Pre-Symposium Tutorials

NOTE: Pre-Symposium Tutorials require a separate fee from the Symposium.
Single Tutorial - $205, Two Tutorials - $385

Tuesday, September 27th 8:00 a.m. – 12:00 p.m

DoD Test and Evaluation Across the Acquisition Lifecycle (Rapid & Mid-Tier Acquisition)

Dr. Michael Flynn CTEP, CSEP, Defense Acquisition University

An overview of the Adaptive Acquisition Frameworks guidance for Defense Acquisition System from a Test and Evaluation perspective with emphasis on the involvement in the Systems Acquisition Lifecycle and T&E's relationship to the Systems Engineering processes used throughout the lifecycle of major acquisition programs from requirements generation, through Post Milestone C. Coverage will include the latest policies and practices and the role of T&E with an overview of Agile Software practices, DevSecOps, Capabilities Based Test and Evaluation and the relationship between Developmental and Operational T&E. Focus will be on the major events that occur during each phase of acquisition, required documentation, and expected entrance and exit criteria for successfully achieving approval. The intended audiences are engineers, program managers, and industry for an understanding of DoD acquisition in relationship to T&E's involvement.

Predicting and Assessing Prototype Capability

Mark Kiemele, PhD, Air Academy Associates

Design of Experiments (DOE) is a method that can and should be used not only in the design and development of systems, but also in the modeling and validation of prototype systems. Building useful prediction models and then validating them can ease the burden of making procurement decisions. This tutorial will examine two prototypes that are built to satisfy a common set of requirements. DOE, together with regression analysis, will be used to model the performance of each prototype. Then validation testing will be used to confirm the models and assess the performance capability of each prototype, i.e., how well the prototypes meet the requirements. This facilitates a comparison of the capabilities of the two systems, thereby enhancing the decision as to which system to pursue. There are no pre-requisites for this tutorial, as the analysis will be demonstrated via computer.

T&E as a Part of Agile Development

Robin Poston, PhD - System Testing Excellence Program, University of Memphis, and Wayne Dumais - Deputy T&E, Department of Homeland Security (DHS)

To discuss T&E in support of agile development, we need to explore the sequence of the evolution of the agile methods, rationale for the application of different methods, compare traditional and agile software development approaches, discuss research conclusions regarding the agile method's impact on software performance, review benefits and challenges of agile, and appreciate the fit of agile methods with Systems Acquisition Life Cycle. Furthermore, in this tutorial we will also discuss when to use agile, the role of the tester on agile projects, and various kinds of testing applicable to agile software developments.

Tuesday, September 27th 1:00 p.m. – 5:00 p.m.

Incorporating T&E into Acquisition Contracts "Shift All the Way to the Left"

Terry Murphy, Deputy Director, Office of Test & Evaluation, Department of Homeland Security (DHS)

So you're a Test and Evaluation Manager (or Key Leader) of a program and you and your T&E working group have just finalized the programs T&E Master Plan. Looks like you've accomplished all the pertinent tasks for T&E and ready for execution. Right? Not so fast, have you ever heard the term if it's not written into the contract it probably won't happen? To many of our T&E professionals are steeped in technical expertise and key on development of sound well defined T&E plans, but all too often they lack program management broness to understand they've missed critical steps. That being said, has the T&E manager coordinated with their programs contracting officer, contract specialist and or contracting officer's representative? Probably not.

This tutorial will provide the T&E professional an overview and process for inclusion of T&E equites into the acquisition contracting artifacts. The goal of this tutorial is not to make T&E professionals contract experts, but rather provide them a keen understanding of their "Key" role, responsibilities, processes, and as key players within this process ensure T&E equities are included within acquisition contracts.

The main focus will leverage the initial procurement notice released to industry per Federal Acquisition Regulation (FAR) Part 15, the Request for Proposal (RFP). Topics will include:

- Request for Proposal background and content
- Detailed overview of each RFP Part and Section with discussion on inclusion of

T&E equites based on lessons with examples
- Discussion on the Statement of Work (SOW) and or Statement of Objectives (SOO) - Differences, purposes, and how the T&E professionals assist in the development

It is critical that our T&E professionals have a full understanding of their "Key" role within the program contract development process. Without the T&E professional working side-by-side the contracting Team there are NO guarantees that T&E equities will be clearly articulated and communicated within the contracting documents. The T&E professional is the key to ensuring that T&E is accurately, effectively, and with clarity included within the program contract actions, thereby reducing:

- Confusion
- Miss-interruptions
- Unclear requirements

There is a gap for our T&E professionals within this area of knowledge, and it's for that reason, this tutorial is recommended.

Security, Orchestration, Automation and Response (SOAR) - Big Data Analytic, Cyber Playbooks, Human Interface

Vivian Richards, Splunk

Alert Fatigue, juggling too many security tools, limited talent pool. These are three critical problems that can burden even the most committed security operations team. What if there was a way to automate detection, investigation, and response? Using a Security Orchestration, Automation and Response tool like Splunk SOAR can help you respond to security threats faster and decrease your average time to detect, investigate, and remediate malware.

By automating repetitive security tasks, like alert triage, Splunk SOAR can help you work smarter and focus on mission-critical tasks. Splunk SOAR technology integrates with your existing security tools to make them work better together and can help you get the most out of your current security investments and strengthen your overall security posture.

Automating a majority of that security workload with automated playbooks means your team doesn't have to do it manually. This frees up time for your team to focus on other mission critical tasks. In short, your team can do more with the people you already have.

In this session, we will discuss how automation can help a security team establish better standard operating procedures to help the team be more effective using built-in case management to apply more operational rigor around security processes.

Think Like an Adversary

Elly Millar, Defense Acquisition University, Cybersecurity Professor

Cyber threat landscape is constantly evolving. Organizations continue to expand their digital edge, heavily relying on mobile and Internet-of-Things (IoT) devices. COVID-19 also accelerated digital transformation and cloud adoption as millions of employees were forced to work from home. People working remotely has opened up new avenues for cyber threat actors to target both individuals and organizations all the while making it more challenging for local Information Technology (IT) staff to have visibility and control over the organization's assets. Increase in collaboration across industries and academia also contribute to the attack surface growth due to the unknown nested third party relationships. Cybersecurity issues are a day-to-day challenge for healthcare, financial, manufacturing, government and other sectors. Every communication path represents a risk and traditional method to secure the IT infrastructures do not work effectively on new modern attack surfaces. Additionally, decreasing costs of computation and data storage make it extremely easy for the cyber threat actors to adapt quickly and become more innovative in their attacks. Cybersecurity challenges are daunting, but instead of throwing in the towel, start to think like an adversary to implement proactive and effective cybersecurity measures. This tutorial will lead the audience with limited background in cybersecurity to understand the concept of cyber threat intelligence starting with the cybersecurity trends, cyber threat terminologies and concepts including attack surface characterization. Additionally, the tutorial will introduce the audience to the Department of Defense Cyber Table Top (CTT) methodology including a CTT Lite exercise to better understand the adversarial perspectives. Knowledge gained from the tutorial will help build a foundation for those with limited to no cybersecurity experiences, but also beneficial to any cybersecurity professionals looking to apply threat engineering and/or threat based cyber testing with an ultimate goal of achieving organizational (or program's) operational resiliency.

TRMC Solutions for Overcoming Challenges in Distributed T&E

Gene Hudgins, JMETC/TENA, KBR

The Test and Training Enabling Architecture (TENA) was developed as a DoD CTEIP project to enable interoperability among ranges, facilities, and simulations in a timely and cost-efficient manner, as well as to foster reuse of range assets and future software systems. TENA provides for real-time software system interoperability, as well as interfaces to existing range assets, C4ISR systems, and simulations. TENA, selected for use in JMETC events, is well-designed for its role in prototyping demonstrations and distributed testing.

Established in 2006 under the TRMC, JMETC provides readily-available connectivity to the Services' distributed test capabilities and simulations. JMETC also provides

connectivity for testing resources in the Defense industry and incorporation of distributed testing and leveraging of JMETC-provided capabilities by programs and users has repeatedly proven to reduce risk, cost, and schedule. JMETC is a distributed LVC testing capability developed to support the acquisition community during program development, developmental testing, operational testing, and interoperability certification, and to demonstrate Net-Ready Key Performance Parameters (KPP) requirements in a customer-specific Joint Mission Environment.

JMETC is the T&E enterprise network solution for secret testing, and uses a hybrid network architecture – the JMETC Secret Network (JSN), based on the SDREN. The JMETC MILS Network (JMN) is the T&E enterprise network solution for all classifications and cyber testing. JMETC provides readily available connectivity to the Services' distributed test capabilities and simulations, as well as industry test resources. JMETC is also aligned with JNTC integration solutions to foster test, training, and experimental collaboration.

TRMC Enterprise Big Data Analytics (BDA) and Knowledge Management (BDKM) has the capacity to improve acquisition efficiency, keep up with the rapid pace of acquisition technological advancement, ensure that effective weapon systems are delivered to warfighters at the speed of relevance, and enable T&E analysts across the acquisition lifecycle to make better and faster decisions using data that was previously inaccessible, or unusable. BDA is the application of advanced tools and techniques to help quickly process, visualize, understand, and report on data. JMETC has demonstrated that applying enterprise-distributed BDA tools and techniques to T&E leads to faster and more informed decision-making that reduces overall program cost and risk.

This tutorial will inform the audience as to the current impact of TENA, JMETC, and BDA on the T&E community; as well as their expected future benefits to the range community and the warfighter.