# 5TH CYBER SECURITY WORKSHOP

## *"Challenges Facing Test and Evaluation"*

# ABSTRACTS AND BIOGRAPHIES

## March 25-28, 2019

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

---

### Program Committee

**PROGRAM CHAIR** - Ms. Chris Susman, SURVICE Engineering Company
**PROGRAM TECHNICAL CO-CHAIRS** – Dave Brown, PhD, CTEP, Chesapeake Systems Engineering; Mr. Pete Christensen, CTEP, The MITRE Corporation; Paul Dailey, PhD, CTEP, Johns Hopkins University Applied Physics Lab; and, Mr. Bruce Einfalt, Applied Research Laboratory, The Penn State University
**EXHIBITS & SPONSORSHIPS** – Ms. Cathy Pritts and Mr. Jim Myers

---

### WORKSHOP DESCRIPTION

Cybersecurity continues to be at the forefront of the DoD acquisition community. As this contested environment brings new challenges at as accelerated rate, the T&E community must be prepared to meet new requirements.

This Workshop provides an opportunity to share ideas among experienced T&E professionals regarding threat ad requirements, test capabilities, autonomous systems, and evaluation methodologies. Our goal is to share ideas on how to better characterize cybersecurity threats, evaluate system performance when attacked by a cybersecurity threat, and assess risk of using the system in the presence of a cybersecurity threat.

Please join us in Belcamp, Maryland, as members of the T&E community from academia, industry, and government discuss the evolving discipline of Cybersecurity T&E. Come share your thoughts, connect with others, and learn from some of the leading experts at this Workshop. The cyber threat will only increase with time. So glad that you are here!

---

### 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!*

Georgia Tech Research Institute

KBRwyle
We Deliver

SURVICE ENGINEERING COMPANY

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 25TH

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

---

### *Blockchain 101: Blockchain De-Mystified*

Instructor: **Duane Wilson, PhD, SURVICE Engineering**

Blockchain De-Mystified: Why is the Blockchain such a technology phenomenon in the today's tech lingo? What are the current use cases of Blockchain? Can the Blockchain solve all of our problems? Is there any application to Test & Evaluation? Will it be here in the future? The aim of this tutorial is to attempt to answer all of these questions and provide a baseline understanding of what Blockchain technology is and what it is not - which is often even more important. We have broken our tutorial down into six distinct - yet related sections to attempt to appease a very diverse audience: Blockchain 101, Blockchain Components, Blockchain Applications, Blockchain Demo, Blockchain Development, and Blockchain Test & Evaluation.

- In Blockchain 101 we will discuss Foundational Concepts of the Blockchain and demystify this term that so widely used today.
- In Blockchain Components we break down the Blockchain into its logical components to show you how simple it is at its core.
- In Blockchain Applications we discuss the myriad of use cases for Blockchain Technology and the different domains in which it is being used in practice.
- In Blockchain Demo we allow you as the attendee to participate by presenting an interactive demo of the Blockchain
- In Blockchain Development we show the code behind the demo and all Blockchains in circulation today to appeal to the developers in attendance.
- Lastly, in Blockchain Test & Evaluation we demonstrate how Blockchain applications can be tested and evaluated and where the T&E community at large would find some relevant uses for this innovative technology.

---

### *Cyber Test and Training Solutions with TENA and JMETC*

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

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.

---

### *Introduction to Cybersecurity Test & Evaluation*

Instructor: **Mr. Pete Christensen, CTEP – 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.

---

## *Integrated Systems Engineering, Agile DevSecOps, and Test and Evaluation*

Instructor: **C. David Brown, Ph.D., CTEP - Chesapeake Systems Engineering**

With recent emphasis on Agile and DevSecOps development methodologies, many practitioners now believe that these new methodologies completely negate or replace the elements of program management, systems engineering, and independent test and evaluation. Nothing could be farther from the truth. In fact, Agile and DevSecOps incorporate many elements, often with only different names. For many programs, especially tightly coupled hardware and software programs, like almost all modern military systems, a hybrid systems engineering and Agile development approach is required. This approach must then be top level managed with program management techniques, and verified and validated with independent test and evaluation, especially for developmental test of integrated hardware-software, operational test, and cyber test and assessment.

This tutorial consists of a quick overview of systems engineering and test and evaluation. This is followed by a brief introduction to Agile and DevSecOps. Finally, we will discuss techniques to effectively integrate the above when and where required.

---

## *Software Assurance*

Instructor: **Mr. Robert Martin – Senior Secure Software & Technology Principal Engineer, MITRE**

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

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

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

---

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

---

## *Building Better Models Using Robust Machine Learning Methods*

Instructor: **Thomas A. Donnelly, PhD – SAS Institute**

Through case studies, you will learn to build better and more robust models with machine learning and predictive modeling techniques. Featured methods will include many types of regression (linear, logistic, penalized), neural networks (single layer, dual layer, boosted), and decision trees (simple, bagged, boosted). To make these methods robust you'll learn to split your data into training, validation (tuning) and test subsets to prevent over fitting. And, when there are not enough data to support splitting, learn how to use penalization criteria to prevent over fitting. You will also see how to use graphical and statistical comparison techniques to help choose the best predictive model.

Featured case studies include building surrogate models of a computer simulation of a helicopter flying surveillance and identifying the best predicting model of the various logistic, decision tree, neural, spline, and regression models. A derivative data set of the 1998 KDD Cup Cyber Attack Data set with over 40 possible causes of 20 types of attack will be used to show the benefit of building a robust ensemble predictor model. It will also be shown how to use penalized regression methods for highly correlated data to create in many cases, models that are almost as good as complex neural networks, but much more interpretable – even offering confidence intervals about predictions. This tutorial is for analysts, scientists, engineers and researchers interested in learning how machine learning can help them use the data they have today to better predict tomorrow.

---

## *Fundamentals of Distributed Testing (1 hour) and Identifying Requirements and Vulnerabilities for Cybersecurity (3 hours)*

Instructors:

**Fundamentals of Distributed Testing (1 hour)**
Mr. Scott "Gunner" Thompson - Electronic Warfare Associates - GSI
**Identifying Requirements and Vulnerabilities for Cybersecurity (3 hours)**
Mike Lilienthal, PhD, TRMC, and Mr. Patrick "Preacher" Lardieri, Lockheed Martin

There are two tutorials presented during the 4-hour block of time allocated. The first hour "Fundamentals" was developed to provide information and an approach for the DoD T&E community on how to use distributed methodologies to plan for, prepare, and execute distributed test events. The tutorial is intended to present executive level material on fundamental concepts of Distributed Testing, as well as generate a discussion on considerations and requirements that can be used for the design of Integrated Cyber Security T&E in a Joint mission environment. Desired outcome is to have attendees incorporate Distributed Testing methodologies into their own processes and guidelines.

The last three hours of the tutorial was developed for the many Service acquisition, System Engineering (SE), and Test and Evaluation (T&E) teams that 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.

The tutorial will:

- Explain the DOT&E 6 Step Cyber T&E process
- Explain the OSD Cyber Table Top (CTT) process
- Explain the National Cyber Range's cyber T&E methodology
- Describe how both tools improve the engineering and testing of cyber resilient systems and how they support the DOT&E 6 Step Cyber T&E Process
- Present lesson learned using these tools over the past 5 years

The CTT (which has been adopted by the Navy and DT&E) 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.

The National Cyber Range is an OSD TRMC capability that provides the ability to conduct cybersecurity test and evaluation of DoD systems in support of cyber risk assessments. It is capable of instantiating systems in classified close test range and enabling red and penetration test teams to conduct hands-on evaluation of cyber attacks on the systems under evaluation. The tutorial is based on the lessons learned from using the CTT and NCR processes to support acquisition programs across the services.

Intended Audience: It is intended for attendance by Acquisition Program Management Offices, Systems Engineers, Chief Developmental Testers, and Lead Developmental Test and Evaluation (DT&E) Organizations.

---

## *How to Successfully Plan Test Strategy for Agile Development in a Gov Framework*

Instructor: **Mr. Hans Miller and Ms. Colleen Murphy – The MITRE Corporation**

This tutorial provides a framework and guidance for programs transitioning to an agile construct or new programs established with an agile construct. The intended audience includes requirements managers, program managers and test managers executing DoD programs; however, the overall principles could apply to multiple agencies. This tutorial is not a singular solution for agile testing; it acknowledges the different approaches needed for different programs and is intended to provide students with an understanding of concepts that can be tailored to their specific program. This course will walk through characteristics of agile process and where it does and does not apply to help inform expectations. It will cover US code, OSD and service policy as it applies to agile testing. The core of the tutorial covers upfront planning and strategy considerations for successful testing; requirements, contracting, infrastructure investments, automation and test execution. It concludes with how to translate that strategy into concise, timely, and relevant documentation from the TEMP, test plan, and test reporting.

---

## *Planning and Executing Cyber Tables Tops, Facilitator Training*

### Instructor: Mr. Vinny Lamolinara and Mike Cobb, PhD – Defense Acquisition University (DAU)

The tutorial introduces and applies the Cyber Table Top (CTT) mission-based cyber risk assessment (MBCRA) method to help discover cyber vulnerabilities, gauge their risk, propose mitigations and inform other competencies, documents and events across the DoD acquisition lifecycle. The workshop will establish an understanding of the threat and "thinking like a Hacker"; provide a "wheel of access" methodology to identify and diagram surface-attack characteristics; include cross-competency personnel, including users, to identify and prioritize cyber-attacks / vulnerabilities in a Red / Blue / White Team "wargame" mission scenario; and provide a construct to characterizes and report risk and mitigations in order to design and maintain cyber resilient systems and personnel in the acquisition and operational phases of an Information or Platform weapons system. Participants will conduct exercises in each phase to reinforce and apply the concepts and methodology will learn how cybersecurity principles apply to their career fields. Students will create a surface attack taxonomy, role play different competencies including engineering, test, cybersecurity, logistics, safety, intelligence, contracts and the adversary. The case studies and scenarios will build up in complexity culminating in a mini-CTT execution and Cyber Risk out brief (to a simulated PM) for an exemplar weapons systems at the UNCLAS level. Students will also apply CTT results to inform Test, AoA ICD/CDD/CPD, RFP/SOW, Specification, Architecture and upgrade / patch / ECP requirements as well as acquisition and risk management strategy. This workshop will allow enable students to participate in CTT efforts in their respective programs. Tailorable to the specific customer needs.

Objectives: Given a cybersecurity scenario, use Surface-attack characterization and Cyber Table Top Methodology to discover cyber vulnerabilities, gauge their risk, propose mitigations and inform other competencies, documents and events across the DoD acquisition lifecycle.

1. Understand and apply the "think like a Hacker" adversarial threat concept to cybersecurity.
2. Understand, apply and create the "wheel of access" surface-attack methodology to create a taxonomy useable to discover cyber vulnerabilities for DoD systems.
3. Understand and apply CTT methodology for various acquisition scenarios.
4. Create program manager level out brief delineating risks, mitigations and implications for test, requirements, design, logistics and safety.

Target Attendees: The acquisition workforce, including industry partners, who design, build, procure, maintain, and provision cybersecurity capabilities.

# ABSTRACTS

---

## *The Benefits of TENA on Cybersecurity*

Ryan Norman - TENA / JMETC

Enabling 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. TENA has been chosen for use by JMETC, 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 presentation will address the benefits TENA to the cyber Test and Training community.

---

## *Binary Cyber Triage*

Eric Missimer, Curtis Walker, Arch Owen - Draper

Having access to source code facilitates cyber test planning, but contractors often only deliver binary, thus providing the cyber test planning team little information on which to do the planning. As such, the government testing teams need a suite of tools that allow them to analyze binary code to identify potential vulnerabilities and thus steer cyber test planning. Draper is developing a suite of tools able to provide varying degrees of insight on binary code, ranging from basic insights such as any libraries that might be incorporated in the code, to more sophisticated insights such as identifying specific potential vulnerabilities including traces that exploit those vulnerabilities. This talk will provide an overview of these evolving tool sets and ideas for evolving these tools.

---

## *Cyber T&E on Internet Protocols and Avionics Data Buses*

Gene Downs, Mark Ebert, Jeff Carr, James Chenault, Gene Downs, David Elkins, Jeff Poole - Redstone Test Center, Environmental & Component Test Directorate, US Army Redstone Test Center, Redstone Arsenal

The last decade saw an explosion of cyber exploitation of Internet Protocols and Industry has developed software test tools to define and protect against these cyber threats. The Army in an effort to reduce risk to Enterprise IT systems developed process and procedures to reduce the impact to “at risk Networks.” This approach is Risk Management Framework for IP networks and has been the program to also address weapon platforms that leverage IP and other communication protocols to include Milt STD 1553 and ARINC 429. Applying RMF standard controls to weapons systems and Non-IP networks introduces several key issues for the Test and Evaluation community. RMF focuses on Enterprise IT platforms, and is poorly equipped to assess weapons systems with Non-IP based networks. The current problem for testing weapons systems is that RMF fails to address critical communication protocols with the appropriate cyber assessment tools. This paper will identify some T&E techniques to close the gap on cyber test tools and to help manage cyber effects on Non-IP based communication networks. This paper will also discuss the T&E issues with the RMF process, and help Program Managers address cyber threats to their platforms.

How can cyber threats cross communication domains, and what impacts to a weapon system could be derived from attack vectors that traverse protocols on a weapons platform? The T&E community will have to enhance current data collection tools and instrumentation to better support cyber Testing. The paper will discuss instrumentation for: IP, 1553, and ARINC 429. Each communication protocol also requires tools that support visualization of cyber threats. This paper will identify existing cyber tools and T&E gaps that exist.

Also presented in the paper is data collection for actionable information. Current IP cyber tools address a vulnerability relative to a defined virus definition file. T&E must derive if the issue / vulnerability is critical to the mission and or performance of the mission. Is the system resilient to a given cyber-attack and are there mitigations in place to filter or isolate an infected network segment? The paper will evaluate current Information Assurance strategies and address efforts to enhance RMF goals. This includes possible ways to perform Test and Evaluation of a weapon system in its operational state, and what actionable information can be collected for a system owner to quantify “acceptable cyber risks.”

---

## *Cyber Threat Automation and Monitoring System*

Himanshu Upadhyay - Florida International University

Florida International University’s Cyber Threat Automation and Monitoring System (CTAM), developed for Department of Defense’s Test Resource Management Center has proved its efficacy in advanced cyber threat monitoring and response using state of the art virtualization technology and malware behavioral analysis using sophisticated machine learning algorithms. Focus of this S&T research is to understand the impact of various test vector on the defined mission using the virtual test bed.

CTAM system is being developed in phases for T&E purpose to detect, monitor, and analyze the malware behavior during cyberspace attacks by enabling key capabilities like: 1) deployment of virtualized environments along with the advanced instrumentation tools for control and monitoring of malware; 2) cyber-attack emulation through infection and propagation of simulated endpoints; 3) fine-grained introspection, data collection, and monitoring of various aspects of the infrastructure through the centralized system; 4) profiling of malware behavior from a virtual infrastructure perspective; 5) rapid cleanup, reconfiguration and redeployment for efficient real-time profiling of test vectors in cyberspace; and 6) generation of reports, including visualizations which assess the potential damage to operational cyberspace assets.

CTAM system consists of four major components Virtualization, Advanced Cyber Analytics, Test Control Center, and Test Vector Repository.

- Virtualization provides the capabilities to create system under test (SUT) virtual machines to perform mission critical test execution. The virtualization component consists of the various modules like virtual machine image repository, malware installer, introspector, security/kernel agent, security/kernel monitor and security/kernel drivers to build and monitor the test bed. This component also provides the functionalities for the Smart Memory Acquisition using best in class VMI technology LibVMI to introspect the kernel of the operating system to extract the various data structures for memory forensics.
- Advanced Cyber Analytics provides the capabilities to analyze the memory data structures extracted from the system under test (SUT) with focus on Windows and Linux virtual machines deployed on Xen and KVM/QEMU hypervisor using traditional machine learning algorithms, DLL Monitor, Invariant Data Structures and File Monitor.
- Test Control Center provides a centralized user interface to control and manage the CTAM virtualization and cyber analytics components. It consists of six major modules: Test Vector Management, Testbed Configuration, Test Case Management, Virtual Machine Management, Testbed Monitor, and Machine Learning Model Management.
- Test Vector Repository consists of a wide range of test vectors, many derived from malware collected in the wild. These vectors are executed on the SUT virtual machines to study the impact on defined mission. The repository consists of various test vectors – rootkits and malware collected from various sources as well as custom test vectors.

Next phase of this project involves development and enhancement of the CTAM system to TRL6 on XEN and KVM/QEMU platform, CTAM as a Service, Advanced Cyber Analytics with Deep Learning (Deep Neural Network, Convolutional Neural Network and Recurrent Neural Network – LSTM) , Stream Processing with Spark and Analytics Control Center.

---

## *Cybersecurity - A Vendor Perspective Part 2: DSS Comprehensive Security Review*

Jeff Rusincovitch - Zodiac Data Systems, Inc.

The U.S. Government, OEMs and prime contractors are recognizing the importance of cyber security and continuing to mature cybersecurity requirements. These requirements apply not only to protecting data on vendor networks but also require a comprehensive mitigation plan for the flight test products, to include supply chain integrity and software development processes. This presentation is a second installment to "Cybersecurity - A Vendor Perspective" from the 2017 ITEA Cyber Security Workshop. It will recap, from the vendor's perspective, the Risk Management Framework (RMF) and discuss the strategy, progress, and commitment for achieving a robust RMF system. This presentation also will discuss methodology and results from our recent comprehensive security review inspection by the Defense Security Service (DSS). Finally, this presentation will discuss, from the vendor's perspective, compliance with DFAR 252.204-7012 and NIST 800-171 Security Controls for protecting Covered Defense Information (CDI).

---

## *Defining Solid Security Requirements*

Randall W. Rice, CTAL-SEC - American Software Testing Qualifications Board

In this session, Randall Rice addresses the shared space between two very challenging areas: Getting good requirements and establishing effective cybersecurity defenses. User stores, while helpful to define functions, are typically not detailed enough to define both intended and unintended behavior of a system, especially in the context of information security. Unfortunately, industry metrics tell us that the great majority of software defects (security and other) can be traced back to flawed or missing requirements.

In DoD and other federal projects, the challenge of defining cybersecurity requirement is unique due to procurement rules and vendor practices. These challenges will be addressed with solution strategies.

In this session, Randall will cover:

- The lifecycle view of requirements and security
- Stakeholder and customer involvement in gathering and documenting requirements for security
- Dealing with the unique challenges of DoD and other federal projects
- The importance of clearly defining the security aspects of a system
- How to drive the scope of requirements by understanding known threats and available defenses
- How to define "misuse cases" and problem frames from the cybersecurity perspective
- How to revise and maintain requirements when threats change, new threats emerge or new features are added to the system

---

## *Functional Data Analysis – An Improved Approach for Modeling a Stream of Data*

Thomas Donnelly - SAS Institute Inc.

With nearly continuous recording of sensor values now common, a new type of data called "functional data" has emerged. Rather than the individual readings being modeled, the shape of the stream of data over time is being modeled. As an example, one might model many historical vibration-over-time streams of a machine at start-up to identify functional data shapes associated with the onset of system failure. In the DoD test community data streams might be aircraft sensor data at various phases of flight, gun barrel degradation versus cumulative round count, the transport and dispersion of a chemical agent cloud, or a radar/sonar signature versus angle.

Functional Principal Components (FPC) analysis is a new and increasingly popular method for reducing the dimensionality of functional data so that only a few FPCs are needed to closely approximate any of a set of unique data streams. When combined with Design of Experiments (DoE) methods the response to be modeled in as fewest tests as possible is now the shape of a stream of data over time. Example analyses will be shown where the form of the curve is modeled as the function of several input variables allowing one to determine the input settings associated with shapes indicative of good or poor system performance. This allows the analyst to predict the shape of the curve as a function of the input variables.

## *Life-long protocol influence and shaping of smart autonomous systems to assure meaningful human-autonomy teaming: A New Australian Research Program*

Kate Yaxley - University of New South Wales – Canberra (UNSW-C)

As the world embraces the evolution of cognitive-cyber-physical (C2P) systems, so too are militaries, bringing about systems with the ability to comprehend and act on large amounts of information autonomously, yet need to operate symbiotically with our warriors. This quickly evolving human-autonomy relationship hinges upon trust, which needs to be understood by our warriors, and equally by our smart autonomous systems (SAS). Trust shapes our willingness to collaborate, innovate and learn and is formed from a fusion of beliefs, observations, and purposeful interactions with others, including SAS. To ensure trust is interoperable between humans and SAS, trust in SAS needs to be defined through baseline protocols (beliefs encoded into processes, rules, and interpretation functions) with the elasticity to be influenced and shaped through-life user observations and interactions. The complexity of such a design necessitates an iterative life-long learning strategy coupled with test and evaluation methods for the design, development, acceptance and operational use of SAS.

Currently, security protocols for networks are using measures of trustworthiness and reputation to assess whether nodes are secure for routing processes. To design trustworthy SAS, these localised abstractions of trust need to propagate across the C2P system-of-systems to deliver a whole-of-system trust-assurance and certification.

Introducing meaningful human-autonomy teaming (M-HAT) to the development and iterative through-life operation of SAS, trust protocols need to be adaptively calibrated in a manner that is appropriate to the level of cooperation required for effective and ethical use of SAS in the profession of arms. M-HAT will require the use of representative commanders in the development and acceptance phases of test and evaluation, preferably in structured usability trials. The representative commanders will need to follow a developed curriculum to allow for the development of an enlisted warrior-to-leader capable of invoking trust in others, thereby building trustworthiness and reputation into the dyad of blended human and C2P systems.

Using test-led methodology to establish frameworks and develop the design space should mean trust protocols and protocol influence can be developed in a more robust and timely way. Due to the multi-factor nature of the C2P environment, combinatorial testing could be more efficient in evolving reputation in SAS by iteratively testing and evaluating quantitative and qualitative measures of through-life learning and thus the maintenance of trust.

New sponsored Australian research into protocol influence and behaviour shaping of trust in SAS aims to explore test-led usability methodologies to drive requirements definitions for future C2P systems. We invite attendance from those interested in collaborating or those with particular viewpoints to share on the topic.

---

## *Performing Reliable Cyber Assessments in the Land of Unknowns*

Sandeep Pisharody, PhD - MIT Lincoln Laboratory

Current government and private organization operations require a cyber environment that is available and resilient, leading to substantial investment in cyber defensive technology as well as human capital to serve as cyber defenders. Assessment of these investments, and cyber event preparedness is often done via live range exercises. However, conducting a live exercise that is repeatable is difficult due to variances in the test conditions and differences in human cyber defenders, and the inability to restrict inputs to the desired range. Alternately, low-cost cyber modeling and simulation approaches for assessments often is repeatable and has controlled inputs/parameters but lacks real-world data, making the results low-fidelity and non-actionable. This paper examines how to successfully navigate a risk-uncertainty framework for cyber assessment. We discuss our approach in leveraging results from a live range assessment in conjunction with cyber modeling and simulation techniques. These techniques help lay the foundation for higher fidelity results through further study as well as draw conclusions that would help with executive decision making.

---

## *The Promise and Peril of Deep Learning*

John McKay, PhD - Applied Research Laboratory - Pennsylvania State University

Cyber security is a crucial field of study in our age of technological ubiquity. Indeed, in this era of technological ubiquity, applications that can prevent and/or detect malicious intrusions are vital to ensuring personal information is kept safe and users have trust in their devices. Unfortunately, the challenge of cyber security has arguably never been harder; there are more vulnerable devices with internet access than ever before and attackers have become incredibly apt at exploiting flaws towards their own ends. For this reason, there is growing interest in using machine learning algorithms towards cyber security applications. This is because machine learning, mostly in the form of deep learning, has far exceeded impressive benchmarks in such areas as image classification in recent years. We are starting to see algorithms capable of exceeding human performance in automated tasks.

With this push towards machine learning for cyber security starting to make waves, it is worth understanding that there are key flaws in our current understanding of these deep learning models that should give cyber security analysts pause. So-called “adversarial attacks” have become a major problem for deep learning classifiers. Research has shown that directed but tiny, imperceptible changes to inputs can cause havoc to deep learning classifiers, not just causing them to misidentify queues but even towards an adversely-chosen class and with a high confidence. The reasons why this happens are not settled and relate to the black-box nature of what neural networks learn.

The intent of this talk is to give the audience a background in modern machine learning and how a fundamental lack of knowledge concerning the learned mechanics of such models need to be addressed as these models get incorporated into security programs.

---

## *Software Defined Radio Enabled RF Cyber Robustness Testing*

Adam Wilkerson - GANCorp

When developing a cyber exploit of any system, the attacker must consider multiple factors. These factors can largely be grouped into the two categories of access and effects. To implant and enact any effect on any modern system, an attacker must first gain access through some attack surface to that system. From the radar to the radio, most modern systems have at least one Radio Frequency (RF) receiver onboard. These receivers are frequently unguarded and provide an attack surface for would-be cyber actors. RF receivers are susceptible to a wide range of sophisticated effects beyond blanket noise or repeater jamming. Through these receivers, attackers could activate previously-implanted software or manipulate data streams to disrupt system operations. The bitwise timing of these signals is typically quite short and manipulating data streams for effect requires more knowledge than operating frequencies and modulation schemes. But the details required for seizing control of RF surfaces on target systems are frequently easy to determine by actors wanting to affect such a system. As a result, hardening these systems needs to be considered from the outset of their design and thoroughly tested over the lifetime of any system. Recreating transceivers for the signals processed through these surfaces has become easier in recent years with the technological development of software-defined radios (SDR). SDR technology has enabled rapid and inexpensive development of models to process the functions of radios and modems to process a wide array of signals in a multitude of environments. Using SDRs to simulate signals, the RF surfaces of systems can be stimulated, and commanded into different modes and issued orders to affect the processing of data coming into the system. Likewise, SDRs can be used to simulate attackers in real-time situations, listening and injecting data via these surfaces in a quickly-configurable, modular way. Combining these tools with high-power amplifiers enables field-testing of potential threats for detailed analysis of possible exploitations to systems in an open-air Test and Evaluation Environment. SDRs can also be configured to handle bitstreams over conventional modems, like those seen in lab environments. By configuring SDRs to process data, a model of a system under test can broadcast an RF signal through a closed mesh in a lab environment to create a closed-loop test of RF surface vulnerability. Likewise, an attacker can be included in any such test to stimulate the model with attack data, attempting to remotely control the system to functionally disable it. In our paper, we'll outline a system that is usable both in open-air testing and closed-loop lab tests to simulate friendly RF signals. This SDR-based solution will also have an attacker component, enabling thorough testing of a system's RF vulnerabilities. This depth of research by the T&E community will enable developers and acquisition specialists to harden systems from the outset, protecting customers' assets from the ground up.

---

## **System Security Profiling (SSP)**

Mr. Gary Wright - Johns Hopkins Applied Physics Laboratory

The System Security Profiling (SSP) process applies a systems engineering approach to cyber security testing, combining Red, Blue, and White team activities and perspectives into a unified process that is designed to enhance overall value compared to traditional "red team" penetration testing. Originally developed at NSA in the 1990s, the SSP process has been adopted and expanded upon at JHU/APL since 2015, providing the basis for cyber assessment activities spanning multiple sponsor communities and scaling from individual devices to complex networks of systems.

# SPEAKER BIOGRAPHIES

**Mr. Robert Aguilera** is a Senior Vice President for Garud Technology Services, Inc. (GTS). GTS is a Maryland-based, Economically Disadvantaged Woman Owned Small Business (EDWOSB), and a highly-specialized provider of Technical and Professional services (https://www.garudtechnology.com/).

Rob is a senior acquisition professional with more than 30 years of support to DoD and DHS Research, Development, Test and Evaluation (RDT&E) initiatives including Basic and Applied Research, Technology Demonstrations/Experimentation and prototype efforts.

He is a retired Naval Officer of 25 years that completed two tours in his career at the US Navy's Operational Test Authority. In the last 11 years in private industry, Rob has supported T&E efforts in both DoD and DHS.

In DHS, Rob overseas a portfolio of activities that includes Operational Test Agent (OTA) support to several DHS Oversight programs in CBP & FEMA. Most recently GTS completed FOT&E of FEMA's Logistics Supply Chain Management (LSCMS) and CBPs TECS Modernization programs. Both were Level 2 (ACAT 2 equivalent) oversight programs, and both test events involved cybersecurity/resilience activities. GTS is also designated the OTA for two agile pilot programs in FEMA's IT acquisition portfolio, Grants Outcome (FEMA GO) and National Flood Insurance Program (NFIP) Pivot.

**Mr. Mark A. Bradbury,** Principal Engineering Fellow, Technical Director and Innovation Area Lead for cyber warfare, Technical Director for the Cyber Operations, Development, and Evaluation (CODE) Center
Raytheon Intelligence, Information and Services (IIS), Cybersecurity and Special Missions (CSM)
Location: Dulles, Virginia and Richardson, Texas.

As the TD and IA Lead for cyber warfare, Mark is responsible for engineering solutions and technical direction for DoD cyber warfare programs and associated internal research and development activities. In addition, as the TD for the CODE Center, Mark provides leadership and direction in the development of the CODE Center requirements, facility, infrastructure, software and operations.

**Mr. Joseph F. Bradley, Jr., PMP, CISSP**, a member of the Senior Executive Service, is the Director of the Cyber Resiliency Office for Weapon Systems and the Director of Engineering and Technical Management for the Air Force Life Cycle Management Center at Hanscom AFB, Massachusetts. Mr. Bradley entered federal service in 1983 as an Electrical Engineer at the Naval Underwater Systems Center (now the Naval Undersea Warfare Center), Newport, R.I. performing systems engineering on the OHIO Class ICBM Submarines. Since then he has served in a broad range of senior engineering and program management positions in acquisition, sustainment, cyber security and science and technology organizations supporting USAF warfighters.

In his previous position, Mr. Bradley was the Director of Engineering and Technical Management for the Air Force Nuclear Weapons Center, Kirtland AFB, Albuquerque, NM., responsible for the development, implementation and oversight of technical policies, processes, and standards for 400+ Scientific, Engineering and Cyber professionals. As the Chief Systems Engineer for the Strategic Systems Program Executive Officer, he was responsible for systems engineering for programs acquired and sustained across the Nuclear Enterprise. As the Nuclear Weapons Center's representative on the Air Force's Cyber Resiliency Task Force, he is responsible for initiatives and activities aimed at identification and mitigation of cyber threats.

Previously, Mr. Bradley was the Deputy Director of Strategy, Operations and Resources for the Air Force's International Affairs Office (SAF/IA) at the Pentagon. Mr. Bradley was responsible for ensuring that USAF International Strategy supported National Policy and COCOM Objectives. Mr. Bradley authored the SAF/IA Strategic Plan incorporating newly developed goals and objectives and revised the organizational vision to reflect the US' strategic shift to the Pacific. He identified International Program benefits to the US Defense Industrial Base and provided monthly talking points for the Chief of Staff of the Air Force and Secretary of the Air Force.

Prior to his career broadening tour at the Pentagon, Mr. Bradley was the Director of Engineering/Chief Systems Engineer for the Air Force Program Executive Officer for Battle Management at Hanscom AFB. Mr. Bradley was responsible for the acquisition and sustainment of over 180 programs within the $140B portfolio. In addition, he provided engineering leadership, guidance, and oversight to more than 1300 scientists and engineers. Mr. Bradley has significant Foreign Military Sales experience in Eastern Europe, South America and the Mid-East. Mr. Bradley has held leadership positions in the private sector and ran his own business before returning to federal service in 2008. Mr. Bradley provided systems engineering support to programs across the Hanscom enterprise including the Objective Gateway Program, the Airborne Warning and Control System, the Digital Airspace Surveillance RADAR, the Joint Mission Planning System (JMPS), and the Cooperative Engagement Capability initiative. Mr. Bradley also supported significant strategic USAF Foreign Military Sales initiatives including the Saudi Arabian Air Force Command and Control System, the Eastern European Air Sovereignty Operations Center and the Baltic Regional Air Surveillance Coordination Center.

**C. David Brown, PhD**, **CTEP,** is the former Deputy Assistant Secretary of Defense for Developmental Test and Evaluation and former Director of the DOD Test Resource Management Center. In this dual-hatted role, he oversaw, directed, and advocated for all defense developmental testing and all of the DOD major test ranges. Before that, and again now, he is a consulting engineer for the MITRE Corporation and for the Institute for Defense Analyses in the areas of DOD acquisition program management and systems engineering. He also teaches program management and systems engineering for Johns Hopkins University. He previously served as the Director for of the Combined Test Organization for the Army Future Combat Systems. In this position, he was responsible for planning and overseeing the testing for this revolutionary development program that was transforming the Army's acquisition as well as warfighting capability. Prior to that, he was the Director for Test and Technology for the Army Developmental Test Command where he oversaw the management of all Army conducted developmental testing, technical operations at five installations of the Army's major test ranges and test sites, and test support and test technology development.

Dr. Brown also served as the focal point for the Army's application of modeling and simulation techniques to technical test and evaluation. A major initiative of his was the development of the Virtual Proving Ground, the Army's multi-million-dollar, multi-year virtual testing program. His additional work has entered the area of robotic vision, and autonomous vehicle navigation, specifically in an uncontrolled environment. Dr. Brown was a member of the Senior Executive Service, holds three patents, and has authored numerous technical papers. He is a registered Professional Engineer, is a Certified Test and Evaluation Professional, was a member of the Army Acquisition Corps, and is a retired Army Reserve Colonel. He has a doctorate degree in electrical engineering from the University of Delaware, and is also a graduate of the Industrial College of the Armed Forces.

**Diana L. Burley, PhD**, is executive director and chair of the Institute for Information Infrastructure Protection (I3P) and full professor of human & organizational learning at the George Washington University (GW). Named one of SC Magazine's Eight Women in IT Security to Watch in 2017 and the 2017 SC Magazine ReBoot awardee for educational leadership in IT security, Dr. Burley is a global cybersecurity expert who regularly consults on developing robust cybersecurity education and awareness programs, managing cybersecurity risk, assessing the threat environment, and strengthening organizational cybersecurity posture. She has testified before Congress and chaired National Academies convenings on a range of cybersecurity topics.

In 2018, the global task force she led on behalf of the world's leading computing societies published the first set of global cybersecurity curricular guidelines for post-secondary academic institutions. These guidelines, endorsed by the ACM, IEEE, AIS, and IFIP, form the foundation for the first cybersecurity degree accreditation program offered by ABET. She is a member of the US National Academies Board on Human-Systems Integration, the research staff of the Cyber Mission Operations Group of the Johns Hopkins University Applied Physics Laboratory, and the CYBER Corps Advisory Board for the Idaho National Laboratory Cyber and Homeland Security Division.

Prior to GW, Dr. Burley led the CyberCorps program and managed a multi-million-dollar computer science education and research portfolio for the US National Science Foundation. Dr. Burley has written nearly 90 publications on cybersecurity, information sharing, and IT-enabled change; including her 2014 co-authored book "Enterprise Software Security: A Confluence of Disciplines." She has secured more than $7 million in sponsored research support and served two appointments on the Cyber Security Advisory Committee of the U.S. Commonwealth of Virginia General Assembly Joint Commission on Technology & Science.

Her honors include: 2016 Woman of Influence-Public Sector/Academia by the Executive Women's Forum in Information Security, Risk Management and Privacy; the 2014 Cybersecurity Educator of the Year; and a 2014 Top Ten Influencer in information security careers. She is the sole recipient of both educator of the year and government leader of the year awards from the Colloquium for Information Systems Security Education and has been honored by the U.S. Federal CIO Council for her work on developing the federal cyber security workforce. She holds a BA in Economics from the Catholic University of America; M.S. in Public Management and Policy, M.S. in Organization Science, and Ph.D. in Organization Science and Information Technology from Carnegie Mellon University where she studied as a Woodrow Wilson Foundation Fellow.

**Mr. Daniel T. Carroll,** Office of the CTO, Cybersecurity Practice, Dell EMC Federal. Dan Carroll leads the cybersecurity practice development for the Office of the CTO, Dell EMC Federal. He focuses on designing and implementing cybersecurity frameworks to help Federal customers meet their diverse cybersecurity missions. Dan works with the cybersecurity community to gather critical requirements to shape the products and solutions for Dell EMC government customers

Prior to Dell EMC, Dan held the position of head contract negotiator at NetApp for enterprise service agreements with the Fortune Global 500. His responsibilities included government and commercial organizations.

Dan served in the U.S. Marine Corps and was stationed at Marine Corps Base Quantico, VA. He participated in development and implementation of the initial Navy Marine Corps Intranet (NMCI). NMCI established an interoperable command and control network that provides the IT platform necessary for transitioning to a net-centric environment.

**Mr. Peter H. Christensen, CTEP,** is employed by the MITRE Corporation. Pete is currently assigned as the Cyber Lead for MITRE's work in support of the Deputy Assistant Secretary of Defense (DASD) for Information and Integration, Portfolio Management, Cyber Directorate. In other MITRE roles, he supported the Office of the Secretary of Defense (OSD) Program Division as Test and Evaluation Portfolio Manager, Naval Sea Systems Department Head, and Lexington Park Site Lead.

From 2014 through 2017, Pete was asked to serve on Intergovernmental Personnel Assignment (IPA), with Test Management Resource Center (TRMC), as the Director, National Cyber Range (NCR). In that role Pete was responsible for customer outreach, event planning and execution of Cybersecurity Test & Evaluation (T&E) and Training events conducted at the NCR, including Program Management of the NCR Contract and NCR Complex expansion. Under Pete's leadership, NCR utilization dramatically increased and the Government, FFRDC, Contractor Team successfully executed over 200 events.
As MITRE's Test and Evaluation Portfolio Manager, Pete was responsible for coordinating Test and Evaluation Activities for several Acquisition and Technology and Logistics and OSD Sponsors. Pete supported the DASD for Developmental Test and Evaluation, the TRMC and the OSD, Director of Operational Test and Evaluation (OT&E).

From 2001 through 2006, Pete served as an IPA in Scientific Advisory Roles with the Marine Corps Operational Test and Evaluation Activity. Pete led two Operational Test Agency Initiatives to address OT&E of Information Assurance and Interoperability Testing. Pete concurrently provided oversight and direction to the OT&E for several programs undergoing OT&E including the M777 Lightweight 155 Howitzer and Expeditionary Fighting Vehicle.

Pete is an Adjunct Professor at Capitol Technology University in Laurel Md. For the last 12 years, since 2006, he has taught courses in the Cybersecurity Master's Program on Network Systems Security Concepts and Malicious Software.

Pete is a retired U.S. Navy Commander. He had a wide range of assignments as a Naval Flight Officer flying over 2200 Hours and 550 Carrier Landings in EA-6B Prowlers. His last Navy assignment was as a Program Manager in the Advanced Tactical Aircraft Protection Systems Program Office where he managed three Electronic Warfare programs. His last operational flying tour was with VAQ-136 on USS Midway.

Pete is an active member of the International Test and Evaluation Association (ITEA), a Certified Test and Evaluation Professional (CTEP), has served on the ITEA Board of Directors and authored many articles in *The ITEA Journal of Test and Evaluation*.

---

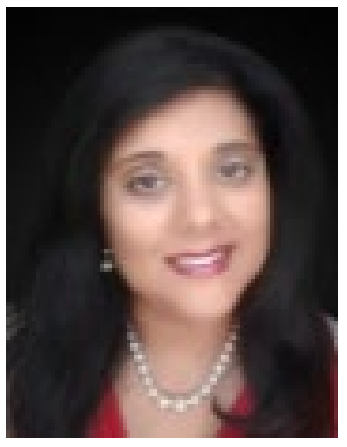
**Mike Cobb, PhD,** is a DAU Professor of IT and Cybersecurity.

Prior to joining DAU, Mike served as the director of the School of Computer Science and IT at Stratford University and the Director of Operations at the Inter-American Defense College.

He retired from the United States Army in August 2009.

---

**Portia I. Crowe, PhD**, serves as the Chief of Cyber Engineering for the U.S. Army Program Executive Office Command, Control and Communications-Tactical (PEO C3T). She is responsible for providing a full-spectrum, systems-of-systems approach to securing, advancing and synchronizing cyber defense activities, cyber security, and information management. She works closely with industry partners and academia to ensure freedom from danger in cyberspace dealing with communication networks, crypto devices, tactical radios and mission command assets. Dr. Crowe maintains an advanced understanding of the cybersecurity industry using her technology, engineering and cyber expertise.

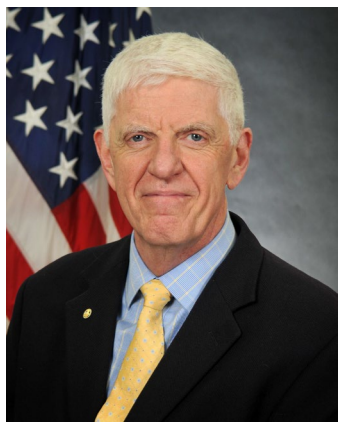


Dr. Crowe engages in Science, Technology, Engineering and Math activities and advises K-College curriculums in system engineering and cybersecurity. She is also a member of various esteemed science and technology advisory councils.

Dr. Crowe holds a Bachelor of Science in Computer Science from Rutgers University, a Master of Science in Engineering Management from New Jersey Institute of Technology, a PhD in Systems Engineering from Stevens Institute of Technology, a Cybersecurity Graduate Degree from UMUC and Seton Hall Law training in Cyber Law, Policy and Data Privacy. She has over 10 publications to include IEEE and INCOSE, various journals and the Army's AL&T publications.

**Mr. Gregory "Greg" P. Curth**, Joint Staff J6/DDC5I/C5 Assessments Division, Suffolk, VA. Mr. Greg Curth is a retired US Navy Captain Aviator serving as the Deputy Cyber Capability Integration Element Lead for the Joint Staff J6/Deputy Director Cyber and Command, Control, Communications, Computers, Cyber and Integration (C5I)/ C5 Assessments Division (C5AD). The C5 Assessments Division conducts assessments of existing and emerging Cyber and C4 capabilities in a persistent environment to achieve interoperable and integrated solutions that satisfy joint, interagency and mission partner operational requirements.

In 2013, Mr. Curth joined the J6 C5 Assessments Division with General Dynamics Information Technologies supporting numerous interoperability and cyber projects. In 2015 he was hired as a Government Employee leading the cyber capability assessment team under the assessments branch. In 2017 he took over the project lead for the DoD Enterprise Cyber Range Environment (DECRE) Command and Control Information systems (C2IS) integrating C5AD's cyber capabilities with other DoD designated ranges to provide a close loop distributed environment for cyber assessments and training. Responsible for leading the operational capability development of the DoD Enterprise Cyber Range Environment. As the event director he leads the training for CCMD CMFs mission rehearsal, defense of Key Cyber Terrain, development of advanced Tactics, Techniques and Procedures (TTP), and executes Command and Control of Cyberspace against advanced valid cyber threats. This innovative approach supports quantifiable measurement of threat cyber effects, effectiveness of cyber detection and prevention tools, cyber effects on blue force mission and C4I mission capabilities, and demonstrates the effectiveness of blue force cyber response actions in an operationally realistic environment. This environment will enhance 133 Cyber Mission Teams ability to conduct mission rehearsal, team training, training, techniques, and procedures (TTPs) development and certification.



From 1977 to 2013, Mr. Curth served in the US Navy, starting out as a Submarine Sonar Technician, then earned his commissioned, Naval Aviator Wings and completed various flying operational tours deploying around the globe in the venerable SH-60B to include an Instructor Pilot tour at HSL-40. He Commanded Tactical Air Control Squadron 21 and later served on the Commander Second Fleet Staff and finally at Navy Warfare Development Command in Norfolk, Virginia.

He has an undergraduate degree in Computer Science from Villanova University and has earned a Masters in Information Systems from George Washington University. He is a graduate of the Army's Command General Staff College and the Armed Forces Staff College. Mr. Curth is also designated a Certified Information System Security Specialist (CISSP) and a Certified Ethical Hacker.

---

**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.

---

**Ms. Rose Daley** has over 30 years of experience as a cyber and software systems engineer, including her most recent activities analyzing resilience for weapons systems and improving operational efficiency for defensive cyber operations. She has both architected and implemented large-scale software systems for the Navy, the Intelligence Community and Federal civilian government. In addition to cyber defense operations, her broad software experience ranges from shipboard combat systems and shore-based training to desktop applications and enterprise-class information systems on both open and closed networks. She holds an M.S. in Computer Science from the Johns Hopkins University, and B.S. in Electrical Engineering from Rensselaer Polytechnic Institute.

---

**Mr. Jonathan Davis** currently resides in Havre de Grace, Maryland with his wife Lisa. He works for the MITRE Corporation, a non-profit government organization. His current role is as a Security Architect supporting the National Background Investigation Service (NBIS) with a goal of revamping the security clearance investigation process.

He is also a Chief Warrant Officer 3 in the US Army Reserves, with a primary MOS of 170A – Cyber Operations Technician. He is currently with a CPT located at Fort Dix working towards their Initial Operating Capability, enabling them to engage in the digital landscape.

He has a Bachelor of Science in Information Technology from Kutztwon University and is currently pursuing a Master of Science in Information Security Engineering from the SANS Technology Institute. He treats the DoD Approved 8570 Baseline Certifications positions as a personal checklist and can operate in majority of the roles.

---

**Tom Donnelly, PhD,** works as a miller of the SAS Institute supporting users of JMP in the Defense and Aerospace sector. He has been actively using and teaching analytical and modeling methods – particularly Design of Experiments – for the past 35 years.

Donnelly joined SAS in 2008 after working as an analyst for the Modeling, Simulation & Analysis Branch of the US Army's Edgewood Chemical Biological Center (now Army Futures Command CDC CB). There, he used DOE to develop, test, and evaluate technologies for detection, protection and decontamination of chemical and biological agents.

Tom received his PhD in Physics from the University of Delaware.

**Mr. Gene Downs** is currently a senior program manager at Trideum Corporation in Huntsville, AL, where he is responsible for an effort to establish a prototype weapon system cybersecurity test capability for Redstone Test Center. He has over 30 years of experience with developmental testing and systems engineering on Army and Air Force projects. These include: Eight years of acquisition program support to two project offices: The Joint Tactical Unmanned Aerial Vehicle project office supporting the Hunter First Article Test / System Qualification Program, and the Robotic Systems / Joint Project Office seeking to apply Simulation Based Acquisition concepts to their system development programs; Eight years as the Army requirements lead on a Navy led Central Test and Evaluation Investment Program (CTEIP) effort to establish an enterprise level capability to enable real-time cross domain resource interoperability for DoD T&E; Four years creating and testing a prototype counter IED detection system that included over 400 test runs; Four years creating and testing manned and unmanned aircraft towed systems; Two years drafting test operating procedures for unmanned air and ground systems and systems of systems; and, Two years restructuring the corporate and contract specific safety program needed for employees conducting hands-on demilitarization and disassembly of rockets and missiles. This included the removal of warhead and propellant grain energetic material from their casings as well as conducting remote segmentation of rocket motors using a water-cooled bandsaw and other methods.

**Mr. Bernard "Chip" 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 a defense industry company where he was a Senior Analyst, Division Manager, and Operations Manager, and Corporate Vice President -- all supporting test and evaluation in the DoD. During his time with industry, 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 was very grateful for the opportunity to become part of the JMETC Team. JMETC has demonstrated its value over the past ten years and looks forward to meeting the challenges of the future, particularly in the Cyber arena. Now Mr. Ferguson has taken responsibility as the Deputy to the Cyber Test Range Executive Agent, to stand up that office and assist in making the DoD cyber test infrastructure efficient and effective.

**Mr. John Forte** currently serves as the Deputy Executive for JHU/APL's Homeland Protection Mission Area. His programs focus on securing the nation and its interests against asymmetric, terrorist-type attacks of catastrophic consequence through applied technology and systems engineering. Defeating chemical, biological, radiological, nuclear and explosive weapons as well as countering advanced persistent cyber threats is the mission area's central challenge. John is the Mission Area's lead in assured communications as well as in understanding and mitigating cyber threats of national importance, to include threats to state and local environments, critical infrastructure and to senior leaders and first responders. He serves on the Board of Advisors to JHU's Information Security Institute (ISI) on various aspects of cybersecurity in support of their focus on research and education in information security, assurance and privacy.

John is also the founder and Co-Director for the JHU Institute for Assured Autonomy. Conducting intelligent and autonomous systems assurance research and establishing partnerships across government, industry and academia for the safety, trust and security of the convergence of IoT, networks and infrastructure, artificial intelligence, machine learning and robotics within real-world environments.

John has served in multiple senior leadership and technical positions within the military and in the public and private sectors. He earned a BSEE from the University of Tulsa and an MSEE from George Washington University with a focus in Communications and Networks. John also completed Executive Programs at the Harvard Kennedy School on Cybersecurity: Intersection of Policy and Technology; as well as on National and International Security.

**Mr. Matthew J. Frandsen** is the Chief, Cyber Test Operations Division, Headquarters Air Force Operational Test and Evaluation Center, Kirtland Air Force Base, NM. He serves as the HQ AFOTEC staff lead for OT&E of system cyber capabilities. His responsibilities include establishing procedures for executing A-3 intent for OT&E of system cyber capabilities and product standardization across AFOTEC detachments; monitoring test planning, execution, reporting and closeout activities to provide timely access to current cyber intent; and reviewing and coordinating on production of test plans and reports. He is responsible for maintaining the AFOTEC Cyber Support Package, supporting AFOTEC cyber-specific OT training, and representing AFOTEC in cyber test-related working groups across the acquisition community that have AF and DoD-level impacts.

Mr. Frandsen was commissioned in the United States Air Force in 1986 upon graduation from the United Sates Air Force Academy. During his active duty career, he served in various positions including 92nd Information Warfare Aggressor Squadron Operations Officer, 744th Communications Squadron Commander and 49th Mission Support Group Deputy Commander. He was also deployed in support of Joint Task Force Andrew and Operations SOUTHERN WATCH, NOBLE EAGLE, and ENDURING FREEDOM before retiring from active duty in May 2012.

Mr. Frandsen rejoined the Air Force as a civilian in August 2012. Prior to his current position, he served as the Kirtland Air Force Base Information Technology Director.

**Lt Col Benjamin "WIMS" George** is currently serving as the Commander of 346th Test Squadron, Joint Base San Antonio – Lackland, Texas. As the Commander, Lieutenant Colonel George leads the 190-member squadron in conducting cyberspace operational testing and evaluation, and cyberspace assessments, as well as providing the Cyber Test and Training Range for the Air Force and other mission partners. Lieutenant Colonel George is married to his wife, Kelly, and has four children.

Lt Col George was commissioned in 2000 as a distinguished graduate of the U.S. Air Force Academy. He earned a MS in Mechanical Engineering from George Washington University's Joint Institute for the Advancement of Flight Sciences at NASA Langley Research Center, VA. He served as the Executive Officer to the Director of the Space and Missile Systems Centers, Detachment 12, Kirtland AFB, NM where he also supported space flight test and evaluation. In 2005, he graduated from the U.S. Air Force Test Pilot School, earning the Raymond L. Jones Award as the top engineer graduate.

As a Flight Test Engineer at Eglin AFB FL, Lt Col George conducted developmental flight tests on the F-16, F-15, and Air-to-Ground munitions. Following an assignment as Chief Engineer and Assistant Director of Operations for the Department of the Air Force, Lt Col George was selected as an Air Force Technical Fellow with the Department of Energy at Oak Ridge National Laboratory, TN. Additionally, he served as the Anti-Tamper Program Element Monitor for the Special Programs Directorate of the Office of the Assistant Secretary of the Air Force for Acquisition, Pentagon, Washington, D.C.

**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.

**William J. Hughes,** Cost Analysis and Research Division (CARD), Institute for Defense Analyses (IDA). Mr. Hughes is currently an Adjunct Research Staff Member with CARD at IDA. He began working for IDA in Sept, 2010. Currently he is working assignments to define 5th Generation Air-Air threats, supporting JIDO on advanced techniques, and sustainable range issues.

Prior to retiring after 43 yrs. of Government Service, and Joining IDA, Mr Hughes was the Director of the Joint IED Defeat Test Board. Bill established the C-IED T&E facilities, developed; protocols for T&E, threat assessments and test articles, interoperability testing across the services and the international community, and testing in direct support of theater requests. He integrated live, virtual, and constructive scenarios across services and test ranges and coordinated efforts across the DOD, COCOMs, and OGAs.

In prior assignments, Bill was the Associate director of the Army Evaluation Center and the Evaluation Analysis center and Division Chief of the Chemical/Biological/Nuclear Effects Division in ARL, all of which he played a major role in establishing.

Bill also chaired the US technical negotiating team in support of the Coordinating Committee for Multilateral Export Controls (COCOM) negotiations for the State Department, was an Operations Research Analyst in AMSAA, and was an Electronic Warfare Technician for the Navy. (He started his career as a WG-1).

Bill holds a BA in Mathematics from Rutgers University, a 4 yr apprenticeship in Electronic Warfare from the Navy and was a Mid-Career Fellow, Princeton University, Woodrow Wilson School of International Affairs

Mr. Hughes has received numerous awards including, two DARCOM Systems Analysis Awards, the ITEA General Powers award, three Superior Civilian Service Medals, the Meritorious Civilian Service Medal and the Exceptional Civilian Service Medal.

---

**Mr. Paul C. Johnson** has a Master's of Science in Operations Research from the Florida Institute of Technology and currently serves as the Scientific Advisor for the Marine Corps Operational Test and Evaluation Activity (MCOTEA), Quantico VA. MCOTEA conducts operational tests and evaluations of Marine Corps equipment prior to fielding with the operational forces.

---

**Ms. Ashley Kamauf** is the Inspection Body Program Manager for the American Association for Laboratory Accreditation (A2LA). She supports the day-to-day operations of accreditation by assisting A2LA clients in obtaining and maintaining accreditation to ISO/IEC 17025 and ISO/IEC 17020. As a member of the Inspection Body and Materials testing team, she deals with Mechanical, Information Technology, and Acoustics & Vibration testing laboratories, as well as being the primary point of contact for all organizations in the Cybersecurity Inspection Body Program, including the Federal Risk and Authorization Management Program (FedRAMP). The initial qualification to become a FedRAMP Third Party Assessment Organization (3PAO) is to gain accreditation through A2LA, which is a process that Ashley facilitates. In addition to her daily tasks, she performs on-site quality system assessments and performs oversights of A2LA assessors. She also conducts training, on behalf of A2LA, for CABs and assessors on the ISO/IEC 17020 standard.

---

**Patrick (Pat) J. Kastner** is the acting Deputy Director for National Preparedness Programs and the Test Area Manager for Aviation Systems, in the Test and Evaluation Division, S&T. His portfolio currently includes DHS Level I and designated Level II aviation acquisition programs for fixed, rotary, and unmanned aircraft supporting the Coast Guard and CPB, and USCG surface ships. His previous assignment was with the Army Test and Evaluation Command (ATEC). He is retired Army, serving in Aviation and Acquisition assignments.

Pat's previous acquisition assignments include Assistant Program Manager, Target Acquisition Detection System/Pilot Night Vision System (TADS/PNVS) for the AH-64 Apache program office, and Product Manager for the M/AH-6 Mission Enhanced Little Bird (MELB) for the U.S. Army Special Operations Command.

Pat is a 1979 graduate of the United States Military Academy at West Point, N.Y., and has a M.A. in Procurement and Acquisition Management. He presently holds DAU and DHS Acquisition Level III certifications in Test and Evaluation, and Program Management.

---

**William (Bill) L'Hommedieu** is the Chief Engineer for the Avionics Cyber Range supporting the 96th Cyber Test Group. He is a Certified Information Systems Security Professional since 2007. Bill started his career in the U.S. Navy as a Cryptologic Technician in 1979, he left the Navy in 1984 to work as a contract network engineer starting at CINCLANTFLT, Norfolk, VA and then moving to Eglin AFB in 1986. Taking advantage of adult education available at Eglin AFB, He received his B.S. in Electrical Engineering Technology from Troy State University in 1994. During this time, he began to experiment with personal computers honing the skills needed in the new area of computer and network security. After graduation, Bill took on the role as the lead network engineer for Air Force Air Superiority Office. He designed and engineered a compartmented special access network fiber optic network capable of physically segmenting networks on demand, logically/physically isolating data storage and providing secure and logically isolated email across different programs. In 2003, recognized as an expert in computer security Bill was brought over to the 46th Test Squadron to start an information assurance test program which became 46 TS I-Flight where Bill was named the flights Technical Advisor. Bill currently serves as the Chief Scientist supporting the Cyberspace Test Technology, Science and Technology (S&T) Executing Agent. Additionally, Bill supports the 96th Cyber Test Group with technical direction and advice on Cyberspace investment programs. When not figuring out the latest hacker technology, Bill is an automotive enthusiast where he occasionally drives in high performance driving events and tinkers on all sorts of mechanical and electrical gadgets.

**Mr. Patrick Lardieri** is a Lockheed Martin Fellow and is the Technical Director for Lockheed Martin's smi. Mr. Lardieri has worked the NCR program throughout its lifecycle, spanning its inception as a technology research program under the Defense Advanced Research Projects Agency (DARPA) through its present form as an operational cyber testing and training range for the DoD's Test Resource Management Center (TMRC).

Mr. Lardieri is recognized by DARPA, TRMC, the NCR user community, and Lockheed Martin as one of the principal leaders that brought the NCR from concept to reality. He has contributed to the design, implementation, and operation of all aspects of the NCR, including building a technical 100+ person staff that includes cyber operations, networking and IT, system testing, cyber training, and software development experts. In collaboration with government partners, Mr. Lardieri has led 30+ events on the NCR for users from multiple services and government organizations. Mr. Lardieri has been recognized for his leadership and contributions to the NCR by Lockheed Martin as a member of the NCR Nova Award team, by TRMC via formal citation, and by range users in written and verbal feedback.

Over his 29+ year career at Lockheed Martin, Mr. Lardieri has served as the technical lead for multiple DARPA, AFRL, and ONR applied research programs in automated cyber testing (e.g., DARPA NCR), distributed real time computing (e.g., DARPA PCES and ARMS), adaptive networking (e.g., DARPA SAPIENT), software producibility (e.g., AFRL SPRUCE), and intelligent training (e.g., ONR AET). He has published more than 20 papers and given multiple invited talks and keynotes at refereed conferences. Mr. Lardieri has participated in several DoD technology policy planning workshops on software producibility and security challenges. Within Lockheed Martin, Mr. Lardieri has supported tiger-team reviews and technology transition into key DoD programs, including Aegis Open Architecture, DDG-1000, and JSF.

Mr. Lardieri holds Bachelor of Arts in mathematics and Bachelor of Science in electrical engineering from Rutgers University and a Master of Science in electrical engineering from University of Pennsylvania.

Mr. Lardieri is currently a member of USAF Scientific Advisory Board, SEI Technical Assessment Group, and the Senior Advisory Board, AJ Drexel Cybersecurity Institute.

---

**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.


---

**Melanie L. Loncarich, PhD,** is currently serving as the Special Assistant for Policy and Education at the Deputy Under Secretary of the Army - Test and Evaluation. She is responsible for policy and education across the Army Test and Evaluation Enterprise. She is the Test and Evaluation Acquisition Functional Adviser and chairs the Secretary of the Army chartered Test and Evaluation Manager Committee. Dr. Loncarich manages the Department of the Army Test and Evaluation Master Plan approval process and represents Army Test and Evaluation on Office of the Secretary of Defense efforts.

Dr. Loncarich began her Federal career at the U.S. Army Aberdeen Proving Ground in 1999, spending the first 8 years as a Developmental Test Manager in the Command, Control, Communications, and Computers (C4) Division at the U.S. Army Developmental Test Command. In 2007, she acquired a Project Analyst position in the Test Technology Directorate at the Army Test and Evaluation Command (ATEC) and then temporarily served as the Assistant to the ATEC Technical Director. That assignment postured Dr. Loncarich for a leadership position as the Chief the Mission Command and Integration Division at the U.S. Army Evaluation Center.

Dr. Loncarich earned a Doctor of Management degree from the University of Maryland, University College with expertise in Knowledge Transfer in Multigenerational Organizations. She holds a Master's Degree in Computer Engineering from Loyola University, a Master's of Business Administration in Finance from Wilmington University, a Master's of Business Administration in Management Information Systems from Wilmington University, and a Bachelor of Science degree in Aviation Science with concentration in Software Engineering from the University of Maryland Eastern Shore.

Dr. Loncarich has over 19 years of service with the Department of Defense as a Federal Civilian. She completed the Defense Acquisition University Senior Service College Fellowship in 2016 and the Executive Leadership Development Program in 2012. Her awards include the Federal Executive Board "Rookie of the Year", Superior Civilian Service Award, Commander's Award for Civilian Service, Achievement Medal for Civilian Service, and Certificates of Achievement.

---

**John McKay, PhD**, is a research and development engineer at the Applied Research Laboratory at Pennsylvania State University focusing on sonar image processing. He recently completed his electrical engineering doctoral program at Penn state where he studied synthetic aperture image formation and analysis.

He had previously earned a master's degree in applied mathematics with emphasis in ecological and epidemiolocal modeling at Arizona State University and a Bachelor's in pure mathematics at the University of Pittsburgh. His current interests are sonar/radar specific neural network architectures, phase inclusive classification algorithms, and frequency domain methods for synthetic aperture imaging.

**Mr. Robert "Rob" McKelvey** has been a part of the Army Evaluation Center's Survivability Directorate since May 2006.

His Live Fire experience comes from combat and tactical vehicle programs like the Mine Resistant Ambush Protected (MRAP) Family of Vehicles (he was the live fire lead for all MRAP All-Terrain Vehicle (M-ATV) variants) and led the first use of Home-Made Explosives for under-vehicle blast testing. He was also a Lead Evaluator and Test Manager on Joint RPG and RKG Defeat Systems.

His work with RPG Defeat Systems and the M-ATV was directly applicable for the Forward Operational Assessment (FOA) Team, so he was deployed to Kabul, Afghanistan, with FOA #20 from January to July 2013 as the team's Survivability Subject Matter Expert. He became dual-hatted following a team injury and was elevated to FOA #20's Acting Deputy Commander late in the tour.

He served as the Assistant Technical Director of the Aberdeen Test Center over a one-year long developmental assignment. His duties included steering future interoperability standards as a Victory Standard Support Office Member, chairing coordinated testing between Army test ranges, leading the engineering and development of an Aberdeen National Cyber Range proposal, and championing over 290 other strategic test center initiatives.

He currently serves as the Army's Lead Cybersecurity and Electronic Warfare Evaluator for Robotic and Autonomous Systems.

He holds a Bachelor of Mechanical Engineering from Penn State and a Master of Program Management from the Naval Postgraduate School.

**Jeff McNeil, PhD**, Principal Investigator, Test Capabilities Development is a professor within the Clemson University Watt Family Innovation Center, presently dedicated to full-time research supporting Test Capability Development for the DoD Executive Agent for Cyber Test Ranges. After receiving a bachelor's degree in physics from the University of Nebraska-Lincoln, Dr. McNeil has spent over 26 years serving across government, industry, and academia. A US Marine Corps Reserve Colonel, his recent military billets include Intelligence Plans and Operations Officer for Marine Forces Central and Pacific Commands, Joint Concept Development and Experimentation Deputy Director for International Engagement, US Strategic Command Assessment Officer, US Pacific Command Cyberspace Plans Officer, and currently Senior International Affairs Analyst for National Defense University. 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 Ph.D. 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.

**Tom Meservy, PhD,** is an Associate Professor of Information Systems at Brigham Young University. He received a Bachelor's in Management and a Master's Degree in Information Systems Management in 2001 from BYU and then worked in industry as a software developer and architect. In 2007 he received a PhD in Management and a minor in Cognitive Science from the University of Arizona. While in graduate school, he developed software systems to automatically track human behavior to augment humans in detecting deception. He spent 5 years at the University of Memphis and now has been at BYU for 7 years. He is affiliated with the Systems Testing Excellence Program at the FedEx Institute of Technology/University of Memphis. He enjoys consulting related to his areas of expertise.

As an academic he has published numerous articles in the most prestigious Information Systems journals and conferences. In general, his research looks at how technology can be used to augment human abilities to generate, share, and evaluate information. Tom uses a variety of research methods and tools including computer vision techniques, eye tracking, and fMRI (brain imaging). Much of his research has been funded.

Tom loves to teach and has received several teaching awards including the University-wide teaching award at the University of Memphis. Currently he teaches classes about enterprise infrastructure and networking including trends related to virtualization, containerization, and the cloud. Tom has numerous technical certifications including certifications from Microsoft, Oracle, Cisco, and Amazon Web Services.

He enjoys skiing and traveling with his wife and 5 children (ages 6-18). He lived for two years in Guatemala, speaks Spanish, and has roasted marshmallows over a volcano!

**Ms. Ellena S. Millar** has over 20 years of IT/Cybersecurity experience in both commercial and government sectors.

She began her DoD career at Defense Information Systems Agency - Europe in Stuttgart, Germany. She was first introduced to what was previously known as Information Assurance when she served as the lead for active RFID implementation for the Naval Expeditionary Forces. Shortly after, she made the transition from tactical IT to Cybersecurity.

She served in various cybersecurity roles, in hindsight, that prepared her for the position she holds today. She supported program offices as an Information Systems Security Engineer and a fully qualified validator navigating through the challenges of implementing DoD/DON cybersecurity policies. She worked as a Security Assessor before joining the Office of Designated Approving Authority office, now known as the Navy Authorizing Official (NAO).

At the NAO office, she led several Echelon II organizations through the Certification and Accreditation process. She was also part of the Navy's Enterprise Mission Assurance Support Service (eMASS) initiative from its infancy, which in an integral part of the Risk Management Framework process today.

In 2012, she was nominated as the Deputy Director of the Cyber Readiness Directorate at Navy Information Operations Command - Norfolk and eventually fleeted up as the Director. She led the Navy Red Team, Blue Team and the Naval OPSEC Support Team supporting COCOM level Fleet and Joint exercises, readiness assessments, web risk assessments and OPSEC training. She also supported real-world operations under the direction of FCC/C10F. She earned her second Navy Meritorious Service Award for her leadership and dedication during Operation Rolling Tide.

Ms. Millar joined COMOPTEVFOR in October 2015 where she leads the Navy Cybersecurity Operational Test and Evaluation mission with an organic red team. In 2016, her team began implementing the Cyber Survivability Evaluation to shift the focus from compliance vulnerabilities to cyber-attack kill chain and its impact on the warfighting mission. Her strategic vision continues to focus on being relevant and value added to the warfighters aligning to COMOPTEVOR's vision – to be the "Voice of operational truth with the Fleet".

---

**Col Hans Miller, USAF (ret)**, is a Principal Test and Evaluation Subject Matter Expert at the MITRE Corporation. He retired with over 25 years of experience in combat operations, experimental flight test, international partnering, command and control, policy, and strategic planning of defense weapon systems. His last assignment was as Division Chief of the Policy, Programs and Resources Division, Headquarters Air Force Test and Evaluation Directorate at the Pentagon. He led a team responsible for Test and Evaluation policy throughout the Air Force, coordination with OSD and Joint Service counterparts, and staff oversight across the spectrum of all Air Force acquisition programs. Prior to that assignment, he was the Commander of the 96th Test Group, Holloman AFB, NM. The 96th Test Group conducts avionics and weapon systems flight tests, inertial navigation and Global Positioning System tests, high-speed test track operations and radar cross section tests necessary to keep joint weapon systems ready for war.

Hans Miller was commissioned as a graduate of the USAF Academy. He has served as an operational and experimental flight test pilot in the B-1B and as an F-16 chase pilot. He flew combat missions in the B-1B in Operation Allied Force and Operation Enduring Freedom. He served as an Exercise Planning Officer at the NATO Joint Warfare Center, Stavanger, Norway. Col (ret) Miller was the Squadron Commander of the Global Power Bomber Combined Test Force coordinating ground and flight test activities on the B-1, B-2 and B-52. He served as the Director, Comparative Technology Office, within the Office of the Secretary of Defense. He managed the Department's Foreign Comparative Testing, and Rapid Innovation Fund programs.

Hans Miller is a Command Pilot with over 2100 hours in 35 different aircraft types. He is a Department of Defense Acquisition Corps member and holds Level 3 certification in Test and Evaluation. He is a graduate of the USAF Weapons School, USAF Test Pilot School, Air Command and Staff College and Air War College. He holds a bachelor's degree in Aeronautical Engineering and a master's degree in Aeronautical and Astronautical engineering from Stanford University.

---

**Ms. Colleen Murphy** is a Principle Contracting and Acquisition Subject Matter Expert at The MITRE Corporation. Colleen has supported a variety of projects across Defense and Civilian agencies exploring innovative acquisition and contracting solutions such as Middle Tier of Acquisitions and Other Transactions, as well as techniques to accelerate capability delivery. Colleen works with acquisition executives to develop acquisition and contracting solutions for business and weapons systems and Agile development. She is a contributing member of the Acquisition in the Digital Age (AiDA.mitre.org) acquisition platform. Prior to joining MITRE, Colleen was a Lead Contract Analyst at CACI, and a Contract Specialist as an active duty member of the U.S. Air Force. She holds a Master of Business Administration degree from Virginia Tech.

---

**Mr. Terry Murphy** has for 42 years positively impacted our nation's security. Since October 2016, Mr. Murphy has served as Deputy Director, Policy and Workforce Development within the Department of Homeland Security (DHS) Office of Test and Evaluation.

In his current role, he develops, staffs, and adjudicates key DHS Test and Evaluation (T&E) policy directly impacting Office of Test and Evaluation responsibilities and authorities. Mr. Murphy joined DHS July 2015.

He previously served as Senior Analyst within the Office of the Deputy Assistant Secretary of Defense, Developmental Test and Evaluation from 2011 to July 2015. During this time Mr. Murphy led the update of DoD T&E policy; and development of the T&E Management Guide, Cybersecurity T&E Guide, and Incorporating T&E into Acquisitions Guide.

From 2007 to 2010, as T&E Manager for Combat Support Equipment, Marine Corps Systems Command, Mr. Murphy supported system portfolios including Medical, First Responders, and Shelters to facilitate real-world operations.

From 2002 to 2007 Mr. Murphy served as T&E Lead in support of Joint Project Manager – Chemical, Biological, Radiological, and Nuclear Individual Protection (IP) programs. These programs provide the chemical and biological individual protection equipment used by our military and first responders.

Mr. Murphy served 26 years in the U.S. Marine Corps. Mr. Murphy earned a BA in Social Science from Chapman University in 2001; and an MA in Management (2002) and a MS in Engineering (2010), both from National University. He holds DHS Level III certifications in Test and Evaluation and Program Management, and is a certified Project Management Professional (PMP).

**Mr. Arch Owen** is the Program Manager for Weapon Security within Draper's Combat Solutions Program Office. In this role, Mr. Owen oversees a broad range of efforts to secure weapon systems, spanning the full range of threats: e.g. everything from operating in GPS-degraded/denied environments to protecting from deeply embedded software vulnerabilities within the weapon software. Across the portfolio, Mr. Owen is working to bring advanced security techniques to address the challenges the US DoD faces in securing weapon systems from Nation State adversaries. 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.

**Sandeep Pisharody, PhD**, is a technical staff member in the Cyber Operations and Analytics Technology Group at MIT Lincoln Laboratory, working on identifying and recommending ways to improve the cyber defensive posture of US government systems. His areas of interest include network and cloud security, modeling and simulation, metrics development, and analysis of cyber operations.

Prior to joining Lincoln Laboratory in 2017 he spent over ten years in the industry, working as a Network/Security Engineer at Sprint Corp., Iveda Corp., Apollo Education Group, and Insight. Dr. Pisharody holds a BS in Electrical Engineering, a BS in Computer Engineering and an MS in Electrical Engineering from the University of Nebraska – Lincoln. He completed his PhD in Computer Science from Arizona State University.

**Ms. Kimberly Ploskonka** serves as the Deputy Director, Space and Terrestrial Communications Directorate (S&TCD), under the U.S. Army's Combat Capabilities Development Command (CCDC); Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) Center at Aberdeen Proving Ground, Maryland.

As the Deputy Director, Ms. Ploskonka is responsible for managing a technically diverse organization of approximately 400 government and 300 contractor personnel. She assists the Director in providing the strategic direction for the organization and leading research, development, and engineering in resilient, survivable military communications, autonomous and intelligent networking, network situational understanding, cyber electromagnetic activities and cyber defense.

From April to October 2017, Ms. Ploskonka served as the Acting Director, S&TCD CCDC C5ISR Center (previously known as the Communications-Electronic Research, Development and Engineering Center, or CERDEC).

Ms. Ploskonka's prior assignments include: Chief, Tactical Communications Division, CCDC C5ISR Center from June 2012 to February 2017 and Chief, Systems Engineering, Architecture, and Modeling & Simulation (SEAMS) Division, CCDC C5ISR Center from April 2010 to June 2012 at Aberdeen Proving Ground, Maryland. From March 2008 to April 2010, Ms. Ploskonka served as the Chief, Army Systems Engineering (ASE) Branch in the SEAMS Division, CCDC C5ISR Center at Fort Monmouth, New Jersey and as an Electronics Engineer, Tactical Communications Division, CCDC C5ISR from June 2000 to March 2008 at Fort Monmouth, New Jersey.

Ms. Ploskonka's educational achievements include a Bachelor of Science degree in Chemical Engineering from Rutgers College of Engineering in Piscataway, New Jersey in 1996; an Executive Master of Technology Management from Stevens Institute of Technology in Hoboken, New Jersey in 2002; and a Master of Accountancy, specializing in Governmental Accounting, from Rutgers School of Business in New Brunswick, New Jersey in 2015.

Ms. Ploskonka achieved Level III Certification in Engineering, Science and Technology Management in the Army Acquisition Corps.

Her awards include the U.S. Army Commander's Award for Civilian Service in 2018 and the U.S. Army Achievement Medal for Civilian Service in 2009.

**Ms. Jennifer Rekas** is a Senior Agile Systems Engineer with The MITRE Corporation*. She has led numerous Agile/DevOps transformations across a wide variety of DoD, Intelligence Community and Federal Civilian Agencies and regularly provides DevOps training and agile coaching for MITRE sponsors looking to adopt agile practices to deliver better and faster. Jennifer also leads a multidisciplinary team of systems and software engineers to mature DevOps capabilities and enable more effective application in the government domain. Her current research interests include how to utilize DevOps metrics to enable rapid decision making by senior leadership and how-to tailor recognized commercial agile practices for large scale, multi-vendor mission critical DoD systems of systems. Before joining MITRE, Jennifer was a software systems engineer with commercial, government contractors, and other FFRDC organizations.

**Mr. Randall (Randy) Rice** is a leading author, speaker, consultant and practitioner in the field of software testing and software quality. He has over 40 years' 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 is a Director of the American Software Testing Qualifications Board (ASTQB) and holds many ASTQB/ISTQB certifications, including all three core Advanced Certifications, the ISTQB Advanced Security Tester certification, ISTQB Advanced Test Automation Engineer, ASTQB Certified Mobile Tester, and ISTQB Certified Agile Tester, Foundation Level.

Randy is the chair of the ISTQB Advanced Security Tester Working Party which created the 2016 Advanced Security Tester Syllabus.

Randy is co-author with William E. Perry of the books, Surviving the Top Ten Challenges of Software Testing and Testing Dirty Systems.

Randy founded Rice Consulting Services in 1990 and continues to train, mentor and consult with testers and test managers worldwide. Many of his clients include DoD agencies which deal with complex testing problems in critical applications. His clients often rave that his practitioner experience in the trenches adds great value to the concepts he teaches and the consulting he performs.

**Mr. Maurice A. Sanders** is the Cybersecurity Division head at Marine Corps Operational Test and Evaluation Activity, responsible for the planning, execution, analysis and reporting of cybersecurity assessments of acquisition systems. He oversees teams of cybersecurity analysts evaluating the performance of weapons and information systems during operational test and operational assessments for Marine Corps Acquisitions, and, in support of Joint Service and Combatant Commanders assessments.

He was previously a government contractor working in support of DoD CIO. As Senior Cyber Analyst for the Department of Defense Cybersecurity Enterprise-wide Solutions Steering Group (ESSG) he spearheaded efforts to identify, assess, integrate, synchronize, and acquire enterprise solutions that addressed validated requirements and tools gaps necessary for DoD-wide Defensive Cyber Operations.

Retired Marine Corps Lieutenant Colonel. Vast experience in Test and Evaluation and Project and Program Management. Mr. Sanders was the lead Marine Corps operational tester for the MRAP program as well as Combat Service Support Test Division lead in charge of JLTV and LVSR testing.

**Mr. Nickolas B. Savage** is currently in his 20th year with the Federal Bureau of Investigation (FBI) and his 25th year in law enforcement. Mr. Savage was awarded a Master of Science in Information Technology and a Master of Public Management from Carnegie Mellon University and a Master of Science in Criminal Justice from Boston University. Mr. Savage is currently the Assistant Special Agent in Charge in the Baltimore Field Office and has management responsibilities for Counterterrorism, Cyber, Intelligence, and Crisis Response. Mr. Savage has had management responsibility for the Cyber Branch for the FBI Washington Field Office (WFO) which included all criminal and national security cyber investigations and until December 2017, was the laboratory director of three digital forensic laboratories within WFO.

In 2009, prior to his reassignment to the WFO, Mr. Savage came to Cyber Headquarters and was assigned to the National Center for Missing and Exploited Children (NCMEC) as the FBI's cyber liaison. In 2010, Mr. Savage was subsequently assigned to manage the Strategic Initiative and Operations Section (SIOS) and had management responsibilities for the Innocent Images program, Cyber Education, the Public Private Alliance Unit (InfraGard), and the Internet Crime Complaint Center. In 2011, Mr. Savage managed the Cyber Criminal Section and had nationwide responsibilities for all FBI cyber-criminal investigations. In 2012, Mr. Savage had management responsibilities for national security investigations involving Asia, Middle East/Africa, and Europe.

**Mr. Andrew Shaffer** has worked in the software development industry for over 20 years.

He holds a master's degree in Computer Science from Penn State University and currently works at the Penn State Applied Research Laboratory as a Research and Development Engineer.

His current research interests include cybersecurity, high performance computing, cloud computing, and novel computing architectures.

**Mr. Randall (Randy) Smith** is the technical lead for The Boeing Company's Product Cybersecurity Test and Evaluation team. As an Associate Technical Fellow with over 30 years' experience in cybersecurity research and development, Mr. Smith has led numerous research projects (both internally and externally funded), including high-assurance multilevel security and coordinated intrusion tracking and automated response technologies. Mr. Smith's Cybersecurity Test and Evaluation team's responsibilities cut across all of Boeing's product areas, including both commercial aviation and defense sectors, enabling Boeing to develop products and services that can operate effectively in a "cyber-contested" environment.

**Robert N. Tamburello, PhD**, currently serves as the Deputy Director of the National Cyber Range Complex (NCRC) within the DoD Test Resource Management Center (TRMC). In this role, Dr. Tamburello works with an interdisciplinary team to design and conduct events that address the full spectrum of DoD requirements in the cyber test and training domains. In addition, as the Program Manager for the NCRC Expansion, Dr. Tamburello is leading the effort, in partnership with the Services, to increase the DoD's capacity to support cyber test and training requirements through the establishment of new NCRC facilities.

Before joining TRMC, Dr. Tamburello served as the Division Chief for Mounted Systems within the Integrated Suitability and Methodology Evaluation Directorate (ISMED) of the U.S. Army Evaluation Center (AEC) at Aberdeen Proving Ground, MD. In this capacity, he led a diverse group of civilian and military personnel, including Australian Army exchange officers, to perform the operational suitability evaluation of a portfolio of more than 250 ground-based systems including Abrams, AMPV, Bradley, JLTV, MRAP, and Stryker. Immediately prior to serving in this position, he was the Division Chief of the Army Center for Reliability Growth at AEC. Previously, he has served in such positions as the Army Test and Evaluation Command (ATEC) lead for the Army Expeditionary Warrior Experiment (AEWE), the Tactical Vehicles Team Leader in the Reliability and Maintainability Directorate of AEC, and the Wide Area Surveillance Team Leader at the U.S. Army Materiel Systems Analysis Activity (AMSAA).

Over his career, he has led data-driven studies, developed methodologies, presented research findings, published journal articles, and crafted policy. He has also advised numerous program management offices and supervised the development of test plans and evaluations that directly supported milestone decisions associated with the production and fielding of Major Defense Acquisition Programs across all commodity areas. Serving as an instructor for the Army Center for Reliability Growth's Short Course, Dr. Tamburello promoted best practices for system reliability design, test, and evaluation, while concurrently developing new tools and techniques through his research contributions.

Dr. Tamburello began his career at AMSAA, serving as an operations research analyst on the Intelligence and Fusion Team in the C4ISR Branch. His primary work while on the Intelligence and Fusion Team consisted of the in-house development of C4ISR-centric performance models and simulations, including associated validation, verification, and accreditation activities. As well, Dr. Tamburello regularly performed statistically-based analyses of field and test data.

Dr. Tamburello earned his PhD in reliability engineering from the University of Maryland at College Park. As well, he earned a MS degree in applied mathematics from Johns Hopkins University and a BS degree in mathematics from Loyola University Maryland. Dr. Tamburello holds Defense Acquisition Level 3 Certifications in Test and Evaluation as well as Systems Planning, Research, Development and Engineering.

**David Tate, PhD,** joined the research staff of IDA's Cost Analysis and Research Division in 2000. In his 18+ years with CARD, he has worked on a wide variety of topics, including research into: Test and evaluation challenges of AI and autonomy; Risks in the defense software industrial base; Cost/benefit trades in ground combat systems; Technical barriers to mobile ad hoc networking; The affordability of acquisition portfolios; Causes of development schedule growth; Cost and schedule risk in major Department of Energy projects.

He was the leader of the Congressionally-mandated independent development cost review of the Army's Future Combat Systems program in 2007. He has also played a major role in CARD's educational outreach efforts, developing or contributing to cost analysis curricula (including online courses) for DoD, the Department of Energy, the Department of Commerce, the Department of Homeland Security, the Office of the Director of National Intelligence, and George Mason University. Prior to coming to IDA, Dr. Tate was Senior Operations Research Analyst for Telecommunications at Decision-Science Applications, Inc. Before that, he was an Assistant Professor of Industrial Engineering at the University of Pittsburgh. Dr. Tate holds bachelor's degrees in Philosophy and Mathematical Sciences from the Johns Hopkins University, and M.S. and Ph.D. degrees in Operations Research from Cornell University.

**Mr. Dominic Timoteo** received a M.S. in Computational Mathematics from Drexel University in 1984. He has been an employee with the Federal Aviation Administration in Atlantic City since 1974 as a computer programmer, researcher, project engineer and manager in support of various National Airspace System and NextGen Terminal and En Route automation system development projects.

Most recently he has supported FAA enterprise programs for Time Based Air Traffic Management, System Wide Information Management and Information System Security. Mr. Timoteo lives in suburban Philadelphia and enjoys sailing, reading and spending time with friends and family at the Jersey shore.

**Himanshu Upadhyay, PhD,** is serving Florida International University's Applied Research Center as Senior Research Scientist / Program Manager for the past 17 years, overseeing the Cybersecurity / Artificial Intelligence / IT research group. He is also an adjunct professor in the College of Electrical and Computer Engineering teaching Cybersecurity and Applied Artificial Intelligence courses. He brings more than 28 years of experience in cybersecurity, artificial Intelligence, information technology, big data, management and engineering to his role, serving as co-principal investigator for multimillion - dollar cybersecurity and artificial intelligence projects for the Department of Defense, Defense Intelligence Agency and knowledge/waste management, artificial intelligence and big data research projects for the Department of Energy's Office of Environmental Management. He has published multiple papers in the area of cybersecurity, machine learning, big data, knowledge management, nuclear waste management and service-oriented architecture. His current research focuses on cyber forensics, malware analysis, cyber analytics/visualization, artificial intelligence and big data.

**Mr. Isidore Venetos** joined the FAA in 2010 and he currently manages the FAA's Research and Development for Aviation Cyber Security at the William J. Hughes Technical Center. Prior to this, Mr. Venetos worked for the Department of Defense. Previously, he served as the senior engineer for the Electronic Warfare Air and Ground Survivability Division in the Intelligence and Information Directorate, Communications Electronics Research Development and Engineering Center, under the U.S. Army Research Development and Engineering Command.

He was also the Chief of the Information Operations/Signal Intelligence Technology Branch for the Intelligence and Information Directorate. In this position, he was responsible for developing new Information Operations / and Signals intelligence (SIGINT) technologies and effectively demonstrating the utility and viability of the new technologies toward the U.S. Army's mission. He also served as the technical manager for the Signal Warfare Program Office and was responsible for the concept exploration phase for the aerial common sensor, a category one acquisition program, which was designated to replace the Army's premiere airborne intelligence systems. In addition, he was the program manager for the Precision SIGINT Targeting System Advanced Concept Technology Demonstration. This was a joint program being managed by the Office of Naval Research with involvement from the National Security Agency, the National Reconnaissance Office, and the U.S. Army.

Mr. Venetos began his career with the U.S. Army in 1987, and joined the Communication Electronic Command in 1988 under the Intelligence Electronic Warfare Directorate.

Mr. Venetos holds a master's degree in technology management from the University of Pennsylvania (a joint program between the University of Pennsylvania's Engineering Department and the Wharton School), a master's degree in electrical engineering from Monmouth University, as well as a bachelor's degree in electrical engineering from the Illinois Institute of Technology. He also was a Ph.D. candidate at the New Jersey Institute of Technology and is the recipient of the Achievement Medal for his exemplary civilian service in support of the Signals Warfare Program Office and has continuously received commendations throughout his career.

He served as the U.S. National Lead on the Technical Collaborative Panel for Electronic Warfare Systems: Communications Electronic Warfare and as a co-chair on a joint airborne survivability program office's electronic warfare panel.

**Mr. James Wells** is the Deputy Director for Cyberspace and Homeland Security Enterprise programs in the Department of Homeland Security Office of Test and Evaluation. He led the development and coordination of the Department's first cybersecurity operational T&E policy that explicitly integrates cybersecurity into DHS major acquisition decision-making. Prior to joining DHS, Mr. Wells served as the Deputy Director for Cyber & Information Systems under the Deputy Assistant Secretary of Defense for Developmental Test & Evaluation where he managed a team responsible for overseeing the developmental T&E of major acquisition programs across all four DoD Services and many of the Defense Agencies. Mr. Wells became a T&E professional over the course of eight years and a variety of positions in the Army Test and Evaluation Command following ten years of active duty service in the US Army. He has a Bachelor of Science in Mechanical Engineering from the United States Military Academy and a Master of Science in National Resource Strategy from the Eisenhower School at the National Defense University. Mr. Wells holds various government certifications in Test & Evaluation, Systems Engineering, and Program Management. He is an active member of the International Test and Evaluation Association serving as the DHS Advisor to the Board of Directors since 2015.

**Mr. Billy Williams** has worked on and led multiple cyber and data analysis projects across the services in support of data distribution, knowledge management, and distributed test. He is currently working in the Test Resource Management Center program office in support of various projects related to distributed test, cyber security, enterprise software, big data/knowledge management and cyber test and evaluation.

**Duane Wilson, PhD** has been a practitioner in the field of cyber security for almost 20 years. After earning his bachelor's degree in Computer Science, Dr. Wilson went on to earn a Master of Engineering in Computer Science from Cornell University, a second Master of Science in Security Informatics, and a Ph.D. in computer science from Johns Hopkins University. The balance of both scholastic and operational experience allows him to have insight both into the theory and practice of cybersecurity. As a subject matter expert in cyber technology research, Duane's areas of expertise range from cyber security, business development, computer science engineering, and network protection. Duane provides subject matter expertise toward various Cyber Training & Education initiatives through his consulting firm Wilson Innovative Solutions LLC. The company's focus is to provide innovative cyber research and development, advanced cyber security consulting, and cyber security training for all levels of experience in the commercial and federal sectors.

**COL Jason A. Woodford** is the Director of the Survivability Evaluation Directorate for the Army Evaluation Center at Aberdeen Proving Ground, MD. He enlisted in the Utah Army National Guard as a Radio Teletype Operator in 1989. He entered the active Army in 1992 and received his commission as a Field Artillery Officer through the Reserve Officer Training Corps scholarship program at Southern Utah University. He has served at platoon through brigade level and at joint and Army level commands. He has commanded an artillery battery and a recruiting company. He is married to the former Hillary Arneson of Blythe, California and they have three children: Matthew, Erin, and Ashley.

COL Woodford's civilian and military education include Basic Combat Training, Airborne School, Bachelor's Degree in History, Southern Utah University, Field Artillery Officer Basic Course, NBC Officers Course, Field Artillery Officer Advanced Course, M109A6 Paladin Commanders Course, Recruiting Company Commanders Course, Combined Arms Staff Service School, Systems Automation Course, Command and General Staff College, Joint and Combined Warfighting School, Master's Degree in Information Technology Management, Webster University, CompTIA A+, Network+, and Security+ certifications.

**Mr. Gary Wright** is an Electrical Engineer who worked at NSA from 1992-2000, supporting cyber-related activities, including Open Source Intelligence (OSINT), red and blue teaming, table-top assessments, and cyber testing. He also ran a computer security consulting company from 2000-2008, was a director of operational network analysis at Sparta/Cobham/Parsons from 2008-2013, and is currently employed at JHU/APL supporting cyber security testing, solutions, and automation.

**Ms. Kate Yaxley** holds a Bachelor of Engineering (Electrical), obtained at the University of New South Wales in 2011. During her undergraduate studies, she became interested in signal processing, which coupled with her passion for mastery of the electronic spectrum, lead her to completing her Masters of Science in Electrical Engineering at the Air Force Institute of Technology in 2015. Upon completion of her Masters, Kate was employed as an electronic warfare practitioner, focused on the testing and evaluation, utilising test-lead methodology, of researched RF countermeasures. Kate commenced her PhD with the University of New South Wales in 2018 and in 2019 was posted as the Visiting Military Fellow (Air Force) to the School of Engineering and Information Technology. Kate's research includes protocol influence and behavior shaping of swarm and AI. Her particular interests include human-autonomy teaming, shepherding and introducing testing methodology to ensure the safe introduction of swarm and AI in any cyber environment.

# 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!*

**Robert Adamcik, CTEP**
Booz Allen Hamilton

**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

**Geoffrey Brando Reyes, CTEP**
Booz Allen Hamilton

**Erwin Sabile, CTEP**
Booz Allen Hamilton

**Christopher James Sacra, CTEP**
COMOPTEVFOR

**Thomas Sachse, CTEP**
PEO SUB

**Kristopher Scher, CTEP**
Science Applications International Corporation

**Shari Lynn Scott, CTEP**
Booz Allen Hamilton

**Mike Short, CTEP**
G2, Inc.

**Thomas Cash, CTEP**
CGI Federal

**CAPT Caroline Goulart Campos, CTEP**
Brazilian Army Commission (Brazil)

**Peter H. Christensen, CTEP**
The MITRE Corporation

**Francis Xavier Costello, Jr., CTEP**
AMERICAN SYSTEMS

**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

**Anthony Shumskas, CTEP**
TASC, Inc.

**Jody South, CTEP**
AMERICAN SYSTEMS

**Chad Stevens, CTEP**
KBRWyle

**Keith Sumner, CTEP**
Booz Allen Hamilton

**William J. Swank, CTEP**
DASD(DT&E)

**Michael Joseph Taylor, CTEP**
Defence Science and Technology Laboratory (Dstl) United Kingdom

**Miles Thompson, CTEP**
Georgia Tech Research Institute (GTRI)

**John Jozef Hamann, CTEP**
Booz Allen Hamilton

**John Heavener, 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**
Taverene Analytics LLC

**Lt Col. Martin "Marty" J. Mears, CTEP**
Alpha Omega Change Engineering (AOCE)

**Henry C. Merhoff, CTEP**
Louis P. Solomon Consulting Group

**Jason Morris, CTEP**
Booz Allen Hamilton

**Chelsea Prendergast, CTEP**
Joint Research and Development, Incorporated

**Joseph F. Puett III, CTEP**
ManTech International

**Robert Randolph, CTEP**
Department of Defense

**Steven Tran, CTEP**
Northrop Grumman Aerospace Systems

**Gregory Turner, CTEP**
The MITRE Corporation

**James Watson, Ph.D., CTEP**
OSD(CBD)

**Derick Wingler, CTEP**
Booz Allen Hamilton

**James P. Worden, CTEP**
Bevilacqua Research Corporation

**Stuart Wragg, CTEP**
USAF, Edwards AFB AFOTEC DET1

**David Zehr, CTEP**
419 FLTS/DOO


## Past EXHIBITORS:

10X Compliance Technologies
771st Test Squadron
Acquired Data Solutions, Inc.
ACROAMATICS Inc.
Advanced Systems Development, Inc.
Advanced Test Equipment Rentals
AEgis Technologies Group, Inc.
Agiltron
Air Academy Associates
American Software Testing Qualifications Board
Ampex Data Systems
Analytical Graphics, Inc.
Apogee Labs, Inc.
ARL
ARS
AssetSmart
Astro Haven Enterprises
ATAMIR WSMR
ATK
ATTI
Avionics Interface Technologies
Avionics Test & Analysis Corp
BEI Precision Systems & Space Company
Brand Design
CA Technologies
CALCULEX, Inc.
CDW-G
Celeris Systems Inc.
Charles Stark Draper Laboratory
Churchill Navigation
CI SYSTEMS INC.
Cobham Inc.
Command Post Technologies
Compunetix, Inc.
Curtiss-Wright Controls Avionics & Electronics
Defense Acquisition University
Defense Threat Reduction Agency
Dell EMC Corporation
Delta Information Systems
DET S&T
DEWESoft, LLC
DEWETRON, Inc.
Directed Energy Professional Society
Diversified Technical Systems
DRS Technologies
Dynetics, Inc.
Dytran Instruments, Inc.
Edge Consulting
Elotek Systems, Inc.
Emhiser Research
EMRTC New Mexico Tech
Encore
Engility Corporation
EWA Government Systems, Inc.
G.R.A.S. Sound & Vibration
Galleon Embedded Computing
GDP Space Systems
Geil Marketing Associates (GMA)
General Dynamics Mission Systems
Geodetics, Inc.
Georgia Tech Research Institute
Glacier Technologies
HEL-JTO
IAI North America
IAI-ELTA
IDA Technology
Imprimis, Inc.
Innovative Defense Technologies
Integrated Network Enhanced Telemetry Project
International Institute for Software Testing
International Telemetering Conference
International Test and Evaluation Association (ITEA)
ITT Exelis
Ixia
Jacobs Technology, Inc.
Joint Directed Energy Transition Office
Joint Range Solutions
JT4 LLC
Kaman Precision Products
KBRWyle
Keep it Simple
Kistler Instrument Corp.
Kratos Technology and Training Solutions
L-3 Telemetry & RF Products
Lockheed Martin
Malaysian Software Testing Board
ManTech
Manufacturing Techniques, Inc.
Marvin Test Solutions, Inc.
Meggitt Sensing Systems
MIRATEK Corporation
MZA Associates Corporation
Naval Air Systems Command
Naval Aviation Test & Evaluation University
NCSL International
NetAcquire Corporation
New Mexico Tech
NTSA
Nurjana Technologies
Old Dominion University
Olympus Industrial
OnTime Networks
PAE
Parasoft
PCB Piezotronics
Photo-Sonics, Inc.
Playas Training & Research Center
Precision Filters, Inc.
Quintron Systems Inc.
Raytheon
Rockwell Collins
Rotating Precision Mechanisms, Inc.
RoundTable Defense, LLC
RT Logic
Saalex Solutions, Inc.
SAS Institute/JMP
Science Applications International Corporation
Scientech Inc.
Scientific Research Corporation
SemQuest
SimIS Inc.
Smart Card Alliance
Smartronix Inc.
Space Information Laboratories, LLC
Spiral Technology, Inc.
STAR Dynamics, Inc.
SURVICE Engineering Company
SYMVIONICS Inc.
System Testing Excellence Program
Systems Application & Technologies
Systems Engineering & Management Company
TDK-Lambda Americas
Technical Systems Integrators, Inc.
Tektronix, Inc
Teletronics Technology Corp
Telspan Data
TENA JMETC
TEST LLC
Test Resource Management Center
Textron Systems Corporation
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
U.S. Army
Ultra Electronics Herley Lancaster
Ulyssix Technologies, Inc.
Uniforce Sales and Engineering
Universal Switching Corporation
Ward/Davis Associates
Weibel Scientific A/S
Wideband Systems, Inc.
Zodiac Data Systems

## Past SPONSORS:

Acquired Data Solutions, Inc.
Advanced Systems Development, Inc.
Advanced Test Equipment Rentals
AECOM
Aermor LLC
Air Academy Associates
AMERICAN SYSTEMS
Applied Research Laboratory/PSU
Astro Haven Enterprises
Avion Solutions, Inc.
BAE Systems
Belcan Corporation
Bitmicro Networks Inc.
Booz Allen Hamilton
CALCULEX, Inc.
Capability Analysis & Measurement Org. LLC
Charles Stark Draper Laboratory
Clear Creek Applied Technologies, Inc.
COLSA Corporation
Command Post Technologies
Dell EMC Corporation
EMRTC New Mexico Tech
Engility Corporation
Engineering Research and Consulting, Inc.
EWA Government Systems, Inc.
GBL Systems
General Dynamics Mission Systems
Georgia Tech Research Institute
IAI-ELTA
InDyne, Inc.
INQU, LLC
irig106.org
Jacobs Technology, Inc.
Joint Range Solutions
JPI
JT4 LLC
KBRWyle
Kord Technologies
Kratos Technology and Training Solutions
Loch Harbour Group, Inc.
Lockheed Martin
ManTech
MIRATEK Corporation
NetAcquire Corporation
New Mexico Tech
NTS
PAE
PCB Piezotronics
Raytheon
Rockwell Collins
RoundTable Defense, LLC
Scientific Research Corporation
SimIS Inc.
SURVICE Engineering Company
Systems Application & Technologies
The Boeing Company
TRAX International, LLC
TRIDEUM Corporation
Ward/Davis Associates
Zodiac Data Systems

**Symposium Chair**: Peter Nikoloff, NOVA Systems Australia
**Technical Program Chair:** Peter Green, KBRWyle
**International Panel Chair**: Gloria Deane, DOT&E
**Exhibits and Sponsorships Chair:** James Gaidry, CAE
**Awards Committee Chair**: Stephanie Clewer, SA-TECH

**Host Chapter Presidents**
Mid-Pacific Chapter: Shannon Wigent, Laulima Systems, LLC
Southern Cross Chapter: Peter G. Nikoloff, NOVA Systems

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

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

***THANK YOU TO OUR SPONSORS!***

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.