ENCLOSURE 1

ADDITIONAL CONTEXT TO THE PROBLEM

For the current problem set, T&E includes all forms of DoD cyber and multi-domain testing including research and development testing and formal activities including Mission Based Cyber Risk Assessments (MBCRAs) (e.g. Cyber Table Tops, Mission-Based Risk Assessment Process for Cyber), automated security verification testing, cooperative and adversarial test and evaluation (post event analysis), and service or joint experimentation, training and exercises. TRMC desires instrumentation, tools, and methodologies that can gather and use the information obtained from all of these events, operational reporting on incidents, open source and intelligence threat reporting, and field data. This data is vital to improve mission assurance assessment of the DoD as a whole as well as informing the cyber survivability and resilience of our platforms to perform their assigned missions in contested cyberspace. An approach and framework to enable federated understanding across the DoD Services, domains, and industries needs to be designed, created, and secured. Use of modern information processing technologies such as ontologies, taxonomies, ML/AI, and Natural Language Processing are desired to facilitate machine augmented analytics. These tools should enable decision makers to make decisions grounded in facts and data, improve future testing events, and reduce the cost of cyber testing. It is intended that the tools and methodologies developed in this research will be integrated into a single integrated Government off the Shelf (GOTS) open framework solution that will be maintained by the government or government contractors, verified as resilient itself, and accessible to test organizations and other DoD acquisition stakeholders.

Metrics and analytics are sought to quantitatively measure the efficacy and effectiveness of test events using inputs to define the System Under Test (SUT) (e.g. Model based systems engineering designs) and information about the projected cyber threats. These analytics shall be capable of being run on data during test planning, test execution, and when SUT configurations, defensive operations capabilities, vulnerabilities, threats, or operator TTPs (Tactics Techniques and Procedures) are updated. These tools should input Model Based System Engineering (MBSE) artifacts such as a SUT Bill of Materials (BOM) that includes the hardware and associated firmware BOM and Software Bill of Materials (SBOM) in open standard machine readable formats (e.g. CycloneDX, SPDX). These tools should use as inputs the information available from Open-Source products such as MITRE's ATT&CK, D3FEND, CVE, and CWE, as well as other commercial and government (e.g., NIST, intelligence sources) information on potential vulnerabilities and threat TTPs. Metrics and analytic tools solutions providers can assume information about the test will be available in the Me&S data structures and should explore what types of information and formats should be available for adequate metrics. The proposed tools and methodologies should identify test instrumentation and data collection requirements. In addition, visualizations are needed to show the results of these analytics for different stakeholders.

CONCEPT OF OPERATIONS

The Concept of Operations (CONOPS) of the final Measure and Share (Me&S) system is shown in the figure below. The modules colored in yellow are addressed in this problem space. The process of using Me&S begins with the blue box, at the left of the figure, where the user defines the SUT using available

tools and imports or defines relationships, BOMs, and SBOMs. The SUT and subcomponents, along with the Security Classification Guide for the SUT and other MBSE artifacts will be imported into the Me&S data store and a Universally Unique Identifier (UUID) will be assigned for each element in the BOM and SBOM. The SUT definition should include the components, transport and interface controls, relationships of cyber/physical and cyber/cyber components, and component relationships. This step is indicated in the figure by the number 1 double arrow. The SUT may be anything from a small device such as a software defined radio or a large collection of systems of systems such as those use by a Joint Task Force in some theater of operations. Outputs from MBCRA tools identified in Appendix A should be utilized for the SUT definition and analysis.

Once the SUT is defined, the external reporting information denoted in the gray boxes, previously imported from open sources, operational information in the form of potential mission snippets, and intelligence information, is referenced and used by algorithms to map potential vulnerabilities and TTPs to the SUT. This step is indicated in the figure by the number 2 double arrow.

The SUT definition and external reporting information is analyzed and made available to the test planners for consideration in test design to include suggested priority tests. Once a test plan is created and entered with associated artifacts, analytics can be run to measure the efficacy prior to test execution and inform the test designer. When the test plan is executed, additional test artifacts and results are imported into the data storage system. This step is indicated in the figure by the number 3 double arrow.

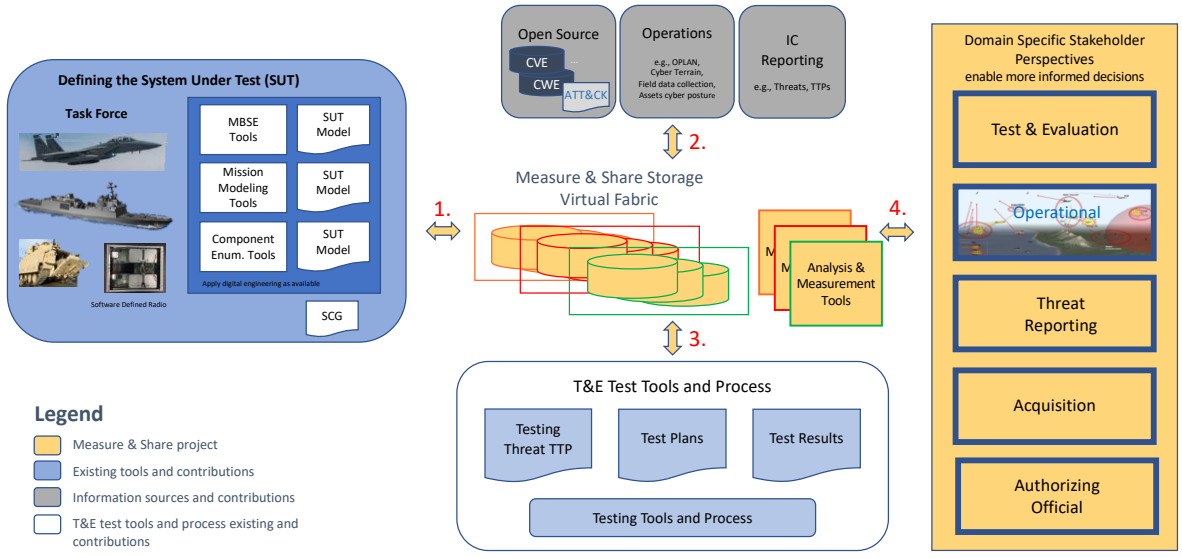

Figure 1 Measure & Share Concept of Operations

Independently, various stakeholders can create and use domain specific Me&S perspectives to view test results at time of test, post-test event (results of one or more tests), and in context of new information. For example:

- Tactical commanders can use perspectives to understand mission readiness for specific OPLANS in the context of the cyber risks, current threats, test results, and mitigations. Analytic results will display confidence in the information. Operators can use these perspectives to provide feedback.
- DoD leadership can use perspectives to gain a holistic understanding of the largest operational cyber risks to the warfighter and identify future test and event requirements. Leadership can use these perspectives to provide feedback.
- T&E leadership can use perspectives to gain insight on the efficacy of a particular test event, or the effectiveness of the use of test resources.
- T&E personnel can use perspectives to plan and execute T&E events more efficiently.
- Acquisition program and T&E leadership can use perspectives to reevaluate the efficacy of tests previously conducted when new threat intelligence information is available and determine the potential need for new testing.
- Acquisition program leadership can use perspectives to view the efficacy of a test on one of their systems, get information on anticipated test costs for new systems, analytics on the Return On Investment (ROI) on a particular test or a series of tests, and gain insights into components and subcomponents architectures and a design pattern's ability to meet DoD cyber requirements.
- Intel practitioners can use perspectives to gain insights into threats and trends discovered across the DoD SUTs and components to enhance Intel reporting, derive new key intelligence questions, and inform acquisition and defensive cyber operations.
- Intel practitioners can use perspectives to gain insights into the use of intel provided for a particular SUT, component, or test and get feedback on threat reporting gaps.
- Authorizing officials can use perspectives designed for them to gain more comprehensive insights into test coverage and DoD cyber-related requirements including Risk Management Framework (RMF) and Cyber Survivability Endorsement requirements, and Service unique needs (e.g., NAVY CYBERSAFE).