inherently incompatible with Cybersecurity. The same is true for the V model of systems development or any other staged model. Fundamentally, the serial nature of these models assumes that, by the time we get to Testing, all the Requirements are well defined so that we can test against them. In Cyber, this steady state might not be achievable since new vulnerabilities and attack vectors are discovered constantly. In this talk, we will present two different approaches to tackle this problem. First, we will present the idea of Continuous Integration (CI) which shrinks the lifecycle down to such a small timeframe (e.g., 24 hours) that it is possible to get ahead of newly discovered Cybersecurity concerns. Since CI is incompatible with the Acquisitions process, we seek to achieve the same goals -- a drastically shortened lifecycle -- by ensuring that systems are architected with the ability to quickly adapt to new requirements or design changes. While this has traditionally been a problem beyond the Test and Evaluation community, we argue that this is precisely a problem for the T&E community. All requirements must be testable, and what will be tested will become a requirement. Our second approach is to suggest that the T&E community establish a set of lifecycle agility tests and use these to drive acquisitions culture to become more compatible with modern Cybersecurity concerns. Netflix has used their Simian Army (Chaos Monkey) to completely change the way that their engineers think about robustness and fault tolerance, and the same can happen for the greater concerns of Cybersecurity.

Cybersecurity Policy and Resiliency

By Mr. Edward A. Adkins - Defense Acquisition University (DAU)

The DAU presentation, entitled “Cybersecurity Policy and Resiliency,” will focus on the various cybersecurity requirements found in in DODI 8500.01, 8510.01 and 5000.02. The presentation will highlight the critical responsibilities of DoD acquisition program managers (PMs), testers and engineers. The presentation will also highlight the major revision in DODI 5000.02 regarding the threat process and threat products. PMs, testers and engineers must understand how this process has changed so they can work effectively with the Intelligence community to obtain and understand threats to our acquisition systems. Finally, the presentation will address the topic of resiliency and how this term is defined in DoD policy. The Test Community must realize this critical and misunderstood aspect of cybersecurity is a future game changing requirement for all acquisition programs and test ranges.

Cybersecurity Vs Cyber Survivability: Implementing a Paradigm Shift in T&E

By Mr. Michael Landolt - Army Test and Evaluation Command

Cybersecurity and cyber survivability are similar but not the same. “Cybersecurity” focuses more on hardening a system to prevent a cyber-attack whereas “cyber survivability” emphasizes how well a unit equipped with that system can continue to operate through a cyber-attack to complete its mission. Talking about system “cybersecurity” can be misleading because some may see it as a characteristic that said system either does or does not obtain. In the extreme, decision makers may unwisely accept the operational risks of systems with substantial cyber vulnerabilities because they have resigned themselves to the false opinion that “cybersecurity” for any weapon system is not achievable. DOT&E uses the term “operational test and evaluation of cybersecurity” to describe T&E that aims to discover how secure a system is and to characterize potential mission impacts of any discovered vulnerabilities. If the point of operational test and evaluation is to characterize the effectiveness, suitability, and survivability of a system when employed by our military; then the T&E community may wish to stop using the term “cybersecurity” when what we really wish to know about is “cyber survivability.” This presentation will explore if we are currently asking the right questions when evaluating systems against threats in the cyber domain. It will also suggest the dangers in continuing to evaluate system cybersecurity vice system cyber survivability. The discussion involves how using the term “cybersecurity” may unintentionally inflate the importance of protecting a system when the threat is always changing and at least one step ahead of defenders. Also included in the discussion are more operationally relevant Critical Operational Issues and Criteria that ATEC has been championing to the user community and how the new JROC System Survivability KPP Cyber Endorsement describes requirements that entail more than just cybersecurity. Overall this presentation will attempt to convince the T&E community to stop using the term “cybersecurity” when we really mean “cyber survivability.”

Defining Resiliency

By Ms. Sarah Pramanik - Northrop Grumman

Designing, implementing and testing for resiliency can be a daunting task when resiliency is vaguely defined. In order for a system to be resilient, it must be resilient against a specific objective, and not just blanket “resilient.” As with all good requirements, it must be understandable, discrete, and verifiable. This presentation will endeavor to provide concrete solutions for defining resiliency in a way that a system can be designed, implemented and tested.

Hardware Assurance Lifecycle Ecosystem: "Distributed Transition Environment"

By Matthew Casto, PhD - Air Force Research Laboratory, Sensors Directorate, Trusted Electronics Branch

Hardware Exploits: Can You Trust Your Devices?

By Ms. Christina Witt, CISSP, CAP - JT3

Do you know where the components of your systems come from? Do you send malfunctioning IT devices back to the vendor for maintenance and repairs? Do you know where the vendors send your equipment for repairs? Hardware hacks are impossible to detect and can gather information and infiltrate systems without the users knowing about it. This talk discusses how those vulnerabilities can enter into any information system from the beginning stages of acquisition: Development, creation at a foundry, programming at the vendor, and even during shipment. Some work arounds are costly but being aware can open discussions to help resolve hardware exploits and ensure DoD systems remain controlled and secured.

Hardware for Cyber (H4C): A Suite of Electronic System Protections from Nano to System Levels

Domenic Forte, PhD - University of Florida

Reverse engineering of electronic systems has been performed for many different reasons, some of which are ethical and others that are harmful. The former includes failure analysis and fault isolation, obsolescence mitigation, proof of IP rights infringement, and security assurance while the latter includes identification of exploits, development of attacks, IP theft, and counterfeiting. This presentation shall discuss (1) recent advances in automation and accuracy of integrated circuit (IC), printed circuit board (PCB), and firmware reverse engineering; (2) the positive and negative impacts of these advances; (3) a suite of solutions being developed at multiple levels of abstraction (device, chip, and PCB) to combat reverse engineering and counterfeiting threats for the most sensitive military IP and electronics; and (4) future research challenges and tasks.

Identifying Requirements and Vulnerabilities for Cybersecurity; Or How I Learned to Stop Worrying and Love the Six-Phase Cybersecurity T&E Process

By CAPT Michael Lilienthal, PhD (USN Ret), Director of Navy and Cyber Programs, EWA

Many Service acquisition and Test and Evaluation (T&E) programs find it difficult and confusing to negotiate the policies and processes to develop their requirements and strategy for cybersecurity T&E. The Cyber Operational Vulnerability Assessment (COVA) is one way to identify credible vulnerabilities and develop actionable requirements that can be used to design efficient T&E. The COVA was developed and implemented by Electronic Warfare Associates Inc, (EWA) as a joint effort by industry partners within the Cybersecurity community and is a structured, mission-based approach to analyzing the risk of cyber threat vulnerabilities. It is a scalable and interactive event designed using the foundation of the highly successful Cyber Table Top Wargame, also spearheaded by EWA. The COVA which also incorporates the important aspects of Electronic Warfare and Electronic Attack, is intended as an aid in developing and understanding cybersecurity requirements, as well as identifying vulnerabilities and adversarial capabilities. This information can then be used to develop and/or refine a strategy and plan for cybersecurity T&E. In short, this presentation will introduce the COVA as a low-cost and proven method to start planning for, or to update, a strategy for cybersecurity T&E. This presentation will present attendees with an detailed overview of the COVA process and methodologies, as well as highlight successful uses. Who should attend this presentation It is intended for use by Acquisition Program Management Offices, Chief Developmental Testers, and Lead Developmental Test and Evaluation (DT&E) Organizations. But anyone in the Acquisition or T&E who is tasked with planning or executing Cybersecurity T&E will benefit.

Institutionalizing a Proactive Cybersecurity Posture

By Mr. Gregory Jaeger - ATI

Like a well-tuned machine or electronic circuit, an integrated Development and Operations Team invokes triggers and feedback loops that forewarn of anomalous system behavior that facilitates preemptive cyber defense actions. Cross-domain collaboration enables Operations roles to improve software assurance and Development roles to advance cyber resilience. The techniques required to combine and develop the workforce involve common sense leadership and fit within current budgets. This presentation explores how a cyber-event led to the development and implementation of a methodology to shift to a proactive cybersecurity posture on a fixed-price contract without additional tools, data or personnel. The transformation applied incremental changes in Team roles, relationships, and activities based on the tenets: 1) cybersecurity is a core requirement; 2) system awareness is the high ground; 3) cyber subject matter expertise is resident in development and operations; and 4) combined perspectives magnify intelligence. The approach institutionalized cybersecurity awareness such that the Team successfully detected and thwarted in hours, the same Struts cyberattack that Equifax failed to notice for more than two months. This methodology matured the existing workforce with requisite system knowledge into a high-performance cybersecurity team that produced measurable cyber risks and strengthened management confidence in making smarter, risk-based decisions.

Lessons Learned and Recommendations for conducting a Cyber Table Top in T&E

By Mr. Tristan Gilbert - WSMR

This presentation is intended to provide Cybersecurity personnel with information about the Cyber Table Top exercise. The information presented here was gathered from a recent exercise and covers suggestions and information with the intent to assist others with conducting their own exercise. The brief will highlight key areas that presented challenges to conducting the exercise along with approaches and recommendations for overcoming them. Information and opinions are presented on scoping, rules of engagement, identification of critical cyber domain, building teams for success, suggested approach for actual execution, and thoughts on how to structure Red Team mission goals and attacks. Additional information is presented on how to structure results and generate a data centric course of action and recommendations to senior leaders. Lessons learned will be shared with insight provided into several intangible benefits of the Cyber Table Top exercise.

Leveraging Machine-assisted Technologies for Platform Security Assessments

By Mr. Elbert Michael Ruiz - Georgia Tech Research Institute

Cyber-Physical Systems (CPS) are loosely defined as an integration of computation, networking, and physical processes working concurrently for a specified high-level function or goal. From a vulnerability perspective, the merging of computational, networking, and physical domains necessarily entails the merging of their respective susceptibility to classes of vulnerabilities. The close coupling between cyber and physical assets can lead to a unique class of hybrid cyber-physical vulnerabilities which can compromise system operations by affecting fundamental CPS properties of correctness and timeliness, leading to catastrophic consequences. Exploring the susceptibility of Cyber-Physical Systems to a multitude of threats and attacks has promoted extremely fertile long-term research areas which can be extended to Weapons Systems, culminating is DoD directives aimed specifically at assessing and addressing the Cyber threats associated with these platforms. The implementation timelines of these directives have not come without consequences however. Many DoD Test and Evaluation groups assigned with the task of assessing their Weapons Systems have a major issue with the sheer quantity of platforms requiring testing coupled with compressed timelines for completing these assessments. Therefore, the primary motivating question we should be asking ourselves is, how can we improve the speed and effectiveness of the cyber vulnerability assessment process? We know that skilled humans are excellent at providing deep insight and drilling deep to uncover specific fundamental vulnerabilities, however this manual analysis is time consuming and expensive. At the other end of the spectrum, many recent research approaches have concentrated on methods of full automation for specific analysis techniques. But even with intelligent approaches, often automatic testing can only generally uncover shallow bugs, or cannot provide adequate coverage due to the full potential solution space proving to be intractable for fully-automated analysis. We believe that by combining the two approaches (e.g. augmenting human intelligence with machine analysis) we can provide a disruptive and highly efficient solution to the issue of scalability and effectiveness of assessments. This talk will focus on the development of some of these hybrid approaches, where we leverage machine-assisted technologies to aide security analysis practitioners identify and focus on high-impact areas of interest.

Leveraging Secure Systems Analysis to Generate Testable Cyber Security Requirements

By Col William E. Young, Jr., PhD (USAF) - Commander, 53d Electronic Warfare Group

Generating testable requirements is clearly one of the most important tasks in systems engineering. System Analysis has long served as the foundation for requirement elicitation, validation, and verification. This presentation explains why a new variant of systems analysis called secure systems analysis holds the key to generating testable cyber security requirements. These requirements are developed not on the basis of the particular technology, but rather in response to the "security problem" stakeholders define. Stakeholders can define the security problem in a wide variety of ways. Examples include assuring target data processing functions, data storage functions, control functions for critical systems, or even the network's connectivity functions themselves. In each case the security problem is expressed in functional terms rather than in terms of a specific security solution. By expressing security in system engineering functional terms, the cyber security challenge can have addressed in the same way that other emergent system properties are addressed. The cyber security requirements become performance based, functional specifications, rather than checklists. The presentation presents a new secure systems analysis methodology called System-Theoretic Process Analysis for Security (STPA-Sec). The technique extends Leveson's System-Theoretic Process Analysis (STPA) safety hazard analysis technique to address security and mission assurance needs from a systems perspective. STPA-Sec applies a system engineering framework to allow engineers to better balance the requirements for desired functionality with the requirement to control undesired functionality (system misbehavior). STPA-Sec augments traditional security approaches by introducing a top-down analysis process designed to help a multidisciplinary team consisting of security, operations, and domain experts identify and constrain the system from entering unsecure states that lead to losses. This new framework shifts the focus of the security analysis away from threats as the proximate cause of losses and focuses instead on the broader system structure that allowed the system to enter an exploitable state. STPA-Sec is being applied in successfully in several industries to generate testable cybersecurity requirements. A military variant of STPA-Sec called Functional Mission Analysis for Cyber (FMA-C) is currently taught by the USAF Cyber College to all USAF Mission Defense Team pathfinders and will soon be taught internationally by Cyber College mobile education teams.

Next Generation Cyber Test

by Mr. Steven Newton, 47th Cyberspace Test Squadron

Quantifiable Cybersecurity Risk Assessments of Weapon Systems during Developmental Test

By Mr. Steve Klynsma - The MITRE Corporation

Cybersecurity risk has traditionally been presented within qualitative risk matrices. Unfortunately, there is little evidence that risk matrices are helpful to inform decision makers, except at the highest abstract level. We propose replacing the risk matrix used often in Development Testing (DT) with quantitative probabilistic methods as espoused by Hubbard and Seiersen in their book "How to Measure Anything in Cybersecurity Risk". We propose to apply their methods during the Engineering and Material Development (EMD) cycle of the acquisition process for weapon systems. To do so, vulnerabilities identified during DT cybersecurity testing are analyzed (within a 90% confidence interval) for likelihood frequency and impact within an operational mission context. Impact is measured and modeled against an appropriate operational impact metric e.g. mission readiness (availability) for the weapon system under assessment. Using Monte Carlo analysis, a residual risk curve is generated which may then be superimposed on a risk tolerance curve defined earlier by the unit commander or the requirements developer. Vulnerabilities which push the potential impact above the user's risk tolerance must be mitigated or remediated. Further "What if" scenarios may also be run against the model to inform the system developer of fixes to prioritize. Goal would be to lower the Residual risk curve completely under the Risk Tolerance curve. This may not be possible but at a minimum, the model would provide a quantifiable operational benefit to mitigating vulnerabilities.

Reversing Cyber Risk Assessments for High-Value Returns

By Brian Mork, PhD - AFRL / XPZ

There are multiple cyber assessment methods available for use by the military acquisition community. Twenty methods were recently surveyed by DASD(DT&E). The Cyber Table Top mission-based cyber risk assessment promoted by DASD is similar to a method prior published by the Air Force Research Lab Information Directorate (AFRL/RI), which has been adopted by the Air Force Operational Test & Evaluation command (AFOTEC) to satisfy their mission to "test and evaluate new capabilities in operationally realistic environments to inform warfighters and influence national resource decisions." These methods capture pieces of the 2015 DoD Cybersecurity T&E Guidebook which emphasizes cooperative vulnerability assessment before adversarial testing. The AFRL/RI method uses Blue Teams with mission knowledge and engineering documentation to discover and publish weapon system vulnerabilities. These vulnerabilities are optionally tested and validated by Red Teams with cyber expertise. Doing adversarial testing and discovery efforts earlier may be more appropriate for the task at hand ("inform warfighters and influence national acquisition decisions") and, in addition, deliver more high-value payoff to engineering teams and program managers so we can design cyber into systems rather than patch unplanned behavior later. It would be better if the Aggressor Team efforts occurred first, followed by contributions from the Blue Teams. This proposal is complicated by challenges of program schedule/cost and skill sets of test/experimentation teams.

Self-Cleansing Intrusion Tolerance (SCIT): A New Approach to Reduce the Impact of Data Breeches

By Arun Sood, PhD, Prof Computer Science and Director International Cyber Center, and Founder and CEO - George Mason University and SCIT Labs

Cybersecurity has become a persistent concern and a complex problem that is often oversimplified and misunderstood. The cyber threat landscape is multidimensional and subject to evolving threats by a variety of actors with sophisticated hacking tools. There are many technologies and protocols to help mitigate cyber threats, but there is really no panacea. Relying only on detection can give a false sense of security. A comprehensive strategy of risk management is the best cyber defense. In short, relying on the detection-only approach is fighting yesterday's war, while the threat landscape continues to rapidly evolve into more sophisticated and more lethal threats. It is time to accept that some level of intrusion is inevitable, hackers will get in past detection systems in a variety of ways. Once a system is hacked, the intruder can use the access to gain varying degrees of command and control causing extensive damage including theft of data and intellectual property. In widely reported breaches, intruders installed infections that stayed inside the system undetected for months. If you are willing to accept the inevitability of intrusion, the goal is to no longer rely only on the hope of eliminating vulnerabilities and detecting intrusions. An innovative solution to mitigate the potential damage caused by intrusion is Self-Cleansing Intrusion Tolerance (SCIT). SCIT employs a server farm using virtualization technology with multiple copies of the pristine uncontaminated server. But only a few selected servers are active or "hot" at any one time for receiving connections or servicing the client. The others are "cold" and not accessible to the users. Every 60 seconds or less (based on your requirements), these servers are rotated from cold to hot state and during the cold state, the server is rebuilt to the pristine configuration. Any intrusion or infection that took place 60 seconds ago is completely wiped out. So, if a hacker had defaced a website hosted on a server that is now back to its original pristine condition, that intruder would now need to re-hack into that system. In addition to the difficulties in re-entering, it is possible that in those 60 seconds, our hacker did not have enough time to gain full access to the site. The server becomes a moving target because it rotates out of the "line of cyber fire" to be rebuilt while another unhacked virtualization takes its place. The infected server can be rotated to quarantine where the infection can be analyzed in a systematic and timely manner without impacting the overall performance of the system. Such an analysis can provide information on the infection, how it was introduced, how it gained control and more, all of which can be leveraged for the development of preventive techniques. In summary, SCIT is a new capability for industry, government, and other institutions to reduce or potentially eliminate costly data and intellectual property breaches in almost real time.

SHIFT LEFT: Army T&E Efforts to Address Cybersecurity Earlier in the Acquisition Cycle

By Mr. Patrick Thompson and LTC Michael Burns - U.S. Army Evaluation Center

Cybersecurity has received significant interest in the recent years. Interest in improving the robustness and resilience of both enterprise and tactical networks has increased with each reported network breach and will continue to increase until our systems provide a more protected terrain on which we engage our adversaries. Most recently, the National Defense Authorization Act of 2017, Section 1647, addressed the cybersecurity posture of systems. Prior to this, the recently updated Department of Defense Instruction 5000.02 "Operation of the Defense Acquisition System" and the Army Regulation 73-1 "Test and Evaluation Policy" addressed the need to establish efforts earlier in the acquisition cycle, commonly referred to as Shift Left, to test-fix-test cybersecurity into networks and networked systems prior to fielding. Although the concept of Shift Left is becoming more frequently used in acquisition discussions, the actual implementation is not defined. This paper presents a hypothetical construct for a Shift Left effort that addresses cybersecurity from program inception. Although hypothetical, it provides an approach that the author suggests is a viable one to build cybersecurity into systems during development rather than investigate, often costlier, means to mitigate issues after a finalized design and material investment in hardware.

Stop Looking Under the (Cyber) Lamp-Post

By Mr. Arch Owen, Mr. Mike Aucoin, Mr. Neil Brock - Draper

The current approach to design and testing of cyber-physical weapon system security "looks under the lamp-post" and not "in the dark" (to paraphrase the story of the man looking for his keys at night only under lamp-posts). I.e. design and testing of system security only looks for, and eliminates, known vulnerabilities. There are no mature, general purpose tools or methods that systematically identify and prevent unknown vulnerabilities. With the cyber-warfare domain becoming more and more central to modern warfare, we cannot afford to only prevent know vulnerabilities. We need to shift our thinking, and our design/test capabilities, to identify and prevent previously unknown vulnerabilities in our weapon systems. This paper will give a perspective of this challenge, discussing three capabilities under development, which can shift this paradigm so that we start to prevent vulnerabilities from ever getting into the weapons systems in the first place. The first is a Machine Learning approach to identity unknown Software vulnerabilities. The second is a Formal Methods approach to identify possible side channel attacks (e.g. Denial of Service via resource loading). The third is a Formal Methods approach to assess whether software, or even specifications, can exhibit specific vulnerabilities (i.e. can a program ever make a launch decision using data from an unsecure source). These three examples show promise for eliminating previously unknown vulnerabilities resulting from coding errors, or even from early stage specifications.

System of Systems in a Cyber Range Environment

By Mr. Roderick Hallum - Scientific Research Corporation

Joint Staff (JS) J6, JS J7, DISA and TRMC are anchoring a collaborative Team of DoD organizations and agencies to provide: (1) Commanders a tool for identifying, assessing, and addressing C4/Cyber readiness; (2) Cyber forces with an operationally realistic, robust training environment capable of supporting the full range of cyber capabilities; and (3) C4/Cyber Program Managers and testers with an environment in which to assess and test vulnerabilities, interoperability, integration and the cyber survivability of the Joint Information Environment (JIE). The Team has successfully established the DoD Enterprise Cyberspace Range Environment (DECRE) Command and Control Information Systems (C2IS) to provide robust, secure, and operationally realistic support to the development, assessment, testing and training of C4/Cyberspace capabilities. Participants include the four designated cyber ranges; J7 Joint Information Operations range, Norfolk VA; J6 C5 Assessment Division, Suffolk VA; Test Resource Management Center's National Cyber Range Complex, Orlando FL; Defense Information Systems Agency's Cyber Security Range, Stafford VA. Each partnering organization has a robust capability unto itself and when integrated, they created a C2 environment, which in the words of the aggressing Red Teams and Blue Teams "looked and felt like a real combatant command network." Other critical participants include the Navy's Combat Direction System activity, the Air Force's 46Th Test Squadron, JAMETIC and Red Teams from across the Services. Training audiences from USPACOM, TRANSCOM and Australia have participated in the 28 two to three-week events that have occurred over the last four years. In preparation for USPACOM's FY17 Talisman Saber (TS) exercises, USPACOM used the environment to train US and Australian Defensive Cyberspace Operations teams to counter an advanced coalition cyber opposing force (OPFOR). This effort supports the DoD Cyber Strategy "defense of key terrain-cyber (KT-C) and enables Defensive Cyberspace Operations teams' the ability to plan and operate within a degraded and disrupted environment and the opportunity to defend key cyber terrain against advanced cyber threat vectors in a closed, realistic environment. This environment currently represents a joint combatant command's JIE installation with C2 enclaves representing the Joint Operations Center (JOC) and Air Operations Center (AOC) each in a separate Base/Post/Camp/Station interconnected by the Department of Defense Information Network (DoDIN). DECRE C2IS is uniquely constructed to provide the operationally realistic, closed environment needed for the development, assessment, test and training of C4/Cyberspace capabilities…the quantifiable measurement of: (1) cyber threats; (2) effectiveness of cyber detection and prevention tools; (3) cyber effects on blue force mission and C4I mission capabilities; and (4) effectiveness of blue force cyber response actions in operationally realistic environments. This presentation will focus on the various components, processes and lesson learned in building the DECRE C2IS environment and its ability to support the development, assessment and testing of C5 systems.

TENA and JMETC for Distributed and Cyber Test and Training

By Mr. Gene Hudgins – KBRWyle and Mr. Robin Deiulio – TENA/JMETC

The TRMC was appointed an Authorizing Official (AO) on 31 March 2016. TRMC has setup an overarching Cybersecurity Program for TRMC owned systems under the purview of the TRMC AO. We are working overarching policy and procedures for future TRMC Cybersecurity Projects specifically for the Research, Development, and Test Communities. TRMC Cybersecurity is currently working through the software assurance process to take together Software Products through the Risk Management Framework Assessment Only process. This briefing will address the current impact of the TRMC Cybersecurity organization on current systems and software products as well as how this will significantly impact our customers at other DoD agencies in the Test and Development community.

Together, TENA and JMETC enable interoperability among ranges, facilities, and simulations in a timely and cost-efficient manner. TENA provides for real-time system interoperability, as well as interfacing existing range assets, C4ISR systems, and simulations; fostering reuse of range assets and future software systems. JMETC is a distributed, LVC capability which uses a hybrid network architecture; the JMETC Secret Network (JSN), based on the SDREN, is used for secret testing and the JMETC Multiple Independent Levels of Security (MILS) Network (JMN) is the T&E enterprise network solution for all classifications and for cyber testing. JMETC provides readily available connectivity to the Services' distributed test and training capabilities and simulations, as well as industry resources. This tutorial will address the current impact of TENA and JMETC on distributed systems engineering as well as their significance to the cyber Test and Training community.

Test Case Design via Model Based Systems Engineering

By Mr. Marshall Bronston - Georgia Tech Research Institute

This presentation will describe an approach to ensure test and evaluation activities are sufficiently robust to support the complexity typical to what is found in testing related to cyber security. Model-Based Systems Engineering (MBSE) provides a rigorous structure in system development which can be applied to cyber-related systems. A systematic application of the 4 basic MBSE views (structure, requirements, behavior, and parametric) permits a disciplined manner to allocate data collection opportunities in a test campaign. Test events can by scoped to take advantage of a broad range of scenarios, constrained red force activities, instrumentation capabilities, and test objectives to efficiently develop results, conclusions, and recommendations. These findings can also be applied to create a holistic view of the confidence a decision-maker can have with T&E outcomes. This presentation will take a notional tactical airborne networking example as a "prop" to develop concepts underpinning MBSE use to create a robust test program. It will leverage lessons from research, developmental, and operational test community efforts to provide answers with justifiable confidence. The presentation will address: MBSE in a Systems Modeling Language context; Cyber security T&E; Application of MBSE to generate useful and appropriate test cases; and, Use of MBSE and its inherent automation to provide linkages and traceability between mission needs, requirements, design, and test activities. A viewer show expects to obtain familiarization with MBSE applied to cyber security T&E in a manner that promotes both curiosity and a desire to provide rigor and discipline to all T&E activities using best practices.

The Test Resource Management Center's Vision for Developing Cyber Test Range Capabilities

By Mr. Bernard B. (Chip) Ferguson - Test Resource Management Center

Mr. Bernard B. (Chip) Ferguson, the Deputy Executive Agent (EA) for Cyber Test Ranges, proposes to present a plenary session briefing on the Test Resource Management Center (TRMC) Cyber T&E Infrastructure (CT&EI) vision for providing the test and evaluation community and the Department of Defense an infrastructure built of cyber test capabilities that enable secure, affordable, readily accessible, operationally realistic cyber range environments. These ranges and environments will be suitable for realistic cyber testing of information technology systems; weapon systems; command, control, communications, computers intelligence, surveillance, and reconnaissance systems; and other network systems. In addition, they will also be suitable for training and sustaining our cyber mission forces.

To provide realistic battlefield environments to test weapon and C4ISR systems, the TRMC foresees the need to integrate the National Cyber Range (NCR) Complex, Designated Ranges, and Service-owned ranges with live, virtual, and constructive (LVC) representations of these systems. The current and proposed cyber ranges have the capability to emulate blue (friendly), red (threat), and gray (Internet) networks, along with other virtualized systems and components. Weapon and C4I systems are available in existing simulators, hardware in the loop (HWIL) facilities, system integration labs (SILs), and installed system test facilities (ISTFs). Interconnected, these cyber range and LVC capabilities have the potential to form the CT&EI. Mr. Ferguson will introduce the CT&EI concept and timeline. In addition, the brief will highlight how TRMC is expanding the current capability of the NCR to five interconnected cyber ranges to create the NCR Complex. Mr. Ferguson will also discuss TRMC's vision to leverage the currently fielded capabilities to build additional cyber range capacity as quickly and efficiently as possible. The brief will address the following three areas of investment: (1) connectivity and integration; (2) cyber test asset protection; and (3) weapon system/component emulation. TRMCs goal is to quickly integrate current cyber T&E assets and capabilities with assets and capabilities that may not have been traditionally used for cyber T&E.

Trusted and Assured Microelectronics Hardware Assurance Evaluation and Test Capabilities

By Mr. Jeremy Muldavin, PhD - ODASD(SE)

The Office of the Deputy Assistant Secretary of Defense for Systems Engineering launched an initiative in Fiscal Year (FY) 2017 in support of trusted and assured access to advanced semiconductor technology for the Department of Defense (DoD) as well as the broader United States Government. The initiative has three main elements: (1) development of an alternate trusted photomask capability to preserve long-term trusted access and protection of Intellectual Property, (2) enhanced verification and validation activities at key government laboratories and the promotion of industry best practices and commercial standards in the areas of microelectronics trust and assurance, and (3) the development and transition of technologies in support of a new trust and assurance approach. In recognition of critical near-term needs, the DoD requested additional funding in FY 2018 to address gaps in availability, access, and assurance including an initial investment in next generation disruptive microelectronics research and development to maintain U.S. technological edge in critical technology and the marketplace. This presentation will describe these efforts and discuss their status and the overarching management approach.

Using Modern SE Methods for Cyber Design & Test

By Mr. Frank C Alvidrez - Spectrum Inc

Modern military and civilian systems of systems, have seen a great increase recently in Cybersecurity vulnerability. This increase, threatens infrastructure, safety, compromises security, causes damage to internal and external information systems, can have considerable cost impact including direct loss of critical funds as well as intellectual property. The damage that these data breaches can be severe and have cascading effects to the normal operations of military and civilian systems. In response to this vile threat, the US Government and civilian entities have responded with new defensive processes and software to combat cyber threats. To be more successful, a modern systems approach must be employed throughout the enterprise and throughout the lifecycle of vulnerable systems. Cyber resiliency must be inherent in the design and enterprise processes. It is much more efficient to stop the cyber threat early and to try to pick up the pieces after a serious breach. Cybersecurity is now becoming a fundamental part of the system engineering process and should be incorporated through all phases of the life-cycle process. This paper will examine using advanced system engineering methods, such as Model Based System Engineering (MBSE), to encapsulate cybersecurity governance, defining cyber requirements, examine some examples of cyber resilient design and highlight the testing and monitoring of modern enterprise systems using the MagicDraw UML tool set with SysML and DoDAF profiles.

SPEAKER BIOGRAPHIES

Mr. Edward (Ed) Adkins is a Defense Acquisition University (DAU) Civil Service Professor of Engineering, Test and Cybersecurity at Eglin AFB FL. Ed joined DAU in 2009 and has taught 5000 classroom hours for DoD Test & Evaluation (T&E) and engineering personnel to obtain level II/III T&E and engineering certifications. He has provided DAU consulting support to the Army, Navy, Air Force (AF) and Marine Corps. Ed has supported programs such as: Joint Light Tactical Vehicle, Littoral Combat Ship, F-35, Small Diameter Bomb II and Long-Range Stand-Off. He currently works closely with the AF Authorizing Official for Weapons and delivers cybersecurity training/workshops to DoD program offices and test organizations. Ed graduated from Virginia Military Institute in 1984. His first AF assignment was as a T&E Manager at Wright-Patterson AFB OH. He served as an AF engineer at General Electric Aircraft Engines and then as an instructor for engineering/T&E at the AF Systems Acquisition School. He was assigned as Program Manager, Sensor Fuzed Weapon Development, followed by a PM position on the Advanced Medium Range Air-to-Air Missile. Ed graduated Air Command and Staff College 1998 and became the Program Director, HARM Targeting System. Ed became a USAF civil servant as Chief System Security, leading systems security engineering for multiple weapons programs. Professor Adkins has 30 years of acquisition, engineering and test experience and is certified Level III in Program Management, Engineering and T&E.

Mr. Frank Alvidrez is a Certified DoDAF Enterprise Architect currently working at Edwards Air Force Base as a Sr. Cybersecurity Operational Flight Test Engineer. He specializes in using advanced Model Based System Engineering techniques to support developmental and operational Air Force Flight Test programs. He has successfully used DoDAF & MBSE tool sets to support flight tests and is currently using advanced techniques for cyber resiliency design and test. He has in-depth experience in Program Management, Enterprise Architectures, Net Centric Data Strategy, SysML, and DoDAF/UPDM Training and cybersecurity. He is a graduate of the FEAC DoDAF Enterprise Architecture Course as well as Defence Acquisition University Executive Program Managers Course. He worked 20 years for the Lockheed Martin Skunkworks and worked many projects to include B-1B, B-2A, B-52, X-35, Navy MRE UAV, YF-22, F-16, C-130, A-4AR, U-2, SR-71, OV-10A/D and other classified projects. He currently teaches advanced DoDAF courses using the DoDAF Profile in UML and SysML. He is a member of the Association of Enterprise Architects (a|EA), INCOSE, and a number of other professional organizations on System Engineering and Enterprise Architectures.

Col. Marshall "Ozz" Bronston (USAF, ret) is a Professional Research Engineer with Georgia Institute of Technology's (GIT) Field Office in Tucson, Arizona. Since joining Georgia Tech in August of 2009, he successfully developed concepts, programs, and systems to increase combat force effectiveness and survivability. Marshall's work within Georgia Tech includes leading multiple engineering teams to improve cyber security of military networks, test and evaluation of a variety of aircraft platform and tactics-related improvements, and new test and evaluation methods & processes. He was the lead systems engineer for the Computer Adaptive Network Defense-in-Depth Joint Capability Technology Demonstration which resulted in transition of the Virtual Secure Enclaves security upgrade to US Navy and Joint computer networks. Marshall was co-project director for a team of 30 electronic warfare (EW) subject matter experts that developed a 14-month resident curriculum for EW reprogramming and multiple other short course variants of the knowledge generated by the team. He is lead instructor for GIT College of Engineering's signature course in graduate-level systems engineering and the Fundamentals of Cybersecurity Test and Evaluation course. Before selection to GIT's research faculty, Marshall held multiple senior staff and command positions in the USAF. As a combat and operational test pilot, he logged well over 4000 flight hours in the F-4, F-16, C-17, and 11 other aircraft types. While serving as a requirements officer, he sponsored and directed over 40 formal service test and evaluation programs and was a senior member of a team with a $14B modernization portfolio. While commanding a flight test center, he led teams that put an "internet in the sky" over Iraq, established his organization as a clear leader in integrating and testing aircraft survivability enhancements, added day/night precision attack capability to a fleet of over 600 F-16s, and turned the A-10 and B-52 into precision attack platforms. Marshall obtained a B.S. in computer science from the US Air Force Academy (1982), an M.S. in Administration from Central Michigan University (1987), a Professional Masters in Applied Systems Engineering from Georgia Tech (2012), and has completed multiple post-grad programs including a Fellowship with the Asia Pacific Center for Security Studies (2005). He received the coveted Top Academic Trophy from his F-16 Fighter Weapons School class. He is a Defense Security Service-certified Information Systems Security Manager and an (ISC)2-certified Computer Information Systems Security Professional (CISSP). In his spare time, he enjoys riding horses and road bikes, having once bicycled solo from coast-to-coast in 38 days.

COL David "Maggie" Brown, (USAF, Ret), is the Director for Cyber Programs at Electronic Warfare Associates, headquartered in Herndon, Virginia. He retired from the USAF as a Command fighter pilot after 30 years of service and a strong background in both operations and T&E. A USAF Fighter Weapons School graduate with 4000 hours flying the F-4, F-117 and QF-106, he has held leadership positions in numerous Operational and T&E organizations. He served as a OT&E Test Pilot, Test Director for multiple programs within the Air Force Operational Test and Evaluation Command, as well as the Director of the Joint Close Air Support, Joint Test and Evaluation (Office of the Director, Operational Test and Evaluation), and Commander of the Joint Fires Integration and Interoperability Team under U.S. Joint Forces Command. He has been with EWA since 2007 working distributed testing initiatives with OSD and DoD customers.

Mr. Kevin P. Burns was raised in Connecticut and attended the United States Air Force Academy, CO, where he concluded coursework as a Distinguished Graduate in 1975. Upon commissioning, he completed a 1-year Master's Program in Electrical Engineering at the University of California, Berkeley. After finishing pilot training in 1977 at Williams AFB, AZ, he was assigned as a T-38 Instructor Pilot at Laughlin AFB, TX. He was subsequently assigned to the F-15 Eagle at Langley AFB, VA, and later at Keflavik, IC, as an aircraft commander. In 1983, Mr. Burns attended the USAF Test Pilot School at Edwards AFB, CA, receiving the prestigious Liethen-Tittle Award as Class 83B's top pilot. Remaining at Edwards, he flew a variety of developmental flight test missions in A-10 and F-16 aircraft.

In 1988, Mr. Burns joined the Air Force Flight Test Center's 6513th Test Squadron, where he accomplished flight test duties in an assortment of prototype fixed-wing fighters. After attending the Air War College at Maxwell AFB, AL, in 1995, he was assigned as the Deputy Chief, Power Projection Division, and as Chief, Theater Air Defense Division, in the Acquisition Secretariat's Global Power Directorate, Washington DC. Beginning in July 1998, Mr. Burns was assigned as Commander, 46th Operations Group, and then as Vice Commander, 46th Test Wing, Eglin AFB, FL, where he led these organizations in the conduct of flight and ground developmental test and evaluation of USAF conventional air armament, airborne countermeasures, and command and control systems. Mr. Burns retired from Air Force Active Duty on September 30, 2002 and resumed working at Eglin AFB for Sverdrup Technology, Inc., performing management and test advisory duties for Air Armament Summit V and a new-start classified weapon program office. In 2004, Mr. Burns accepted government employment with the 53d Wing as its Test Management Group's Technical Advisor, where he is relied upon by all echelons of OSD, HAF, MAJCOM, USAF Warfare Center (USAFWC), and 53d Wing for sound advice on relevant aspects of CAF and space developmental and operational test.

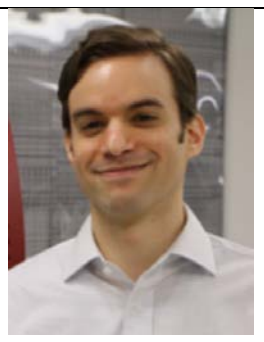
James Cannady, PhD, is a Principal Research Scientist in the Georgia Tech Research Institute (GTRI) CIPHER Lab. He has worked extensively with Federal, State, and local governments to improve the security of their critical information systems. Dr. Cannady's research efforts concern the intersection between artificial intelligence and information security. In particular he is working to develop new adaptive intelligent systems that can be applied to protect computer systems and networks. These techniques include the use of advanced neural networks in the detection of network-based attacks. He is the co-founder of the Georgia Tech Information Security Center. Prior to his academic career Dr. Cannady was a Special Agent with the U.S. Naval Investigative Service, specializing in counterintelligence matters and the protection of military computer and communication systems. He has worked extensively within U.S. Government and NATO organizations where he has developed policies and procedures that have enhanced the security of critical information systems.

Mitch Crosswait, PhD, is the 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.

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 enroute 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.



Domenic Forte, PhD, received his B.S. degree in Electrical Engineering from Manhattan College, Riverdale, NY, and his Masters and Doctorate in Electrical Engineering from the University of Maryland, College Park. Dr. Forte is an Assistant Professor with the Electrical and Computer Engineering Department at University of Florida, Gainesville, FL where he leads multiple efforts within the Florida Institute for Cybersecurity Research (FICS Research). From 2013 to 2015, he was an Assistant Professor of the Department of Electrical and Computer Engineering, University of Connecticut in Storrs, CT. His research covers the entire domain of hardware security from nanoscale devices to printed circuit boards (PCBs). Topics include hardware security primitives, hardware Trojan detection and prevention, security of the electronics supply chain, security-aware design automation tools, reverse engineering, and anti-reverse engineering. He also performs research in biometric system security, reliability, and implementation with specialization in physiological signals such as electrocardiogram (ECG) and photoplethysmograph (PPG). Dr. Forte is a recipient of the NSF Faculty Early Career Development Program (CAREER) Award (2017), Army Research Office (ARO) Young Investigator Award (2016), Northrop Grumman Fellowship (2012), and George Corcoran Memorial Outstanding Teaching Award (2008). His research has been also recognized through best paper awards and nominations from multiple organizations and conferences. He is a member of the Institute of Electrical and Electronics Engineers (IEEE) and IEEE Circuits and Systems Society (CAS). He serves on the organizing committees of top conferences in hardware security such as IEEE International Symposium on Hardware Oriented Security and Trust (HOST) and Asian HOST. He also serves on the technical program committees of including Design Automation Conference (DAC), International Conference on Computer-Aided Design (ICCAD), Network and Distributed System Security Symposium (NDSS), IEEE International Test Conference (ITC), and International Symposium for Testing and Failure Analysis (ISTFA). He is a co-author of the book “Counterfeit Integrated Circuits-Detection and Avoidance”, co-editor of the book “Hardware Protection through Obfuscation”, and co-editor of the book " Security Opportunities in Nano Devices and Emerging Technologies ". He is an Associate Editor of Journal of Hardware and Systems Security (HaSS) and was the Guest Editor of the IEEE Computer 2016 Special Issue on “Supply Chain Security for Cyber-Infrastructure.”2.

Mr. J Tristan Gilbert is a Certified Information Systems Security Professional (CISSP) who is currently working as a Lead Computer Engineer for the Army Test and Evaluation Command (ATEC) at White Sands Missile Range (WSMR) for the Range Operations Directorate. The Range Operations Directorate is responsible for the operation of sensor and processing systems supporting the Open-Air Test mission at WSMR. Tristan has expertise in Systems and Network Administration, Security Technical Implementation Guide (STIG) compliance, Vulnerability Scanning and Assessment and is primarily focused on the Cybersecurity posture and associated documentation of these systems. Tristan is also currently serving in the Range Commanders Council (RCC) as the Cybersecurity Group (CSG) Vice-Chair. Tristan holds a Bachelor of Science in Electrical and Computer Engineering from New Mexico State University, a Master of Science in Program Management from the Naval Postgraduate School, and several industry standard security and technical certifications from CompTIA, EC-Council, and Cisco.

Mr. Roderick Hallum is a senior analyst with Scientific Research Corporation supporting the Joint Staff J6 and the Defense Enterprise Cyber Range Command and Control Information Systems (DECRE-C2IS) partnership. Rod had his first exposure to T&E in 1983 after graduating from the Program Managers Couse with the Product Assurance Test and Evaluation Division of the Bradley Fighting Vehicle program office. He started working in cyber in 2001 as the lead contractor on a CTEP program to develop a methodology and measures and metrics for testing IA/CND for the Operational Test Agencies. For the past 5 years he has been the lead analyst for the DECRE-C2IS partnership. He is a retired Army Armor officer. He has a bachelor’s degree in chemistry from the CITADEL and did his masters work in systems management with the Florida Institute of Technology.

Mr. Greg Jaeger leads teams who build and sustain complex systems in diverse industries, including manufacturing and e-commerce. With more than 30 years of coding and management experience, Greg developed communication skills at technical, client, and management levels. Throughout the 1990s, Greg managed contractor teams that built and deployed reverse engineering and agile manufacturing systems worldwide through programs structured using DOD-STD-2167A, TQM, and JAD/RAD methods. The programs honed a breadth of process engineering and management disciplines for effectively conveying client visions throughout program execution. Greg was an early adopter of Internet technology by writing web-based applications to streamline project management, testing, and team and client communications. This experience was extended to the on-demand manufacturing industry through an e-commerce service that culminated in "Parts à la Carte"® – a commercial web service for inventors and custom part buyers to engage a manufacturing broker who validated their technical data packages and brokered contracts with competitive manufacturers. The manufacturing brokerage was adapted to the DoD Electronic Mall (DOD EMALL) system in 1998 as a collaborative commerce service. A decade later, Greg managed the DOD EMALL sustainment program until its replacement in 2017. The journey embraced current methodologies and frameworks including PMI, CMMI, Agile, DevOps, NIST Risk Management and the NIST Cybersecurity Framework. Greg challenged the EMALL Team to become proactive amidst zero-day cybersecurity exploits, limited system insight, and incomplete vulnerability data. Through role changes, reuse of existing data, and dynamic collaboration of development and operations members, the Team magnified system and cyber awareness that enabled Greg to make preemptive, risk-based decisions.

The resultant methodology strengthened teamwork and institutionalized security across the management, development, and operations domains. Greg received a B.S. in Electrical Engineering and a Graduate Certificate in Program Management from The Citadel. Greg is a member of IEEE, holds a CISSP Certificate, and remains current in software engineering, management, and cybersecurity through various memberships and affiliations. Greg mentors and remains active in the application of PMI, Agile, CMMI, and NIST frameworks/standards and directly participates in the IEEE P2675 DevOps Standard Working Group.

Mr. Michael Landolt is an Army Civilian working in the Army Evaluation Center as a survivability evaluator. He has seventeen years of acquisitions experience including ten as an acquisitions officer in the United States Air Force holding multiple positions in T&E and program management. He is DAWIA Level III certified in T&E and Level II certified in Program Management and Engineering. Michael has a BS in Electrical Engineering from the Illinois Institute of Technology and an MBA from Nichols College. His cybersecurity professional certifications include COMPTIA Security+ and (ISC)2 Certified Information System Security Professional (CISSP).

CAPT Michael G. Lilienthal, (USN Ret), PhD, CTEP, is the Director of Cyber and Navy Programs at Electronic Warfare Associates, Government Systems, headquartered in Herndon, Virginia. He received his Doctor of Philosophy in Experimental Psychology, specializing in psychophysical scaling and measurement from the University of Notre Dame. He is a graduate of the Navy War College Command and Staff College, has a Certificate in Systems Engineering from the Navy Postgraduate School, is a Certified Professional Ergonomist and an IEEE Certified Biometrics Professional. Dr. Lilienthal served in the Navy for over 30 years as an Aerospace Experimental Psychologist working a variety of programs in research, training, human systems integration, policy development, test & evaluation and modeling & simulation, including a Joint tour with the Army G-3/5/7 as the Deputy Director of the Biometrics Task Force. He retired as a CAPTAIN and following this has been working for EWA since 2009 in the area of Joint distributed testing programs for DoD for Navy ACAT programs.

Al Morris is a retired Army NCO with over 30 years in Aviation and Information Assurance/Cybersecurity experience. Mr. Morris has his CISSP, CHFI, and CEH Certifications. Mr. Morris has been with PeopleTec for 9 years where he has been the Information System Security Manager (ISSM) for 4 Acquisition Category 1 programs. He was the first ISSM for the Utility Helicopter Project Office. After building their Information Assurance program and training their personnel, Mr. Morris was asked to move to the newly stood up Improved Turbine Engine / Future Vertical Lift Project Office. This Project Office has since split into two new organizations, Aviation Turbine Engine Project Office (ATE PO) and the Future Vertical Lift Project Office (FVL PO). Mr. Morris is currently the ISSM for both organizations.

Brian Mork, PhD, (BS Analytical Chemistry, Math minor, Physics minor, Magna Cum Laude, Phi Beta Kappa, Hope College; PhD Analytical Chemistry, Univ Illinois; Masters Strategic Studies, Air University) is a Senior Plans and Programs Engineer at the Air Force Research Lab Headquarters, Dayton, OH. His expertise is in Engineering, Aviation Operations, Education, and Science. Brian is a 30-year US Air Force pilot veteran, flew KC-135s for Strategic Air Command during Desert Storm, and is the only pilot graduate of Air Force Space Command's Space Tactics School. As a Senior System Engineer, he designed SCADA architecture for automotive manufacturers and oil pipeline shipment control centers. He was a faculty lead for the launch of the USAF Academy's first satellite and served as an Assistant Professor at a private undergraduate college. As a government SETA contractor, he was the AFTC DEW SME, and as an instructor pilot and platform instructor at USAF Test Pilot School, he specialized in mission systems such as Radar, Directed Energy Weapons, Cyber, Communications, and EO/IR sensors. Currently, he expedites technology maturation and transition for the special access portfolio of the Air Force Research Lab technical directorates.

Joseph W. Nichols, PhD, a senior-level executive, is the Technical Advisor for Flight Test and Evaluation, Air Force Test Center, Edwards Air Force Base, Calif. He is the senior technical advisor to the AFTC Commander regarding health and suitability of airframe, avionics, installed propulsion, C4ISR, cyber and electronic warfare flight and supporting ground test capability across AFTC's test ranges and facilities valued at more than $31 billion, including 116 aircraft and 164 ground test facilities. AFTC's workforce of 18,000 military, civilians, and contractors and its ranges and facilities are located across the U.S. including Edwards AFB; Eglin AFB, Fla.; Holloman AFB, N.M.; and Arnold AFB, Tenn. Dr. Nichols establishes flight test and evaluation technical policy and procedures and provides technical expertise and direction to the AFTC work force. He formulates testing approaches to assure scientific validity, effectiveness and efficiency in accomplishing ground and flight tests. Dr. Nichols represents the center on the Air Force Materiel Command Engineering Council, the Executive Committee of the Range Commanders Council, and the Spectrum Stewardship Senior Steering Group. Dr. Nichols served for 26 years as an Air Force officer, retiring as a colonel. During this military career he served as a flight test engineer, test squadron commander and group commander. He was a senior nonrated aircrew member with flight test experience in the F-111, F-16, C-130 and C-17. Dr. Nichols was appointed a Senior Leader executive in October 2013.

Mr. Arch Owen is the Business Area Lead for Guided Solutions within Draper's Defense Systems Program Office. In this role, Mr. Owen oversees many programs involving Guidance, Navigation, Control, Autonomy, and Open Software Architectures. Across the portfolio, Mr. Owen is engaged with the challenges the US DoD faces in securing weapon systems, from design to development and testing. He is working to bring advanced Cyber Security techniques to secure these and other Weapon Systems. Prior to joining Draper, Mr. Owen held positions at OptaSense (A QinetiQ subsidiary), QinetiQ North America, BBN, and General Electric spanning a variety of positions including advanced technology development, management, and international business development.

Mr. Ron Prado is with the Georgia Tech Research Institute and is the Chief Scientist for the Network Vulnerability Division with over 25 years of broad experience in weapons and avionics system testing and evaluation including EW, C4I, and Cybersecurity T&E. Mr. Prado has led the instrumentation and testing of systems at various stages of development including applied research, developmental, and operational testing, and within a number of environments from lab testing, system and hardware integration, to over-the-air ranges and facilities. Cybersecurity resilience efforts include development and testing of cybersecurity solutions for weapons and wireless communications systems. Mr. Prado also leads GTRIs cybersecurity testing of weapon and avionic system and subsystems with special focus on deep embedded and wireless system analysis. Mr. Prado holds a bachelor and Master of Science in electrical engineering from Georgia Tech and currently teaches the Georgia Tech Fundamentals of Cybersecurity Test & Evaluation Professional Development short course.

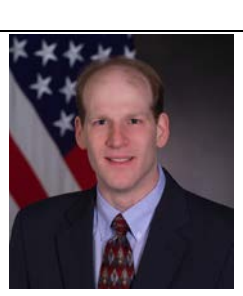
Sarah Pramanik, PhD, CISSP, CEH, CNDA, is the Northrop Grumman Aerospace Sector Software Products Directorate Cybersecurity Champion. She works as a security architect and security engineer on multiple programs. She is providing subject matter expertise for the development, integration, verification and execution of cybersecurity activities across both software and system teams. Dr. Pramanik has worked in multiple areas of cybersecurity, including vulnerability and penetration testing, information system security engineering, cybersecurity training and security architecting. She likes research and breaking things. She also enjoys working with the next generation of cyber engineers. She holds a B.S. and M.S. in Computer Science and a PhD in Engineering with an emphasis in Security from The University of Colorado, Colorado Springs.

M. John Rafferty, Jr. is an Electronics Engineer for the F-35 Partner Support Complex at Eglin Air Force Base, FL. He has worked for the 53rd Wing for 15 years, serving as a Mission Data Engineer on the F-16 Block 52, Block 60, and F-35 mission data teams. He is currently the Lead Mission Data and Electronic Warfare Suite Trainer for the Norway and Italy Reprogramming Lab, informing our partners on how to provide the ELINT/SIGINT data needed for the F-35 Lightning II to perform its situational awareness and air superiority missions.

Mr. Steven J. Rajotte began his active duty career as an engineer supporting the Air Force Satellite Control Network and then as a program manager at the GPS NAVSTAR Joint Program Office, Los Angeles AFB, CA. He then transitioned to operational flying and accumulated over 2,600 hours as an Instructor and Evaluator Pilot in the KC-135 with over 490 combat flying hours in theater during his assignments at Fairchild AFB, WA and McConnell AFB, KS. This unique combination of acquisition and operational experience led him to pursue assignments in Developmental Test, Operational Test, and Test Management. He began his T&E career as the AMC Chief Operational Test Director, McGuire AFB, NJ and then served as the KC-46 Chief Test Director, Wright-Patterson AFB, OH. After retiring from active duty, Mr. Rajotte continued as a government civilian serving as a Chief Developmental Flight Test Engineer for mobility aircraft (C-17, C-130, KC-10, KC-135) and F-16s at Edwards AFB, CA. He was then competitively selected by HQ AFMC Engineering Directorate to support the HQ AFMC/A3 Air, Space and Information Operations Directorate as a trusted T&E expert and policy consultant. While serving on the HQ staff he developed policy for the emerging area of cyber T&E and was recently selected to take the lead for cyber workforce development supporting SAF/AQ's recently commissioned Cyber Resiliency Office for Weapon Systems (CROWS). Mr. Rajotte is currently the Cyber Workforce Development Branch Chief for the CROWS, Wright-Patterson AFB, OH, working to develop a cyber-savvy workforce capable of integrating cyber security measures into all phases of the acquisition process, resulting in the delivery of cyber-resilient weapon and support systems to the warfighter. As part of this process he develops weapon system-focused cyber training for the 36,000 acquisition professionals across the Air Force.

Mr. Randall (Randy) Rice is a leading author, speaker, consultant and practitioner in the field of software testing and software quality. He has over 38 years of experience in building and testing software projects in a variety of environments and has authored over 70 training courses in software testing, security testing and software engineering. Randy holds many ISTQB certifications; including all three ISTQB "core" Advanced Certifications, the Advanced Security Tester certification, Certified Mobile Tester, and Certified Agile Tester, Foundation Level. Randy is the chair of the ISTQB Advanced Security Tester Working Party that created the 2016 Advanced Security Tester Syllabus. He is also a director of the American Software Testing Qualifications Board (ASTQB). Randy is co-author with William E. Perry of the books, Surviving the Top Ten Challenges of Software Testing and Testing Dirty Systems.

Mr. Elbert Michael Ruiz joined GTRI in 2015 as a Senior Research Engineer, specializing in embedded system design, analysis, and vulnerability assessment. Prior to GTRI, Mr. Ruiz worked for over 15 years as a civilian within the Intelligence Community, where he obtained experience working in a wide variety of technical disciplines including custom ASIC design, RF and antenna engineering, circuit design, FPGA development, wireless networking, and embedded software/firmware development. He served as a technical project lead for a quick-reaction applied research organization where he led the development and delivery of several custom embedded communications systems. He also has working experience in computer forensics, software vulnerability analysis, and network security/incident response. He was awarded the Secretary of Defense Medal for the Global War on Terror in 2010, and several Unit merit awards. Mr. Ruiz earned his Bachelor's degree in Electrical Engineering in 2003, and Master's degree in Electrical and Computer Engineering in 2004, both from the Georgia Institute of Technology, and has an active ham radio license (KJ4GAO).



Mr. George Rumford is the Deputy Director for Major Initiatives and Technical Analyses for the Department of Defense (DoD) Test Resource Management Center (TRMC), a field activity that reports directly to the Under Secretary of Defense for Acquisition, Technology, and Logistics. In this capacity, Mr. Rumford serves as the Program Manager for the Test and Evaluation / Science and Technology (T&E/S&T) Program. Sponsoring advanced technology research and development in industry, academia, and government laboratories, the T&E/S&T Program develops technologies to upgrade the capabilities at test and training ranges to support future warfighting systems.

Advancing common instrumentation solutions at test and training ranges, Mr. Rumford also oversees the Test and Training Enabling Architecture (TENA) Software Development Activity (TENA SDA) and the Joint Mission Environment Test Capability (JMETC). The TENA architecture provides a common integrating software solution for the variety and multitude of range systems, simulations, and facilities in the test and training communities, and JMETC provides an enterprise solution to network test facilities and laboratories across the Services and in industry, including at multiple independent levels of security classification, to enable early testing of warfighting systems in an operational Joint context. In addition, he is the Senior Technical Advisor for the National Cyber Range (NCR) and all TRMC Cyber T&E Infrastructure investments to conduct realistic cybersecurity testing, evaluation, experimentation, and training. Prior to joining the TRMC, Mr. Rumford worked at the Defense Information Systems Agency (DISA) and for the Army at White Sands Missile Range, supporting testing of missile defense systems, space systems, and several multi-Range, multi-Service exercises. Born in St. Louis, Missouri, Mr. Rumford has received degrees with honors in Electrical Engineering and in Computer Engineering from the University of Missouri.

Ms. Sarah Standard is a 1988 US Naval Academy graduate and a retired Navy Captain, retiring in 2013. Commissioned as a Supply Officer, she served 5 years of active duty before transitioning to the reserves and after earning her MA in Applied Mathematics from the University of Maryland, College Park, with applications in Numerical Analysis, Operations Research, and Databases, she transitioned to the Information Professional community in 2004. She also has certificates in Enterprise Architecture and Chief Information Officer from the National Defense University. Previous assignments in the reserves include serving as the Reserve N6 with the Space and Naval Warfare Systems Command, as Information Management Cell Lead and then as Knowledge Management Officer with the Commander, Second Fleet (C2F), as Commanding Officer for Communication and Information Systems (CIS) C2F, and as CIS Director for Commander, Third Fleet. In 2010, Sarah returned to active duty and instructed calculus and cybersecurity courses at the US Naval Academy until 2013 and returned as a civilian adjunct through 2014. In 2014 she began working for AVIAN, LLC where she developed and instructed a NAVAIR-specific cyber warfare course for the NAVAIR acquisition workforce, teaching over 3000 in the first year offering the course. In 2016 she transitioned as a cybersecurity SME for The Patuxent Partnership and was subsequently selected to serve as the Cybersecurity/Interoperability Technical Director to the Principal Deputy Director, DASD(DT&E).

Mr. Patrick Thompson currently serves as the Technical Director for Ballistics and Non-Ballistics Survivability for the Survivability Evaluation Directorate, U.S. Army Evaluation Center. Mr. Thompson has over 30 years of RDT&E experience. He began his career in 1983 with what is now the Army Research Laboratory/Survivability Lethality Analysis Directorate (ARL/SLAD) at White Sands Missile Range, NM. While there, he performed electronic countermeasures vulnerability assessments using full-digital and Hardware-in-the-Loop (HWIL) Models and Simulations. In 1996, he took a position as an evaluator with the Survivability Directorate of the Army Evaluation Center (AEC). During his career with AEC, he has participated in the evaluation of systems supporting all warfighting functions. He holds a MS in Electrical Engineering from the University of Texas—El Paso and a BS in Chemical Engineering from Stanford University. He is a member of the Army acquisition corps and is level three certified in Test and Evaluation and Engineering.

Mr. Paul Waters graduated from the Air Force Academy and started testing airplanes at Edwards AFB in 1985. He has performed structures testing and test capabilities development for over 24 years. He also served as an Assistant Professor in the Engineering Mechanics department at the U.S. Air Force Academy for over 6 years. Paul has a PhD from the University of Colorado in Aerospace Engineering. Currently, Paul is the Technical Director for the Test Engineering Group at Edwards AFB and is responsible for the development of new test capabilities for the Group, particularly in Range and Instrumentation disciplines. Paul is also the ISSM for the Group for DT&E systems.

Mr. Adonis Williams is a Cybersecurity Test Engineer at The Boeing Company in Seattle, Washington. He holds a B.S. in Mechanical Engineering and M.S. in Systems Engineering from Missouri University of Science and Technology. As a Cyber Table Top Facilitator, Adonis leads programs through vulnerability identification exercises which prioritize targets for cybersecurity testing across platforms. Adonis's previous flight test experience encompassed avionics and mission systems testing on both commercial and military derivative aircraft. Prior to his current role, Adonis served as the Technical Lead Engineer (TLE) for the Boom Control Law System on the KC-46 Tanker Program. In his free time Adonis enjoys volunteering, fitness, traveling, and spending time with friends and family.

Christina Witt is the Team Lead for the JT3 Information Assurance Documentation and Validation Team at Edwards AFB. She is certified in RMF with ISC2 CAP and has obtained her ISC2 CISSP. Christina Witt has two Master's of Science degrees: Cybersecurity & Management of Information Systems with a concentration in Cybersecurity. She has specific training from the Institute of Analytic Interviewing in Insider Threat Mitigation and Countermeasures. Her fascination in Cybersecurity includes computer forensics, social engineering, and experimenting with various hacking techniques. In her spare time, she volunteers in her community educating others about the importance of Cybersecurity and how to protect personal home networks, Internet of Things devices, and other wireless devices. Outside of the cybersecurity realm she enjoys riding motorcycles, exploring the desert and mountains on dirt bikes, and playing Ingress.

ITEA Corporate Members

Acquired Data Solutions, Inc.
Advanced Systems Development, Inc. (ASD)
Advanced Test Equipment Rentals
AEgis Technologies Group, Inc.
Aermor LLC
Agency of Defense Development Technical Library
Air Academy Associates
AMERICAN SYSTEMS
Analytical Graphics, Inc.
Apogee Labs, Inc.
Applied Research Laboratory/ Penn State University
Arcata Associates, Inc.
Astro Haven Enterprises
AssetSmart
ATAMIR WSMR
Australian Defence Force Tactical Data Link Authority
Avionics Interface Technologies
BAE Systems (Australia)
BEI Precision Systems & Space Company
Black Diamond Consulting
Brazilian Aeronautical Commission, D.C.
CALCULEX, Inc.
Capability Analysis & Measurement Org. LLC
Cervello Technologies, LLC
Command Post Technologies
Compunetix, Inc.
Defense Acquisition University
Dell EMC Corporation
DEWESoft, LLC
Dynetics, Inc.
Emhiser Research
Engility Corporation
Engineering Research and Consulting, Inc. (ERC)
EWA Government Systems, Inc.
Garud Technology Services, Inc. (GTS)
Geil Marketing Associates (GMA)
General Dynamics Mission Systems
Georgia Tech Research Institute - GTRI
Glacier Technologies
InDyne, Inc.
Jacobs Technology, Inc.
Joint Research and Development, Incorporated
JT3, LLC
Kaman Precision Products
KBRwyle
Kistler Instrument Corp.
L-3 Telemetry & RF Products (L3 T&RF)
MacAulay-Brown, Inc.
Maritime Test and Evaluation Authority
MEI Technologies, Inc.
Modern Technology Solutions, Inc. (MTSI)
National Chung Shan Institute of Science and Technology - NCSIST
NetAcquire Corporation
New Zealand Defence Force
Nova Systems
PAE
Photo-Sonics, Inc.
Quintron Systems Inc.
Rockwell Collins
Rolls-Royce plc
Rotating Precision Mechanisms, Inc. (RPM)
RoundTable Defense, LLC
Schafer Corporation
Scientech Inc.
Scientific Research Corporation
Sealing Technologies Inc.
SURVICE Engineering Company
SYMVIONICS Inc.
System Testing Excellence Program
Systems Application & Technologies (SA-Tech)
Systems Engineering & Management Company
Teletronics Technology Corp.
Telspan Data
The Boeing Company
The MIL Corporation
THE SENTE GROUP, INC.
TRAX International
Trident Research
TRIDEUM Corporation
Ultra Electronics Herley Lancaster
Weibel Scientific A/S
Westech International, Inc.
Wideband Systems, Inc.
WJ Hughes FAA Technical Center
Zodiac Data Systems

ITEA Chapter Locations

NORTHEAST REGION
Vacant,
Vice President

MASSACHUSETTS
New England Chapter
Michelle Kirstein, President
Boston, MA

NEW JERSEY
South Jersey Chapter
John Frederick, President
Atlantic City, NJ

OHIO
Miami Valley Chapter
Vacant, President
Dayton, OH

PENNSYLVANIA
Penn State Chapter
Bruce Einfalt, President
State College, PA

MID-ATLANTIC REGION
Jeanine McDonnell,
Vice President

MARYLAND
Francis Scott Key Chapter
https://www.fskitea.org/jome.html
Chris L. Susman, President
Aberdeen, MD

Southern Maryland Chapter
Ed Greer, President
Patuxent River, MD

DC/NORTHERN VIRGINIA
George Washington Chapter
http://gw-itea.org
Richard Bailer, President
Washington, DC

VIRGINIA
Hampton Roads Chapter
Eric S. Whiteman, President
Hampton Roads, VA

SOUTHEAST REGION
Miles Thompson
Vice President

ALABAMA
Rocket City Chapter
Lewis T. Hundley, President
Huntsville, AL

FLORIDA
Central Florida Chapter
Steven C. Gordon, President
Orlando, FL

Emerald Coast Chapter
http://itea-ecc.org
Nathan M. King, President
Eglin AFB, FL

GEORGIA
Atlanta Chapter
http://iteaAtlanta.org
Joseph Hurst, President
Smyrna, GA

SOUTH CAROLINA
Charleston Chapter
Vacant, President
Hanahan, SC

TENNESSEE
Volunteer Chapter
Vacant, President
Arnold AFB, TN

SOUTHWEST REGION
David Webb
Vice President

COLORADO
Rocky Mountain Chapter
http://www.itea-rmc.org
Vacant, President
Colorado Springs, CO

ARIZONA
Huachuca Chapter
Joseph F. Puett, President
Sierra Vista, AZ

Valley of the Sun Chapter
Duard Stephen Woffinden, President
Scottsdale, AZ

NEVADA
Southern Nevada Chapter
Darryl Johnson, President
Las Vegas, NV

NEW MEXICO
Roadrunner Chapter
Ralph R. Galetti, President
Albuquerque, NM

White Sands Chapter
Steve Aragon, President
White Sands, NM

UTAH
Great Salt Lake Chapter
Vacant, President
Dugway, UT

WEST REGION
Terrance McKearney
Vice President

CALIFORNIA
Antelope Valley Chapter
http://www.iteaavchapter.org
Christopher Klug, President
Edward AFB, CA

Channel Islands Chapter
Joyce Matias, President
Point Mugu, CA

China Lake Chapter
Vacant, President
China Lake, CA

Greater San Diego Chapter
Daniel Phalen, President
San Diego, CA

HAWAII
Mid-Pacific Chapter
Shannon Wigent, President
Kalaheo, HI

WASHINGTON
Pacific Northwest Chapter
Ron Thompson, President
Seattle, WA

INTERNATIONAL REGION
Peter Nikoloff
Vice President

AUSTRALIA
Southern Cross Chapter
Peter G. Nikoloff, President
Edinburgh, South Australia

EUROPE
European Chapter
Adrian Britton, President
United Kingdom

ISRAEL
Israeli Chapter
Aaron Leshem, President
Haifa, Israel

Certified Test and Evaluation Professionals

The following individuals have been awarded the Certified Test and Evaluation Professionals (CTEP) designation, which recognizes those individuals who demonstrate the following: They meet the minimum level of competency in the requisite Knowledge, Skills, and Abilities (KSA) that have been identified by T&E subject-matter experts (SMEs); their commitment to maintain currency in the field; and their dedication to advancing the profession.

Please join us in congratulating these T&E professionals on their achievement!

Allan V. Alfafara, CTEP - Northrop Grumman Aerospace Systems
MAJ Cornelius Allen, USA, CTEP - PEO Aviation
Dana Allen, CTEP - Air Force Space and Missile Systems Center
Benjamin Andersen, CTEP - Modern Technology Solutions, Inc.
Rebecca L. Badgley, CTEP - Advanced Management Strategies Group
Suzanne M. Beers, Ph.D., CTEP - The MITRE Corporation
David Scott Bough, CTEP - Prevailance, Inc.
Richard Boyer, CTEP - Scientific Research Corporation (SRC)
Rebecca Bradshaw, CTEP - TransCore
Gary Brandstrom, CTEP - Raytheon Missile Systems Co.
E. Wyatt Brigham, CTEP - Northrop Grumman Aerospace Systems
C. David Brown, Ph.D., CTEP - DT&E
John Burke, CTEP - JRAD
Thomas Cash, CTEP - CGI Federal
Peter H. Christensen, CTEP - The MITRE Corporation
Peter G. Crump, CTEP - Georgia Tech Research Institute (GTRI)
Paul R. Dailey, Ph.D., CTEP - Johns Hopkins University Applied Physics Lab
William Fiedler, CTEP - AEgis Technologies
Michael Flynn, Ph.D., CTEP - Defense Acquisition University (DAU)
Christine Fuentes, CTEP - The MITRE Corporation
Ralph R. Galetti, CTEP - Boeing-SVS
John Geskey, CTEP - Applied Physics Laboratory/The Johns Hopkins University
Melforde Granger, CTEP - Department of Defense
Greg Griffitt, CTEP - Avian Engineering, LLC
Phil Hallenbeck, CTEP - The MITRE Corporation
Brian Paul Hodgkinson, CTEP - Northrop Grumman Aerospace Systems
Garfield S. Jones, CTEP - Department of Homeland Security
Karen Kissinger, CTEP - TASC, Inc.
Michael Lilienthal, Ph.D., CTEP - EWA Government Systems, Inc.
Eric Lowy, CTEP - FAA
Charles McKee, CTEP - T&E Executive
Lt Col. Martin "Marty" J. Mears, CTEP - Alpha Omega Change Engineering (AOCE)
Henry C Merhoff, CTEP - Louis P. Solomon Consulting Group
Chelsea Prendergast, CTEP - Joint Research and Development, Incorporated
Joseph F. Puett III, CTEP - ManTech International
Robert Randolph, CTEP - Department of Defense
Erwin Sabile, CTEP - Booz Allen Hamilton
Thomas Sachse, CTEP - PEO SUB
Kristopher Scher, CTEP - Science Applications International Corporation
Mike Short, CTEP - G2, Inc.
Anthony Shumskas, CTEP - TASC, Inc.
Jody South, CTEP - AMERICAN SYSTEMS
Keith Sumner, CTEP - Booz Allen Hamilton
William J. Swank, CTEP - DASD(DT&E)
Miles Thompson, CTEP - Georgia Tech Research Institute (GTRI)
Steven Tran, CTEP - Northrop Grumman Aerospace Systems
Gregory Turner, CTEP - The MITRE Corporation
James Watson, Ph.D., CTEP - JRAD
James P. Worden, CTEP - Bevilacqua Research Corporation
David Zehr, CTEP - 419 FLTS/DOO

Professional Certification

Elevating the Test and Evaluation Profession with a Globally Recognized Credential

ITEA administers, manages, and awards the Certified Test and Evaluation Professional (CTEP) credential which provides significant benefits to T&E professionals, organizations, and their customers. Over 500 T&E subject-matter experts (SMEs) have been involved in the development of this credential. These SMEs—T&E executives, managers, supervisors, individual contributors, and technicians—have come from a diverse cross-section of the T&E profession, representing industry, government, academia, laboratories, ranges, weapon systems, information technology, transportation, electronic communications, consumer electronics, and more.

PURPOSE OF THE CTEP CREDENTIAL

- Recognize individuals who demonstrate:
  - KNOWLEDGE, SKILLS, AND ABILITIES: They meet the minimum level of competency in the requisite KSAs that have been identified by T&E subject-matter experts (SMEs).
  - COMMITMENT to maintain currency in the field.
  - DEDICATION to advancing the profession.
- Develop and promote common standards, principles, procedures, processes, and terms for the T&E profession.
- Support professional development and education to enhance the KSAs of T&E professionals.

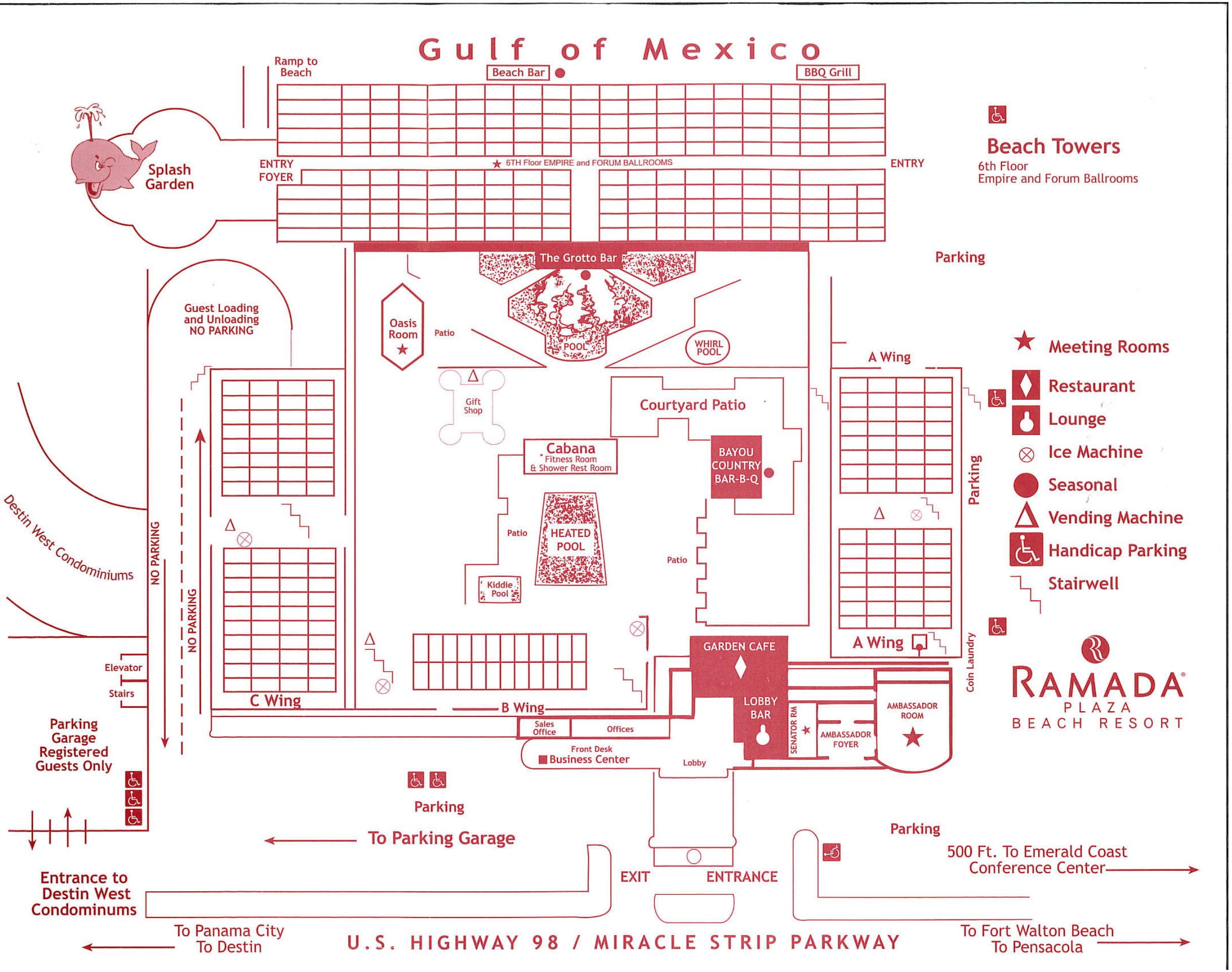
PROFESSIONAL CERTIFICATION VERSUS "CERTIFICATE" PROGRAMS

Please note that a “professional certification credential” is quite different from the “certificate” programs that are currently available to test professionals. “Certificate” programs award a certificate of completion or achievement to individuals after they successfully complete a course of study or meet some minimum requirements.

In contrast, a professional certification credential:

- Is a time-limited recognition requiring periodic submission for re-certification to demonstrate continued currency in the profession, including demonstration of full-time employment in the field and continuing education.
- Awarded based on the candidate’s passing a competency exam, which could be written and/or observational, and would not be related to the completion of any specific course or curriculum of courses.
- Bestows upon an individual to right to use the credential’s designation in conjunction with their name (e.g. CSE, CPA, or CPM) after an assessment and verification that they have met predetermined and standardized criteria.
- Confers occupational identity and provides a method for maintaining quality standards of knowledge and performance and stimulating continued self-improvement.
- Provides differentiation among test professionals, using standards developed through a consensus driven process and based on existing legal and psychometric requirements.
- Requires adherence to a Professional Code of Ethics.

NOTES


Gulf of Mexico
Ramp to Beach
Beach Bar
BBQ Grill
Splash Garden
ENTRY FOYER
6TH Floor EMPIRE and FORUM BALLROOMS
ENTRY
Beach Towers
6th Floor
Empire and Forum Ballrooms
Parking
The Grotto Bar
Guest Loading and Unloading NO PARKING
Oasis Room
Patio
POOL
WHIRL POOL
A Wing
Gift Shop
Courtyard Patio
Cabana
Fitness Room & Shower Rest Room
BAYOU COUNTRY BAR-B-Q
Patio
HEATED POOL
Kiddie Pool
Patio
Parking
Destin West Condominiums
NO PARKING
NO PARKING
Meeting Rooms
Restaurant
Lounge
Ice Machine
Seasonal
Vending Machine
Handicap Parking
Stairwell
Elevator
Stairs
C Wing
B Wing
GARDEN CAFE
LOBBY BAR
SENATOR RM
AMBASSADOR FOYER
AMBASSADOR ROOM
A Wing
Coin Laundry
RAMADA PLAZA BEACH RESORT
Sales Office
Offices
Front Desk
Business Center
Lobby
Parking Garage Registered Guests Only
Parking
To Parking Garage
Parking
500 Ft. To Emerald Coast Conference Center
Entrance to Destin West Condominums
EXIT
ENTRANCE
To Panama City
To Destin
U.S. HIGHWAY 98 / MIRACLE STRIP PARKWAY
To Fort Walton Beach
To Pensacola

THANK YOU TO OUR SPONSORS!

Platinum Sponsor

ZODIAC DATA SYSTEMS

ZODIAC AEROSPACE

Gold Sponsors

AMERICAN SYSTEMS

CCAT CLEAR CREEK APPLIED TECHNOLOGIES

Georgia Tech Research Institute

KBRwyle We Deliver

Gold Sponsor

EWA Government Systems, Inc. Enabling a more secure future

Bronze Sponsor

CAPABILITY ANALYSIS MEASUREMENT CAMO LLC

ITEA is a 501(c)(3) professional education association dedicated to the education and advancement of the test and evaluation profession. Registration fees, membership dues, and sponsorships are tax deductible.

Sponsorship dollars defer the cost of the workshop and support the ITEA scholarship fund, which assists deserving students in their pursuit of academic disciplines related to the test and evaluation profession.