4TH CYBER SECURITY WORKSHOP

"Challenges Facing Test and Evaluation"

PROGRAM GUIDE

March 27-30, 2017

Water's Edge Events Center
4687 Millennium Drive ~ Belcamp, MD

Program Committee

PROGRAM CHAIR - Ms. Chris Susman, SURVICE Engineering Company
PROGRAM TECHNICAL CHAIRS – Mr. Robert Laughman, US Army Evaluation Center, Duane Wilson, Ph.D., Wilson Innovative Solutions LLC, and Mr. Pete Christensen, TRMC
EXHIBITS & SPONSORSHIPS – Ms. Cathy Pritts and Mr. Jim Myers

WORKSHOP DESCRIPTION

Cyber test and evaluation continues to be on the forefront of the acquisition community. In a recent article in *The Defense AT&L Journal*, The Under Secretary of Defense for Acquisition, Technology, and Logistics commented that achieving a survivable cyber test rating in an operational environment is nearly impossible in the current test environment.

This workshop provides an opportunity to share ideas among experienced T&E professionals regarding threat and requirements, test capabilities, cloud-based and IT services, and evaluation methodologies. Our goal is to share ideas on how to better characterize cyber security threats, evaluate system performance when attacked by a cyber security threat, and assess risk of using the system in the presence of a cyber security threat.

Thanks you for joining us as members of the T&E community from academia, industry, and government discuss the evolving discipline of Cyber Security T&E. Please take this opportunity to share your thoughts, connect with others, and learn from some of the leading experts in attendance. The cyber threat will only increase with time.

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

---

THANK YOU TO OUR SPONSORS!

AMERICAN™ SYSTEMS

Founded in 1975, AMERICAN SYSTEMS is one of the largest employee-owned companies in the United States. With offices worldwide and a headquarters in Chantilly, Virginia, we provide a wide variety of services tailored specifically to our customer base. Our approximately 1,300 employee-owners have a vested interest in their work and are committed to delivering the highest-quality strategic solutions to every customer, every time.

EWA Government Systems, Inc.
Enabling a more secure future

EWA Government Systems, Inc. provides products and services to government and commercial markets in engineering, intelligence support, homeland security, special programs, EW operational technology, test & evaluation, and training. Our extensive range of capabilities also includes cyber defense, radar simulators, radar design and development, range instrumentation, and EW scenario simulators, and wireless applications.

KBRwyle
We Deliver

KBRwyle is part of KBR, Inc. (NYSE: KBR). The organization's capabilities span the full spectrum of government mission requirements including research and development, testing, engineering, logistics, deployed operations, and life-cycle sustainment. KBRwyle is the #1 SETA and A&AS contractor to U.S. Naval and Army Aviation, and U.S. Army Air and Missile Defense. It is also the #1 life sciences provider to NASA. KBRwyle is headquartered in El Segundo, California and maintains over 50 office locations.

SURVICE ENGINEERING COMPANY

A nationally recognized specialist in combat system survivability, weapon system effectiveness, and system safety, the SURVICE Engineering Company is a small business that's provided military and industry customers with high-quality analytical products and services for more than 25 years. During this time, we've continued to grow in size, capability, and national recognition; however, we've never lost sight of our original mission—to provide safe, survivable, and effective combat systems for U.S. military personnel.

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.

MONDAY MORNING, MARCH 27TH

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

Identifying Requirements and Vulnerabilities for Cybersecurity, and the Fundamentals of Distributive Testing

Instructor: **Mr. Dave Brown and Mike Lilienthal, PhD, EWA**

With the increased emphasis that the Department of Defense is placing on the use of scientific principles in the test and evaluation environment, you may have heard of the term STAT (Scientific Test and Analysis Techniques). This 4-hour tutorial will provide an overview of some of the most important scientific test and analysis techniques that can and should be used in test and evaluation activities. This session is meant for executives, leaders, managers, and practitioners who need to know what STAT includes and what it can do for their organizations even if they themselves never design a test or evaluate its results. Design of Experiments (DOE) is most definitely a critical component of STAT, but this session will address other important tools as well. Methods for prioritizing requirements and translating them into measurable entities will be discussed, along with Measurement System Analysis (MSA). MSA should answer the question of whether we can trust the data that we are getting from the test. Transfer functions and their use in prediction and optimization will also be presented. After this session, leaders, managers, and practitioners will have a high-level understanding of a variety of methods that are implicit in STAT. No prior statistical prowess is needed to garner some key principles/take-aways from this session.

SimSpace Demonstration

Instructor: **Mr. Lee Rossey, SimSpace**

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

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

Cybersecurity Test & Training using TRMC Resources & The National Cyber Range

Instructor: **Mr. Pete Christensen, TRMC**

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

Planning and Executing Cyber Table Tops, Facilitator Training

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.

TENA/JMETC-Distributed Test & Training Solution for all Classifications & Cyber

Instructor: **Mr. Gene Hudgins, KBRWyle**

The Test and Training Enabling Architecture (TENA) was developed as a United States (US) Department of Defense (DoD) Central Test and Evaluation Investment Program (CTEIP) project to enable interoperability among ranges, facilities, and simulations in a timely and cost-efficient manner, as well as to foster reuse of range assets and future software systems. TENA provides for real-time software system interoperability, as well as interfaces to existing range assets, Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems, and simulations. TENA has also been selected for use in Joint Mission Environment Test Capability (JMETC) events, well-designed for its role in prototyping demonstrations and distributed testing. JMETC is a distributed live, virtual, and constructive (LVC) testing capability developed to support the acquisition community during program development, developmental testing, operational testing, and interoperability certification, and to demonstrate Net-Ready Key Performance Parameters (KPP) requirements in a customer-specific Joint Mission Environment (JME).Through its persistent connectivity established on the Secure Defense Research Engineering Network (SDREN), a part of the Global Information Grid (GIG), JMETC provides readily available connectivity to the Services' distributed test capabilities and simulations, as well as industry test resources. JMETC is also aligned with the Joint National Training Capability (JNTC) integration solutions to foster test, training, and experimental collaboration. TENA provides the architecture and software implementation and capabilities necessary to quickly and economically enable interoperability among range systems, facilities, and simulations. TENA also fosters range asset reuse for enhanced utilization and provides compos-ability to rapidly assemble, initialize, test, and execute a system from reusable, interoperable elements. Because of its field proven history and acceptance by the range community, TENA provides a technology already being deployed in the US Department of Defense, and being used by Coalition partners as well. This tutorial will inform the audience as to the current impact of TENA and JMETC on the Test, Training, and Evaluation community; and its expected future benefits to the range community and the warfighter.

TUESDAY, FEBRUARY 24TH

Workshop Opening Plenary Session

8:00 a.m. Opening Remarks – **Ms. Chris Susman**, SURVICE Engineering Company

8:15 a.m. Opening Keynote - **Mitch Crosswait, PhD**, Deputy Director, NetCentric, Space and Missile Defense Systems, DOT&E

8:45 a.m. Featured Speaker – **Steve Hutchinson, PhD,** Director, Test and Evaluation, DHS

9:15 a.m. Guest Speaker – **J. Brian Hall, PhD**, Acting DASD, DT&E

9:45 a.m. Break

10:15 a.m. ***Cyber T&E of Weapons Systems, AF Short Course Overview*** - Mr. Tim Ewart, Deputy Director, A3/6, AFMC

10:45 a.m. ***Cybersecurity T&E Lessons Learned*** - Mr. Pete Christensen, TRMC

Noon Lunch

Requirements and Special Topics Special Session

Session Chair: **Mr. Jason Seilback**

1:30 p.m. ***Requirements Translation*** - COL Steve Rehn and Mr. Russ Fenton, Cyber COE

2:00 p.m. ***Self-Cleansing Intrusion Tolerance: A Unique Approach to Reduce the Impact of Data Breaches*** - Arun Sood, PhD, Professor Computer Science, George Mason University, and SCIT Labs, Director International Cyber Center, Founder and CEO

2:30 p.m. ***T&E of Weapon System Cyber Security Capabilities*** - Darryl Ahner, PhD, and Bill Rowell, PhD, STAT in T&E Center of Excellence

3:00 p.m. ***Hacking Demonstration*** - Din Cox, PhD, Founder/CEO, Gaugon Labs

---

4:00 p.m. Networking Reception

WEDNESDAY – MARCH 29TH

Workshop Plenary Session

8:00 a.m. Technical Track Sessions Overview – **Jeff McNeil, PhD**

8:15 a.m. Keynote Address - **Mr. Derrick Hinton**, Director, TRMC

8:45 a.m. **T&E Current Activities and Future Vision Panel**

Moderator: **Mr. Peter Christensen**, Director, National Cyber Range

Panelists:
Mr. Giorgio Bertoli, CERDEC
Mr. Christian Riddle, NAVAIR
Mr. Dave Havrin, MCSC
Mr. Anthony Castanares, U.S. Army Research Laboratory
Mr. Terry Murphy, DHS
Ms. Sarah Standard, Cybersecurity/Interoperability Technical Director, DASD DT&E

10:00 a.m. Break

Technical Track Sessions

	Testing Track 1A	**Testing Track 2A**
Session Chair	**Jeff McNeil, PhD**	**Bruce Einfalt**
10:30 a.m.	***GPS Newest Operational Control Segment -*** Mr. Mark Bradbury, Raytheon	***Vetting Commodity IT Software and Firmware (VET) Program*** - Ray Richards, PhD, DARPA
11:00 a.m.	***Financial Sector Overview of Cybersecurity Testing -*** Mr. Timoetel Greaves, Chief, Capital Programming and Mr. Joshua Annan, Assistant Contract Administrator, Maryland Transit Administration	***Army Training Perspective*** - COL Eric Aslakson, US Army Cyber School
11:30 a.m.	***Use of TENA to Propagate Standard Cyber Effects in Testing*** - Mr. Ryan Norman, TRMC	***Redefining the Insider Threat*** - COL Monti Knode, TRANSCOM

Noon Lunch

Technical Track Sessions

	Testing Track 1B	**Testing Track 2B**
Session Chair	**Jason Seilback**	**Paul Dailey, PhD**
1:30 p.m.	***T&E Lessons Learned in Cybersecurity -*** Mr. Jerry Hancock, FAA	**ICS Testing Panel** Moderator - **Mr. Daryl Haegley**, DASD EI&I **Panelists:** **Mr. Chad Hartman**, Bechtel **Mr. Zachary Benz,** Sandia National Lab **Ms. Katy Bragg**, Pacific NW National Lab
2:00 p.m.	***Cyber Exercise Program: DHS CYBERSTORM -*** Mr. John Foti and Mr. Gary Benedict, DHS	
2:30 p.m.	***NIST CCoE*** - Mr. Zach Furness, MITRE	***Challenges in CEMA Testing*** - Mr. Anthony Castanares, ARL

3:00 p.m. Break

Technical Track Sessions

	Testing Track 1C	Testing Track 2C
Session Chair	**Jason Seilback**	**Bruce Einfalt**
3:30 p.m.	**Commercial Test Capabilities Panel** Moderator - **Chip Ferguson, TRMC** **Panelists:** **Ms. Katie Pehrson**, Bechtel **Mr. Patrick Lardieri**, Lockheed Martin **Mr. Randy Smith**, Boeing **Mr. Mark Bradbury**, Raytheon **Paul Dailey, PhD, CTEP**, JHU APL	***Formal Methods for Cyber Vulnerability Testing*** - Messrs. Neil Brock, Mike Aucoin, and Arch Owen - Draper Lab
4:00 p.m.		***NIE/AWA Cyber Security Challenges and Successes*** - COL Dave Wellons, (USA, Ret), Deputy Director Integration Test and Evaluation Directorate, OTC
4:30 p.m.		***Automated Attack Framework for T&E*** - Mr. Andrew Shaffer, ARL/PSU

THURSDAY – MARCH 30TH

Workshop Plenary Session

8:00 a.m. Technical Track Sessions Overview – **Mr. Rob Laughman**

8:05 a.m. Keynote Address - **Mr. Medhat Abunhantash**, Deputy Director, CECOM, SEC

8:30 a.m. Featured Speaker – **Joe Nichols, PhD,** Technical Advisor, Air Force Test Center

---

Cloud/IT Special Session A

Session Chair: **Mr. Pat Thompson**

9:00 a.m. ***Application Security: On Premises and in the Cloud*** - Din Cox, PhD, Founder/CEO, Gaugon Labs

9:30 a.m. ***ICS Security Monitoring*** - Mr. Moses Schwartz, Bechtel

---

10:00 a.m. Break

Cloud/IT Special Session B

Session Chair: **Mr. Rob Laughman**

10:30 a.m. ***Lessons Learned and Tools for Use in Testing Secure Cloud Providers*** - Duane Wilson, PhD, Wilson Innovative Solutions LLC

11:00 a.m. ***Considerations for Test and Evaluation in the Cloud*** - Mr. Chris Goldberg, Architect, Federal Infrastructure Managed Services, IBM Global Business Services

11:30 a.m. ***Microsoft's Cyber Defense Operations Center*** - Mr. Marek Jedrzejewicz, Microsoft

---

Noon Lunch

Technical Track Sessions

	Analysis Track 1A	**Analysis Track 2A**
Session Chair	**Jeff McNeil, PhD**	**Bruce Einfalt**
1:00 p.m.	***Cyber DT Lessons Learned -*** Paul Dailey, PhD, CTEP, JHU APL	**OTA Panel** Moderator - **COL Scott Brooks**, AEC **Panelists:** **COL Matt Magness**, AFOTEC **Mr. Patrick Valentia**, MCOTEA
1:30 p.m.	***Cyber Risk Assessment Process and Methods -*** Mr. Tom Llanso, JHU APL	
2:00 p.m.	***Shift Left: Putting the Process into Action -*** Mr. Patrick Thompson, AEC	***Cyber Situational Awareness Capability: Using APL Toolset*** - Mr. Keith Wichmann, JHU APL

2:30 p.m. Break

Technical Track Sessions

	Analysis Track 1B	**Analysis Track 2B**
Session Chair	**Chris Susman**	**Duane Wilson, PhD**
3:00 p.m.	***Big Data Analysis Tools*** - Norman Smith, PhD, President, Consulting Services, Energy Rising International	***Cybersecurity Perspective on Sustainment Issues*** - Mr. Carl "CJ" Akridge, AEC
3:30 p.m.	***Resilince for Weapon System Cyber Defense*** - Ms. Rose Daley, JHU APL	***Computer Network Defense Service Provider*** - Duane Wilson, PhD, Wilson Innovative Solutions LLC
4:00 p.m.	***Army Cyber Survivability: Shift Left Progress*** - Mr. Rob Laughman, AEC	***Cybersecurity vs Cyber Survivability: A Paradigm Shift*** - Mr. Mike Landolt, AEC

Workshop Plenary Session

4:30 p.m. Closing Keynote Address – **C. Dave Brown, PhD, CTEP**, formerly DASD DT&E

ABSTRACTS

Cybersecurity vs Cyber Survivability: A Paradigm Shift

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.”

DECRE C2IS V&V Report

By Mr. Randy Coonts - Joint Staff J6, DDC5I, Integration and Interoperability Division, C4/Cyber Integration Branch

This report documents the Validation and Verification (V&V) of the DoD Enterprise Cyberspace Range Environment (DECRE) Command and Control Information Systems (C2IS) environment for Cybersecurity Test and Evaluation, provides a capability and limitations analysis, and recommends courses of action for improvement and investment. The approach is to V&V the DECRE C2IS environment for operational realism using USPACOM architectures to emulate the command and control (C2) and security structure, and to leverage Joint Interoperability Test Command’s (JITC) Test Plan elements and tasks. Methods of analysis include mission task/use case analysis for operational realism, data flow analysis, and analysis of instrumentation to enable quantitative decision quality data. Results of the analysis demonstrate the operational realism of the DECRE C2IS environment. DECRE C2IS is a persistent, distributed environment with IS and C2 systems to provide support to Program Managers, Developers, and Operational Test Agencies (OTA). The DECRE C2IS partnership integrated their separately developed capabilities into a robust, operationally realistic representation of the DOD Information Network (DODIN) interconnecting joint Combatant Command (CCMD) nodes and C2 enclaves with accompanying C2 and information systems (IS), applications and services. DECRE C2IS is able to build a realistic environment emulating USPACOM architectures with the Global Command and Control System-Joint (GCCS-J), version 4.3.0.0 as the System Under Test (SUT), with critical interfaces, critical data exchanges, defense-in-depth, and any Risk Management Framework-identified vulnerabilities. As a readily available cyber range capability, the DECRE C2IS can tailor the current system of systems environment to support (1) Commanders with 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 that can be synchronized with Combatant Command exercises; and (3) Program Managers, Developers, and OTAs with a tool for assessing the effectiveness of security controls, Cooperative Vulnerability Assessments (CVA), Penetration Testing, Adversarial Assessment, interoperability, integration, and implementation in an operational environment.

Formal Methods for Cyber Vulnerability Testing

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

New methods and tools are required to provide more effective and more thorough cyber-testing than is available in today’s testing repertoire. The traditional cyber-testing process has two key elements: code inspection with tools like HP Fortify and “live” cyber-range testing. Although these are valuable tools for what they were designed to do (i.e. checking for vulnerability to potential or known attacks), these two standard “tools” are not well suited for doing the following: Testing for, and identifying, vulnerabilities not contemplated within software inspection tools, and range testing processes (i.e. “Day Zero” vulnerabilities); Testing for and identifying potential “composition” vulnerabilities when composing higher-level systems, from tested/validated subsystems; and, Efficiently assessing system vulnerability/resiliency to different (sub)system compromises. Working with a number of Universities, Draper has begun developing testing tools and infrastructure using Formal Methods, which have the potential to provide these sorts of cyber-testing capabilities. Formal Methods have been researched in academia for many years but have, to date, had limited application to industrial scale software due to factors such as scalability. Recently however, academic Formal Methods capabilities have become sufficiently capable such that early shortfalls are being overcome. As such, many researchers have started to explore using Formal methods as a means to implement software with guaranteed functionality. Often overlooked however, is the possibility of using Formal Methods not for software development, but for software/cyber testing. Early research shows that Formal Methods might be used to do cyber-testing for issues such as, but not limited to: Identifying Day-zero vulnerabilities; Assessing vulnerability to selected side-channel attacks; Identifying vulnerabilities created when secure sub-systems are integrated into higher level, more complex systems: e.g. what vulnerabilities might be created when integrating radios, sensors, networking, etc.; Leveraging cyber-testing of sub-systems to attest to their security, as part of a cyber-test of a higher-level system build on these attested sub-systems; and, Testing system vulnerability/resiliency to classes of compromises. Academia has started to develop these sorts of Formal methods based vulnerability assessment tools, but these academic tools all use specialty programming languages developed by academia, specifically to enable Formal methods proofs. Working with these institutions, Draper has begun developing translators that convert a variety of system instantiations (e.g. binary, source code, UML representations, …) into these Formal Methods representations, and developing the means to evaluate the resulting Formal Methods representations for specific vulnerabilities.

NIE / AWA Cyber Security Challenges & Successes

By COL Dave Wellons (USA Ret), Deputy Director Integrated Test & Evaluation Directorate – USAOTC

Based upon the Department of Defense's emphasis on realistic cyber security testing during operational test events, it is important to learn from cyber testing conducted during Network Integration Evaluations and Army Warfighting Assessments. Each of these event provides the test community an opportunity to learn from offensive and defensive cyber activities that occur during operational testing of DoD oversight program of record systems. This presentation will provide an overview of the NIE/AWA threat environment, including electronic and cyber threats, as an example of the baseline threat integration required during planning and execution of brigade sized operational tests and experimentation events in today's complex threat environment. After sharing the baseline threat environment, the presentation will focus on the cyber preparations by the CVPA team (Blue Team), the player unit and the Cyber Protection Teams (Green Team) in order to harden the network in preparation for force on force execution. My intent is to share success stories and challenges found in the NIE/AWA environment to help other test communities prepare for similar cyber / threat test events. Upon completion of the preparation phase, we will discuss unclassified trends and lessons learned from NIE/AWA execution from BLUFOR, OFPOR and Test community perspectives. Key highlighted areas include planning TTPs, rules of engagement, target approval process, unclassified OPFOR cyber mission effectiveness reporting and "tech on tech" forums used to share cyber successes within the community. The overall goal of this presentation is to share trend information and lessons learned about cyber testing execution conducted during brigade sized operational tests in a realistic threat environment in order to help the test community plan, coordinate and execute successful cyber test events that meet DOT&E requirements and improves the warfighter's cyber posture against real world threats.

Self-Cleansing Intrusion Tolerance: 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. It can be argued that overreliance on detection is unwise. Perfect detection is technically impossible, and failures lead to huge losses. 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 is rapidly changing. It is time to accept that some level of intrusion is inevitable and hackers will get in. Once a system is hacked, it remains in control of the intruder and provides easy access to spread malicious software and cause extensive damage, to include data theft. In widely reported breaches, intruders installed infections that stayed inside the system for months. If criminals are likely to breach the systems, perhaps a new solution is building an extra layer of defense that shifts the target by reducing the duration of the failure, thus reducing the amount of data lost. So if you are willing to accept the inevitability of intrusion, the goal is no longer to eliminate the vulnerabilities, but to make it extremely difficult for the attacker to exploit them. 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 requirements), these servers are rotated from cold to hot state and during the cold state, the server is rebuilt to the pristine configuration. What this does is that 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. Thus, that server becomes a moving target. Another advantage of this rotation is the ability to rotate the infected server to quarantine, then analyze the infection in a systematic and timely manner without impacting the overall performance of the system. Such an analysis can provide information on type of infection, hacking types, etc., and its knowledge can be leverage by preventive techniques. In summary, SCIT is a new approach for industry, governmental, and other institutions to reduce or potentially eliminate costly data breaches on an ongoing basis.

SHIFT LEFT: A Hypothetical Approach to building Cybersecurity into a Program

By Mr. Patrick Thompson - 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 more costly, means to mitigate issues after a finalized design and material investment in hardware.

T&E of Weapon System Cyber Security Capabilities

By Darryl Ahner, PhD, and Bill Rowell, PhD - STAT in T&E Center of Excellence

Until fairly recently US military forces were viewed as performing operations in support of campaign objectives in four physical domains (land, maritime, air, and space). As its critical importance to achieving campaign objectives became evident, the cyberspace domain was added. Cyberspace is the manmade domain and information environment we create when we connect together all computers, wires, switches, router, wireless devices, satellites and other components that allow us to move large amounts of data at very fast speeds. Cyberspace operations are those operations conducted in cyberspace with the objective of providing friendly freedom of maneuver in cyberspace and projecting power in and through the domain in support of campaign objectives. We will not be focusing on the capability of a weapon system to perform cyberspace operations but rather on the capability of the weapon system while performing its assigned missions to protect, detect, respond and recover when attacked by the expected cyber threats in the expected operating environment, that is, its resiliency. Acquisition of DoD weapon systems is undeniably a challenging process involving an almost endless array of constraints and requiring a highly skilled workforce of dedicated people. However, with the growing cyber threat and its tremendous potential for serious impact on weapon system mission accomplishment the weapon system acquisition process has become even more daunting. Tackling this challenge, DoD leadership has correctly decided that it is better in the long run to build cyber security capability into a weapon system as an integral part of the acquisition process rather than to bolt it on the weapon system or test it into the weapon system after development is complete. Because of the pervasive and highly technical nature of cyber security, this decision has affected all elements of the acquisition process especially T&E (activities, workforce skills, resources,). This presentation will: Clarify the relationship between cyberspace operations and weapon system cyber security; Describe T&E weapon system acquisition process changes, workforce development initiatives, and infrastructure improvements triggered by integrating cyber security capabilities into the weapon system acquisition process; Offer detailed instructions on Drafting capability-based cyber security requirements (Capability Development Document (CDD)) and Translating capability-based cyber security requirements into system requirements that can be put on contract (System Requirements Document (SRD)).

SPEAKER BIOGRAPHIES

Mr. Medhat A. Abuhantash was assigned as Acting Director of the US Army CECOM Software Engineering Center (SEC) in November 2015 after serving as Deputy Director since November 2013. In this role he leads SEC's efforts to provide state of the art software engineering products and services throughout the Army and DoD. SEC supports more than 400 systems/programs from command, control, communications, computers, intelligence, surveillance and reconnaissance to logistics, business and enterprise systems all in the modern digital environment. He oversees SEC's five directorates, insuring effective integrated mission accomplishment by a global organization of over 3,000 military, civilian and industry employees, with an annual budget in excess of $600 million. His previous assignment was Director of SEC's Enterprise Services Mission Area (EMA), leading over 1200 government and contractor personnel providing software engineering, cyber security, infrastructure, field support, and software related product and services enabling the success of the command, our customers, stakeholders and SEC with emphasis on efficiencies, effectiveness and software-business transformation. The EMA core mission services included Cyber Security; Replication, Distribution, Installation & Training; Software Control & Reference Office; Centralized Acquisition & License Management; Business Intelligence; Data Center Services; and management and execution of worldwide Field Support for tactical, logistics, business and retail systems. He formulated plans with a focus on corporate opportunities for enterprise synergy, effective and efficient business operations and processes, program integration, strategic initiatives and corporate Information Technology solutions. His prior assignments include Deputy Director of SEC's Intelligence, Surveillance and Reconnaissance Directorate, coordinating Life Cycle Software Support programs providing functionally survivable, interoperable, logistically supportable and cost effective software for Mission Critical Defense Systems; Project Leader for the Digital Topographic Support System (DTSS) providing oversight for software maintenance and development of the DTSS including Integrated Meteorological and Source Analysis Systems; and Division Chief for Intelligence Fusion Systems, leading an organization of 40 DA Civilian personnel and over 400 government contract personnel operating in 74 locations worldwide. Mr. Abuhantash also served a developmental assignment as the Deputy Commander for the SEC Fort Belvoir office, supporting the commander with day-to-day management and mission execution providing enterprise solutions through information technology products, support and services. Mr. Abuhantash is a graduate of the Kennedy School of Government at Harvard University and the Senior Service College Fellowship. He holds a B.S. in Industrial Engineering, a Masters in Software Engineering, is an Acquisition Corps member, certified level III in Systems, Planning, Research, Development and Engineering, and Computer Engineering, and is fluent in Arabic. His awards include the Army Materiel Command Outstanding Leadership Award, DA Commander's Award for Civilian Service (twice awarded) and the DA Achievement Medal for Leadership. Most notably, Mr. Abuhantash was selected as one of the Twelve Outstanding C4ISR Personnel for the newly created CECOM Life Cycle Management Command in 2004.

Colonel Scott D. Brooks was commissioned a Second Lieutenant and earned a Bachelor of Arts Degree in Biology and Psychology from Western New England College in 1992. Under the Branch Detail Program, Colonel Brooks served three years as an Infantry Officer before becoming a Signal Officer. His military schooling includes the Infantry Officer Basic Course, Airborne School, Ranger School, Jumpmaster School, Signal Officer Branch Qualification Course, Signal Officer Advanced Course, Combined Arms and Services Staff School, Resident Command and General Staff College, and the Army Force Management Course. He also holds a Master's Degree in Management from Webster University. Some of Colonel Brooks' previous assignments include Contingency Communications Package Platoon Leader, Charlie Company and Battalion Assistant S3, 51st Signal Battalion (Airborne), Fort Bragg, North Carolina; Battalion Assistant S-3, 10th Signal Battalion, 10th Mountain Division (Light Infantry), Fort Drum, New York; Commander, Foxtrot Company, 369th Signal Battalion and Commander, Bravo Company, 442nd Signal Battalion, 15th Signal Brigade, Fort Gordon, Georgia; Battalion S6, 1st Battalion, 15th Field Artillery, 2nd Infantry Division, Camp Casey, Korea; Brigade S6, 2nd Aviation Brigade, 2nd Infantry Division, Camp Stanley, Korea; S6, Division Artillery, S6, 1st Brigade Combat Team, Deputy G6, and Division Network Support Company Commander, 10th Mountain Division (Light Infantry), Fort Drum, New York; Chief, Force Requirements Branch, Concepts, Requirements and Doctrine Division, Fort Gordon, Georgia; Commander, 369th Signal Battalion, Fort Gordon, Georgia; and Technical Integration Chief for Command, Control, Communications and Computers Assessments Division, Joint Staff J6, Suffolk, Virginia. Colonel Brooks currently serves as Director, Survivability Evaluation Directorate, Army Evaluation Center, Aberdeen Proving Grounds, Maryland.

C. David Brown, PhD, **CTEP,** is the former Deputy Assistant Secretary of Defense for Developmental Test & Evaluation (DASD(DT&E)) and former Director, Test Resource Management Center (TRMC). As the DASD(DT&E), he serves as the principal advisor on developmental test and evaluation to the Secretary of Defense (SECDEF) and the Undersecretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)). Dr. Brown is responsible for DT&E policy and guidance in support of the acquisition of major Department of Defense (DoD) weapons systems, and providing advocacy, oversight, and guidance to the DT&E acquisition workforce. In Dr. Brown's role as Director, TRMC he advises the SECDEF and USD(AT&L) on matters pertaining to the DoD's Major Range and Test Facility Base (MRTFB), the Nation's critical range infrastructure for conducting effective test and evaluation (T&E). Additionally, he reviews and certifies proposed T&E budgets of Military Departments and Defense Agencies, administers the Central Test and Evaluation Investment Program (CTEIP), and oversees the DoD program for T&E science and technology. Prior to his appointment in September of 2013, Dr. Brown was a consulting engineer for the MITRE Corporation and the Institute for Defense Analyses in the areas of DoD program management, systems engineering, and test and evaluation. He was also an adjunct professor and still teaches graduate courses in program management and systems engineering for Johns Hopkins University. He previously served as the Director of the Combined Test Organization and Executive Director for Test for the Army Future Combat Systems (FCS) program where he was responsible for planning and overseeing the testing and evaluation for this multi-billion-dollar revolutionary development program. Before working on the FCS program, Dr. Brown was the Director for Test and Technology for the Army Developmental Test Command,

where he oversaw the management of more than 1700 tests annually, technical operations at five of the DoD MRTFBs and six associated test sites, and an annual budget of over $450 million in investment in test support and test technology development. Dr. Brown was also the focal point for the Army's application of modeling and simulation techniques to technical test and evaluation, including the development of the Virtual Proving Ground, the Army's multi-million dollar, multi-year virtual testing program. He has also been a test instrumentation engineer, test director, test manager, and an active Army Signal Corps officer in various leadership positions. Dr. Brown became a member of the Senior Executive Service in 1999, holds two patents, and has authored numerous technical papers. He is a registered Professional Engineer, was a member of the Army Acquisition Corps, and is a retired Army Reserve Colonel. He has a PhD in electrical engineering from the University of Delaware, and a MS in National Resource Strategy from the National Defense University Industrial College of the Armed Forces. He is an active member of the International Council on Systems Engineering and the International Test and Evaluation Association.

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.

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.

Paul Dailey, PhD, CTEP, Senior Staff, Johns Hopkins University Applied Physics Lab (JHU/APL) is the supervisor of the cyber mission operations group at the Johns Hopkins Applied Physics Lab in Laurel, MD. His current work and research focuses on cybersecurity T&E for mission systems and cybersecurity technology integration. He coordinates cyber T&E efforts within APL and teaches an internal class on the subject. He also has past experience working test and evaluation for the Department of the Navy and General Electric appliances. Mr. Dailey has more than 13 years' experiences in systems engineering and test and evaluation (T&E) supporting Defense, Homeland Security and commercial programs. He is a graduate of the U.S. Naval Postgraduate School with a Ph.D. in Software Engineering and a M.S. in Systems Engineering and a graduate of the University of Louisville with a B.S. in Electrical Engineering. Currently, he primarily supports multiple cyber-related T&E efforts at JHU/APL and teaches a course on cyber systems T&E in APL's Strategic Education program.

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.

Mr. Chris Goldberg, is a Chief Architect, Managed Services and Cloud Solutions, IBM US Public Sector. Chris is a 15-year veteran of the public sector IT space with a background in infrastructure architecture, cloud computing, cybersecurity, and managed service implementation. In his current role as chief architect for IBM's public sector managed services and cloud solutions organization, Chris has led the technical strategy, design, implementation, and operation of three different federally accredited IBM cloud environments. In previous roles, Chris has served as both a lead architect and systems engineer in support of several different US federal civilian and Department of Defense clients. Prior to joining IBM, Chris was a Signal officer in the US Army, focusing on both garrison and tactical systems. Chris is a graduate of The Ohio State University with a degree in computer science and currently lives in Colorado with his wife and four daughters.

Mr. G. Derrick Hinton is a member of the Senior Executive Service with a 25-year civilian career in the Department of Defense (DoD). In his current role as the Principal Deputy Director, Test Resource Management Center (TRMC) within the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics [USD(AT&L)], Mr. Hinton is the principal staff assistant and advisor to the Director, TRMC for all matters pertaining to assessment of and strategic planning for the Major Range and Test Facility Base (MRTFB); these responsibilities include annual certification of the Military Department and Defense Agency Test and Evaluation (T&E) budgets and development of the Congressionally-directed biennial Strategic Plan for DoD Test and Evaluation Resources. In addition, he oversees the management of the Central Test and Evaluation Investment Program (CTEIP), the Test and Evaluation/Science and Technology (T&E/S&T) Program, and the Joint Mission Environment Test Capability (JMETC) Program, whose annual budgets collectively total over $300M; and the National Cyber Range (NCR). Mr. Hinton began his career serving in the United States Marine Corps Reserve from 1985 to 1991, entering the DoD civilian workforce in 1989 as a Test Engineer responsible for munitions T&E with the 46th Test Wing at Eglin Air Force Base, FL. In 1996, Mr. Hinton joined the AT&L team, initially serving in the Office of the Director, Test, Systems Engineering, and Evaluation. He transitioned to the Office of the Director, Operational Test and Evaluation (DOT&E) in 2001 and joined the Test Resource Management Center (TRMC) in 2005, taking on the role of Principal Deputy Director, TRMC in 2009. During his tenure with AT&L, Mr. Hinton has made significant contributions to policy and T&E investment programs. While dual-hatted as Program Manager for CTEIP and the T&E/S&T Program, he executed a combined annual budget of approximately $200M, led management of all instrumentation development efforts sponsored by TRMC, and held responsibility for maturing and transitioning technology to enhance the overall DoD T&E capability. Mr. Hinton successfully ensured the use of a corporate investment approach to combine Service and Defense Agency T&E needs, thereby maximizing opportunities for Joint and multi-Service efforts and eliminating unwarranted duplication of test capabilities across the MRTFB. Mr. Hinton holds a Bachelor of Science in Industrial Engineering from the University of Alabama, a Masters of Public Administration, and an Acquisition Core Level III Certification in Test and Evaluation from the Defense Acquisition University. He serves as co-chair of the Range Spectrum Requirements Working Group, which develops policies to mitigate radio frequency spectrum encroachment at MRTFB activities. Moreover, he is the principal staff assistant for all Science, Technology, Engineering, and Mathematics activities across DT&E and TRMC.

Mr. Gene Hudgins works for KBRWyle as Director of Test and Training Environments and supports the Test Resource Management Centers' (TRMC) Test and Training Enabling Architecture (TENA) Software Development Activity (SDA) and Joint Mission Environment Testing Capability (JMETC) as the lead for the TENA and JMETC User Support Team. Since October 1998, the Central Test and Evaluation Investment Program (CTEIP) has overseen the development of the TENA – which drastically improves range interoperability and resource reuse among DoD range systems, facilities, and simulations. As a key member of the TENA SDA and JMETC Program Office, Gene is responsible for Distributed Event Coordination, Design, and Integration. Gene also manages TENA training and Range Commanders Council coordination. Gene is an active member of the International Test and Evaluation Association (ITEA) and currently serves as Vice President on the Executive Committee of the ITEA National Board of Directors (BOD). Prior to this work for the TRMC, Gene worked on Eglin AFB as an Instrumentation Engineer and Department Head. Gene has a Bachelor's Degree in Electrical Engineering from Auburn University (War Eagle!), a Master's Degree in Electrical Engineering from the University of Florida (Go Gators!), and an MBA from the University of West Florida.

Steven J. Hutchison, PhD, assumed duties as Director of Test and Evaluation in the Department of Homeland Security in December 2013. Dr. Hutchison served as the Principal Deputy, Developmental Test and Evaluation from October 2011 to December 2013. He served as the Acting Deputy Assistant Secretary of Defense for Developmental Test and Evaluation and Acting Director, Test Resource Management Center from January 2013 to September 2013. Dr. Hutchison served as the Test and Evaluation Executive for the Defense Information Systems Agency (DISA) from August 2005 to October 2011, where his role was to oversee the test, evaluation, and certification activities of the Joint Interoperability Test Command (JITC) and ensure robust test services in support of DISA's acquisition of critical command and control capabilities. Dr. Hutchison served in the office of the DoD Director, Operational Test and Evaluation from 2004 to 2005, and was Assistant Technical Director and evaluator in the Army Test and Evaluation Command from 1998 to 2004. Dr. Hutchison retired from the US Army in 2002. His military career highlights include assignments with the 82nd Airborne and 3rd Infantry

divisions, Assistant Professor in the Department of Mathematics at the United States Military Academy, and his assignment to ATEC. Dr. Hutchison was commissioned as an Infantry officer in 1982. Dr. Hutchison graduated from the United States Military Academy, earned a Master of Science in Operations Research at the US Naval Postgraduate School, and received a Ph.D. in Industrial Engineering from Purdue University.

Mr. Marek Jedrzejewicz is a Principal Security Engineering Manager for the Microsoft Cyber Defense Operations Center where he runs the security monitoring threat detection program across Microsoft's Cloud Services. Marek's role is to help detect threats and potential threats from the trillions of signals received from events and logs across thousands of services and millions of devices so that they can be addressed and removed as quickly as possible. With Microsoft for 15 years, Marek has influenced many areas within networking and security. Marek holds a CISSP, and a Bachelor's degree from California State Polytechnic University.

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).

Mr. Rob Laughman, CISSP, Cybersecurity Technical Director, Survivability Evaluation Directorate, AEC. Mr. Laughman is the Technical Director for Cybersecurity in the Survivability Evaluation Directorate (SVED) of the Army Evaluation Center, and a Certified Information Systems Security Professional (CISSP). Mr. Laughman advises on technical aspects of cybersecurity for the Combatant Command Cybersecurity Task Force and Program of Record evaluations with respect to cybersecurity. He has over 33 years of Federal Service, 10 years in Test and Evaluation, 1 year at RCA working power semiconductors, 4 years at Project Manager Smoke working sensor system impacts of aerosols, 3 years at the Army Research Lab, Survivability Lethality Analysis Directorate working countermeasures effects on smart munitions, and 15 Years at the Army Evaluation Center (AEC) of the Army Test and Evaluation Command. He was selected for the DoD Defense Leadership and Management Program in 2007. Mr. Laughman graduated from the Army War College in 2010 and served a developmental assignment in Office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology from July 2010 to July 2011. He holds a BS in Ceramic Science and Engineering from the Pennsylvania State University, an MS in Strategic Studies from the Army War College and MBA from Drexel University with a concentration in Engineering Management. Mr. Laughman is a member of the acquisition corps, level three certified in Test and Evaluation and level two certified in Engineering.

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.

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

Joe Nichols, PhD, is the Technical Advisor for Flight Test and Evaluation, Air Force Test Center, Edwards Air Force Base, California. He is the senior technical advisor regarding the health and suitability of airframe, avionics, installed propulsion, cyber, and electronic warfare test capability across Air Force Test enterprise. Dr. Nichols served for 26 years as an Air Force officer. During this military career he served as a flight test engineer, test squadron commander and test group commander. He has conducted research into the control and testing of autonomous systems, and led the recent reorganization of the airworthiness process for Air Force test aircraft. He is also the architect of the cyber T&E infrastructure roadmap. Dr. Nichols was appointed a Senior Leader executive in October 2013. He is a graduate of the USAF Test Pilot School and a member of ITEA.

Raymond "Ray" Richards, PhD, joined DARPA in January 2016. His research interests focus on high assurance software and systems. Dr. Richards joined DARPA from Rockwell Collins Advanced Technology Center (ATC) where he led a research group focused on automated analysis, cyber, and information assurance. In this role he helped foster the industrial use of formal methods verification to support security accreditations. Dr. Richards holds Master of Business Administration, Doctor of Philosophy and Master of Science degrees in electrical and computer engineering, as well as a Bachelor of Science degree in electrical engineering, all from the University of Iowa. He has nine publications in the area of formal methods/software security analysis and one patent.

The ITEA Journal of Test and Evaluation Themes for 2017

Please consider writing an article, share this document with coworkers, and provide feedback on the themes. For all themes in 2017-2019, please check the ITEA website at www.itea.org under "SHARE" and "Publications." – Steve Gordon

2017 ITEA Journal Themes

Training the Future T&E Workforce
(Issue 38-2, June 2017)

Test and evaluation over the next decade will need a workforce of professionals from many academic disciplines. The academic majors will certainly include science, technology, engineering, and math (STEM); yet management, communications, psychology, and other types of majors also may be needed for the T&E profession. We will need a steady supply of the right academic majors from our technical schools, colleges, and universities, and we will need initial training for the incoming workforce to be ready to become T&E professionals. The need for an inflow of new talent suffers from a constrained supply and competes with many demands for the same disciplines from industry, academia, and other parts of the government. Increasing the throughput of the right new talent would help considerably. And, innovative ways to attract the new workforce, provide recurring training to the existing workforce, and fund career enhancement will help T&E retain the workforce needed.

(Manuscript deadline: March 1, 2017)

T&E of Cyber Security and Readiness
(Issue 38-3, September 2017)

Key information passed through network connections improves the speed and lethality of combat operations; yet use of the networks opens the door to vulnerabilities. Network connections for home computers, smart phones, social media, and entertainment add enjoyment; yet ease of use often equates to increased ease of misuse and scamming. Systems that support the military, our finances, our health records, and our other personal information must pass information assurance, information security, net readiness, and cyber readiness tests. Yet these tests, when passed, do not provide 100% assurance of protection. Systems and the networks that connect them are subject to all sorts of attacks from all sorts of sources; however, the goal of the attack is nearly always to take something valuable. Money, personal information, trust, freedom, military information and plans, or intellectual property are often taken with very minimal effort and cost. How much testing is required to provide an acceptable level of protection to expected attacks? How do we predict future possible attacks?

(Manuscript deadline: June 1, 2017)

T&E for Enhanced Security
(Issue 38-4, December 2017)

This issue seeks articles about testing for enhanced security in the land, sea, air, space, and cyber domains. The theme includes testing by homeland security and law enforcement of systems to protect water, power, natural gas/petroleum, food, pharmaceuticals, transportation, and communications processing and distribution systems. The United States National Guard, the Department of Homeland Security, and State homeland security components have unique testing needs and experiences, and articles on these topics are encouraged. How do the Federal Aviation Authority and the National Aeronautics and Space Administration collaborate on testing the nation's airspace? How are robotic vehicles tested? Articles from international partners are also encouraged in these listed areas and in the areas of national defense and homeland security.

(Manuscript deadline: September 1, 2017)

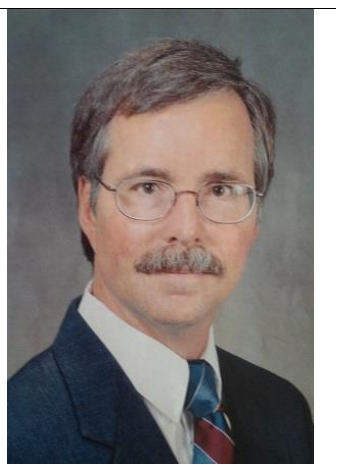
2018-2019 Themes of The ITEA Journal of Test and Evaluation

2018	39-1	March	Testing Using Facilities Around the World
	39-2	June	Unmanned and Autonomous Vehicle Testing
	39-3	September	Test and Evaluation of Hypersonic Systems
	39-4	December	Advanced Instrumentation and Information Systems Technology for T&E
2019	40-1	March	Statistical Methods in T&E
	40-2	June	T&E for Cyber Security and Readiness
	40-3	September	The Right Mix of T&E Infrastructure
	40-4	December	Training the Future T&E Workforce

Mr. Lee Rossey co-founded SimSpace in 2015 with a core team of developers and cyber professionals that had previously worked together alongside the other co-founders in a national defense capacity. Since 2000, Lee served in increasingly more responsible roles at MIT's Lincoln Laboratory (MIT LL), including most recently as Group Leader for the Cyber System Assessments Group. In this capacity, Lee and his team developed tools and processes for conducting independent assessments of cyber systems and capabilities for the U.S. Government. During his tenure at Lincoln Laboratory, Lee led the establishment and growth of the Cyber System Assessment Group to become a nationally-recognized center of excellence. The Cyber System Assessment Group earned a reputation for technical excellence in cyber range development, cyber test and evaluation, cyber red-teaming and cyber exploitation. Lee's expertise provides a solid foundation to lead the development of capabilities to rapidly create and host realistic network environments and network clones, model sophisticated nation-state adversaries and develop data collection and analysis capabilities. In the area of cyber ranges, Lee led the creation, development and deployment of the LARIAT traffic generation tool and related capabilities, which are currently used and operated at the major DoD cyber ranges and numerous other government and contractor laboratories. He has extensive experience in building and leading the development teams ensuring they meet the features, fidelity and priorities for the tests and programs being evaluated. Lee holds dual degrees as a Bachelor of Science in Electrical Engineering as well as Computer Engineering from the State University of New York (Buffalo) and a Master of Science in Electrical and Computer Engineering from the University of Florida.

Bill Rowell, Ph.D., CISSP, CEH is a Senior Operations Research Consultant at The Perduco Group supporting the OSD Scientific Test and Analysis Techniques in Test & Evaluation Center of Excellence as a STAT Cyber Expert. He is a 23-year US Air Force veteran who served in positions as a test analyst, management analyst, weapon system project manager, strategic nuclear forces analyst, chief of major command Artificial Intelligence program office, chief of business process improvement office, and software technology transition officer. As an Air Force Research Associate at Harvard University's Program on Information Resources Policy he authored a book on arms control verification policy issues. Upon leaving the Air Force he held positions as a database developer, capacity and performance management engineer, and senior software engineer before joining The Perduco Group in 2016. He holds a B.S in mathematics from the US Air Force Academy, an M.S. in operations research from Stanford University, and a Ph.D. in operations research from the University of Texas at Austin.

Mr. Moses Schwartz is a security engineer and researcher on the Bechtel Computer Incident Response Team (CIRT) in San Francisco. His focus areas are industrial control system security and security software development. Prior to Bechtel, he spent six years as a researcher at Sandia National Laboratories. He holds a B.S. and M.S. in Computer Science from the New Mexico Institute of Mining & Technology.



Mr. Randall (Randy) Smith is an Associate Technical Fellow at The Boeing Company where he leads a cybersecurity assessment team within the Boeing Test and Evaluation organization. In this role, Mr. Smith brings expertise from across the Boeing Enterprise together to meet the emerging cybersecurity needs of Boeing products and services with emphasis on test. Before focusing on Test, Mr. Smith spent much of his 32-year career involved in both Boeing and DARPA-sponsored cybersecurity research in trustworthy software development, high assurance multi-level security, intrusion trace-back and autonomous response, and coordinated cyber defense. Mr. Smith was a key developer and author of the FAA's position on the security and safety issues related to on-board networks, and was involved in focused research for the Advanced Research and Development Activity (ARDA), now IARPA. When not at Boeing, Randy can be found leading a local Boy Scout troop and exploring the Pacific Northwest (and many other areas) through his geocaching activities.

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.

Duane Wilson, PhD is a subject matter expert in cyber technology research, with more than 15 years in cyber security, computer science engineering and network protection. Formerly he served as Director of Strategic Cyber Initiatives for Sabre Systems Inc., he was responsible for the ongoing maintenance of all cyber activities across the company. Duane has largely contributed to the development of multiple proposals for government entities and commercial clients including a 30-yr strategic plan for the Department of the Navy based on computer immunology, a Cryptographic Workbench solution, Bitcoin Transaction Blockchain for Privacy Identity Management, and Cyber Resiliency for Industrial Control systems and applications (via Office of Naval Research). After gaining a solid foundation in cyber security (specifically cyber defense) at the U.S. Army Research Laboratory early in his career, he went on to join the MITRE Corporation as a Senior Cyber Security Engineer, where he focused extensively on network analyst training, security/risk assessments for high value infrastructure components and security tools evaluation. Duane has contributed to the cyber security industry with the publication of multiple articles over the course of his career to include Visualization in Interrogator using Graphviz proposing the use of network graphs to address limitations in the current Interrogator Intrusion Detection System Architecture, A Discretionary Access Control Method for Preventing Data Exfiltration via Removable Devices, focused on host-level protections for thumb drives or external hard drives, and To Share or Not to Share in Client-Side Encrypted Clouds, presenting an analysis of secure cloud storage providers to identify a major flaw in the design of the sharing methodologies proposed. His last publication, From Pretty Good to Great: Enhancing PGP Using Bitcoin and the Blockchain, describes an alternative method of validating PGP certificates for using in a hosted environment – such as the cloud. Dr. Wilson holds a PhD in Computer Science from The Johns Hopkins University, a Master's of Science in Information Security from Johns Hopkins University, a Master's of Engineering in Computer Science from Cornell University and a B.S. in Computer Science from Claflin University.

NOTES

NOTES

18TH ITEA ENGINEERING WORKSHOP

System-of-Systems in a 3rd Offset Environment

Hosted by the ITEA White Sands Chapter

JANUARY 23-25, 2018
EL PASO, TEXAS

REGISTER ONLINE:
www.itea.org

This workshop will incorporate the Fundamentals of:

- Cyberspace Test Technology
- C4I and Software Intensive Systems
- Distributed Testing
- Modeling and Simulations
- Autonomous System Test
- Hypersonic System Test
- Directed Energy
- Spectrum
- Advanced Instrumentation Systems

Previous SPONSORS Include:

Alion Science and Technology
AMERICAN SYSTEMS
Booz Allen Hamilton, Inc.
CALCULEX, Inc.
Charles Stark Draper Laboratory
Command Post Technologies
EMC Corporation
EMRTC New Mexico Tech
Engility Corporation
Georgia Tech Research Institute
Jacobs Technology, Inc
KBRwyle
Kratos Technology and Training Solutions
MIRATEK Corporation
New Mexico Tech (EMRTC)
Systems Application & Technologies (SA-Tech)
The Boeing Company
TRAX International
TRIDEUM Corporation

Previous EXHIBITORS Include:

Air Academy Associates
Astro Haven Enterprises
ATAMIR WSMR
CALCULEX, Inc.
Celeris Systems Inc.
Charles Stark Draper Laboratory
EMRTC New Mexico Tech
Glacier Technologies
IDA Technology
Imprimis, Inc.
International Test and Evaluation Association
Jacobs Technology, Inc
KBRWyle
Kratos Technology and Training Solutions
L-3 Telemetry & RF Products
MIRATEK Corporation
Photo-Sonics, Inc.
Playas Training & Research Center
SAS Institute Inc., JMP Division
Scientific Research Corporation
Smartronix Inc.
Systems Application & Technologies (SA-Tech)
TDK-Lambda Americas
TENA JMETC
TEST LLC
Tigua Enterprises, Inc.
TRAX International
TRIDEUM Corporation
U.S. Army Electronic Proving Ground - EPG
U.S. Army Virtual Targets Center
U.S. Army White Sands Missile Range - WSMR
Wideband Systems, Inc.

Join Us in El Paso – Mark Your Calendars TODAY!

For information on exhibiting or sponsorships, contact Lena Moran, Phone: 951-219-4817, Email: Lmoran@traxintl.com

www.itea.org

CONNECT with ITEA to LEARN, SHARE, and ADVANCE!

ITEA CORPORATE MEMBERS

Acquired Data Solutions, Inc.	CALCULEX, Inc.	IPEV - Flight Test and Research Institute (Brazilian Air Force)	Roundtable Defense, LLC
Advanced Systems Development, Inc.	Celeris Systems	Jacobs Technology	Saalex Solutions, Inc.
Advanced Test Equipment Rentals	Command Post Technologies	Joint Research and Development, Inc. (JRAD)	Schafer Corporation
AEgis Technologies Group, Inc.	Compunetix, Inc.	JT3 LLC	Scientific Research Corporation - SRC
Agency for Defense Development (Republic of Korea)	Cubic Defense Applications Group	KBRWyle	Smartronix Inc.
Air Academy Associates	Defense Acquisition University	L-3 Telemetry & RF Products	SURVICE Engineering Company
AMERICAN SYSTEMS	Dell EMC Corporation	MacAulay Brown Inc. (MacB)	SYMVIONICS Inc.
Amtec Solutions Group	Delta Information Systems	Maritime Test and Evaluation Authority (New Zealand)	System Testing Excellence Program – University of Memphis
Analytical Graphics, Inc.	DEWESoft, LLC	MEI Technologies, Inc.	Systems Application & Technologies (SA-Tech)
Apogee Labs	Diversified Technical Systems (DTS)	The MIL Corporation	Systems Engineering & Management Company - SEMCO
Applied Research Laboratory/PSU	Dynamic Science, Inc.	Modern Technology Solutions, Inc. (MTSI)	Teletronics Technology Corp
Arcata Associates, Inc.	Dynetics, Inc.	NAC Image Technology	Telspan Data
Astro Haven Enterprises	ERC Inc.	National Chung-Shan Institute of Science and Technology (CSIST)-Taiwan	Textron Systems Corporation
Australian Defence Force Tactical Data Link Authority	Emhiser Research	NetAcquire Corporation	The Boeing Company
Avion Solutions, Inc.	EWA Government Systems, Inc.	Nova Systems (Australia)	TRAX International
Avionics Interface Technologies	Garud Technology Services, Inc.	PAE	TRIDEUM Corporation
Avionics Test & Analysis Corp	General Dynamics Mission Systems	Parsons Corporation	Trident Research
BAE Systems (U.S.)	Georgia Tech Research Institute - GTRI	Photo-Sonics, Inc.	Ultra-Electronics Herley Lancaster
BAE Systems (Australia)	Glacier Technologies LLC	QinetiQ Ltd.	Weibel Scientific A/S
Black Diamond Consulting	IDA Technology	Rockwell Collins, Inc.	Westech International, Inc.
Brazilian Aeronautical Commission	InDyne, Inc.	Rolls-Royce plc	Wideband Systems, Inc.
		Rotating Precision Mechanisms, Inc.	Zodiac Data Systems

CERTIFIED TEST AND EVALUATION PROFESSIONALS (CTEP)

Al Pepper, CTEP - Scientific Research Corporation (SRC)	**E P Lukert, CTEP** - US Army Geospatial Center	**Keith Sumner, CTEP** - Booz Allen Hamilton	**Paul R. Dailey, Ph.D., CTEP** - Johns Hopkins University Applied Physics Lab
Alexander F. Henning, CTEP - U.S. Air Force	**E. Wyatt Brigham, CTEP** - Northrop Grumman Aerospace Systems	**Kenneth M. Sheehy, CTEP** - AMERICAN SYSTEMS	**Peter Christensen, CTEP** - The MITRE Corporation
Allan V. Alfafara, CTEP - Northrop Grumman Aerospace Systems	**Eric Lowy, CTEP** - FAA	**Larry Pigue, CTEP** - SPARTA, Inc.	**Peter G. Crump, CTEP** - Georgia Tech Research Institute (GTRI)
Anthony Shumskas, CTEP - TASC, Inc.	**Eric Rannenberg, CTEP** - Tekla Research, Inc.	**Laura A. Snyder, CTEP** - Joint Interoperability Test Command (JITC)	**Peter Tyson, CTEP** - Avian Engineering, LLC
Benjamin Andersen, CTEP - Modern Technology Solutions, Inc.	**Erwin R. Sabile, CTEP** - Booz Allen Hamilton	**Leslie A. Donoghue, CTEP** - TASC	**Priscilla Glasow, Ph.D., CTEP** - The MITRE Corporation
Bradford Henson, CTEP - SAIC	**Gabrielle Bradway, CTEP** - Alion Science And Technology	**LtCol Mark Raffetto, USMC, CTEP** - Marine Corps Operational Test And Evaluation Activity	**Ralph R. Galetti, CTEP** - Boeing-SVS
Brian Paul Hodgkinson, CTEP - Northrop Grumman Aerospace Systems	**Garfield S. Jones, CTEP** - Department of Homeland Security	**Lyle Kent Burkhart, CTEP** - 605 TES	**Rebecca Bradshaw, CTEP** - TransCore
Bryan Herdlick, CTEP - Johns Hopkins University Applied Physics Laboratory	**Gary Brandstrom, CTEP** - Parsons	**MAJ Cornelius Allen, USA, CTEP** - PEO Aviation	**Rebecca L. Badgley, CTEP** - Advanced Management Strategies Group
C. David Brown, Ph.D., CTEP - Office of the Secretary of Defense	**Greg Griffitt, CTEP** - Avian Engineering, LLC	**Malcolm G.Tutty, CTEP** - DTRMC	**Richard Boyer, CTEP** - Scientific Research Corporation (SRC)
Carolyn Keith, CTEP - TASC, Inc.	**Gregory Turner, CTEP** - The MITRE Corporation	**Marc L. Hoffman, CTEP** - Booz Allen Hamilton	**Robert Brassell, CTEP** - Wyle CAS Group
Chad Lauffer, CTEP - USMC/Amphibious Vehicle Test Branch	**Harold Kang, CTEP** - United States Marine Corp	**Mark Carpenter, CTEP** - The BOEING Company	**Robert Learner, CTEP** - MEI Technologies, Inc.
Chad Williams, CTEP - MCOTEA	**Henry C Merhoff, CTEP** - Louis P. Solomon Consulting Group	**Mark London, CTEP** - Naval Air Warfare Center	**Ronald E. Jackson, CTEP** - TASC, Inc.
Charles McKee, CTEP - T&E Executive	**James Watson, Ph.D., CTEP** - JRAD	**Mark Price, CTEP** - DASD (DT&E)/Foxhole Technology	**Rory Jennings, CTEP** - The MITRE Corporation
Chelsea Prendergast, CTEP - Joint Research and Development, Incorporated	**Jeffrey Gay, CTEP** - NAVAIR/Tekla Research Inc.	**Marlon Ridley, CTEP** - DigiFlight	**Shannon Krammes, CTEP** - Marine Corps Operational Test And Evaluation Activity
Christine Fuentes, CTEP - The MITRE Corporation	**Jody South, CTEP** - AMERICAN SYSTEMS	**Martin Hilton, CTEP** - BAE Systems	**Sonia T. Sethi, CTEP** - Booz Allen Hamilton
Christopher M. Huiett, CTEP - Alion Science And Technology	**John Burke, CTEP** - JRAD	**Martin J. Mears, CTEP**- Jacobs Technology	**Steven K. Whitehead, CTEP** - Naval Sea Systems Command
Corrie Wells, CTEP - AASKI Technology, Inc.	**John Geskey, CTEP** - Applied Physics Laboratory/The Johns Hopkins University	**Mary Elizabeth Fraser, CTEP** - AMERICAN SYSTEMS	**Steven Tran, CTEP** - Northrop Grumman Aerospace Systems
Dana Allen, CTEP - Air Force Space And Missile Systems Center	**John Heavener, CTEP** - Schafer Corporation	**Matthew Lua, CTEP** - Marine Corps Operational Test And Evaluation Activity	**Suzanne M. Beers, Ph.D., CTEP** - The MITRE Corporation
Daniel Knaus, CTEP - Tekla Research, Inc.	**John Ingram, CTEP** - AMERICAN SYSTEMS	**Melforde Granger, CTEP** - Department Of Defense	**Terrance Westerfield, CTEP** - U.S. Army Test & Evaluation Command (TEC)
Darryl Johnson, CTEP - Scientific Research Corp. (SRC)	**John Moloko, CTEP** - Cask LLC	**Michael Flynn, Ph.D., CTEP** - Defense Acquisition University (DAU)	**Thomas Cash, CTEP** - CGI Federal
David L. Goodson, CTEP - Monkey Business Consulting, LC	**John Nixon, CTEP** - TASC, Inc	**Michael Guidry, CTEP** - Jacobs Engineering	**Thomas McGowan, CTEP** - Marine Corps Operational Test and Evaluation Activity
David L. Thomas, CTEP - RoundTable Defense, LLC	**Jonathan Selby, CTEP** - The MITRE Corporation	**Michael Lilienthal, Ph.D., CTEP** - EWA Government Systems, Inc.	**Thomas Sachse, CTEP** - PEO SUB
David Schoonenberg, CTEP - The MITRE Corporation	**Joseph F. Puett III, CTEP** - ManTech International	**Michael Weibel, Ph.D., CTEP** - JRAD	**Wallace John Tubell, CTEP** - Defense Acquisition University (DAU)
David Scott Bough, CTEP - Prevailance, Inc.	**Josh Tribble, CTEP** - AVW Technologies	**Mike Short, CTEP** - G2, Inc.	**William "Dave" Bell, Ph.D., CTEP** - The MITRE Corporation
David Zehr, CTEP - 419 FLTS/DOO	**Justin C. Everett, CTEP** - Joint Research and Development (JRAD)	**Miles Thompson, CTEP** - Georgia Tech Research Institute (GTRI)	**William Eischens, CTEP** - Modern Technology Solutions, Inc. (MTSI)
Debbie Y. Hugh, CTEP - Deloitte Consulting	**Karen Kissinger, CTEP** - TASC, Inc.	**Orlando P. Quimba, CTEP** - TASC, Inc.	**William J. Parker, CTEP** - Joint Interoperability Test Command
Duane Goehing, CTEP - Institute for Defense Analyses (IDA)	**Keith Dillingham, CTEP** - Life Cycle Engineering	**Patrick Rolow, CTEP** - Alion Science And Technology	**William J. Swank, CTEP** - DASD(DT&E)
			William P. Singletary, CTEP - AFOTEC/Det 6

THANK YOU TO OUR SPONSORS!

AMERICAN™ SYSTEMS

Founded in 1975, AMERICAN SYSTEMS is one of the largest employee-owned companies in the United States. With offices worldwide and a headquarters in Chantilly, Virginia, we provide a wide variety of services tailored specifically to our customer base. Our approximately 1,300 employee-owners have a vested interest in their work and are committed to delivering the highest-quality strategic solutions to every customer, every time.

EWA Government Systems, Inc.

Enabling a more secure future

EWA Government Systems, Inc. provides products and services to government and commercial markets in engineering, intelligence support, homeland security, special programs, EW operational technology, test & evaluation, and training. Our extensive range of capabilities also includes cyber defense, radar simulators, radar design and development, range instrumentation, and EW scenario simulators, and wireless applications.

KBRwyle

We Deliver

KBRwyle is part of KBR, Inc. (NYSE: KBR). The organization's capabilities span the full spectrum of government mission requirements including research and development, testing, engineering, logistics, deployed operations, and life-cycle sustainment. KBRwyle is the #1 SETA and A&AS contractor to U.S. Naval and Army Aviation, and U.S. Army Air and Missile Defense. It is also the #1 life sciences provider to NASA. KBRwyle is headquartered in El Segundo, California and maintains over 50 office locations.

SURVICE ENGINEERING COMPANY

A nationally recognized specialist in combat system survivability, weapon system effectiveness, and system safety, the SURVICE Engineering Company is a small business that's provided military and industry customers with high-quality analytical products and services for more than 25 years. During this time, we've continued to grow in size, capability, and national recognition; however, we've never lost sight of our original mission—to provide safe, survivable, and effective combat systems for U.S. military personnel.

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.