Autonomous and Robotic Systems Cyber and Electromagnetic Activities (CEMA) Test and Evaluation Planning Guide

Mr. Robert F. McKelvey III
U.S. Army Evaluation Center – Survivability Directorate
Emerging Leaders Cohort – Individual Project

29 INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

98 INTENTIONALLY LEFT BLANK

1. CYBER AND ELECTROMAGNETIC ACTIVITIES (CEMA) TEST AND EVALUATION (T&E) PROCESS INTRODUCTION

1.1 Purpose

The purpose of this planning guide is to document an evaluation framework for CEMA and develop example inputs for a U.S. Army Evaluation Center (AEC) System Evaluation Plan (SEP). The evaluation framework will align phases of the acquisition lifecycle for cybersecurity and electronic warfare (EW) T&E on autonomous platforms and will synchronize processes such as developmental systems engineering and the Risk Management Framework (RMF) with the overall T&E effort. Collaborating activity across the spectrum of stakeholders, developers, and system evaluators will help identify and verify requirements and baseline capabilities, expose reachable and exploitable vulnerabilities, and provide a more advanced evaluation for a system in an operational environment. Vulnerabilities, identified early in the acquisition lifecycle, will provide feedback to responsible stakeholders with applicable data to improve system capabilities and will ultimately lead to a robust and securer system.

1.2 Background

Cybersecurity, formally known as Information Assurance (IA) per the National Security Presidential Directive-54/Homeland Security Presidential Directive-23, expands current procedures and methodologies in an attempt to synchronize the compendium of guidance and requirements documentation currently available. Cyber threats have increasingly accelerated to become a prominent threat for tactical and enterprise systems. Any data exchange, however brief, provides an opportunity for a determined and skilled cyber threat to monitor, interrupt, or damage information and combat systems. Department of Defense (DoD) acquisition processes must deliver systems that provide secure, resilient capabilities in the expected operational environment. To provide systems capable of achieving cybersecurity protection, operational testing must develop and examine system T&E in the presence of a realistic cyber threat early in the acquisition lifecycle.

EW is defined as military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. EW consists of three divisions: electronic attack (EA), electronic protection (EP), and EW support (see Figure 1). Adversaries are constantly developing and adapting new Electromagnetic Activity (EMA) threat capabilities, exploiting these technologies, and using them to disseminate attacks against wireless networks, radios, electronics equipment, and computer networks. The DoD must deliver systems with EMA capabilities and adequate survivability to counter the hostile use of cyberspace, space, and the electromagnetic spectrum.

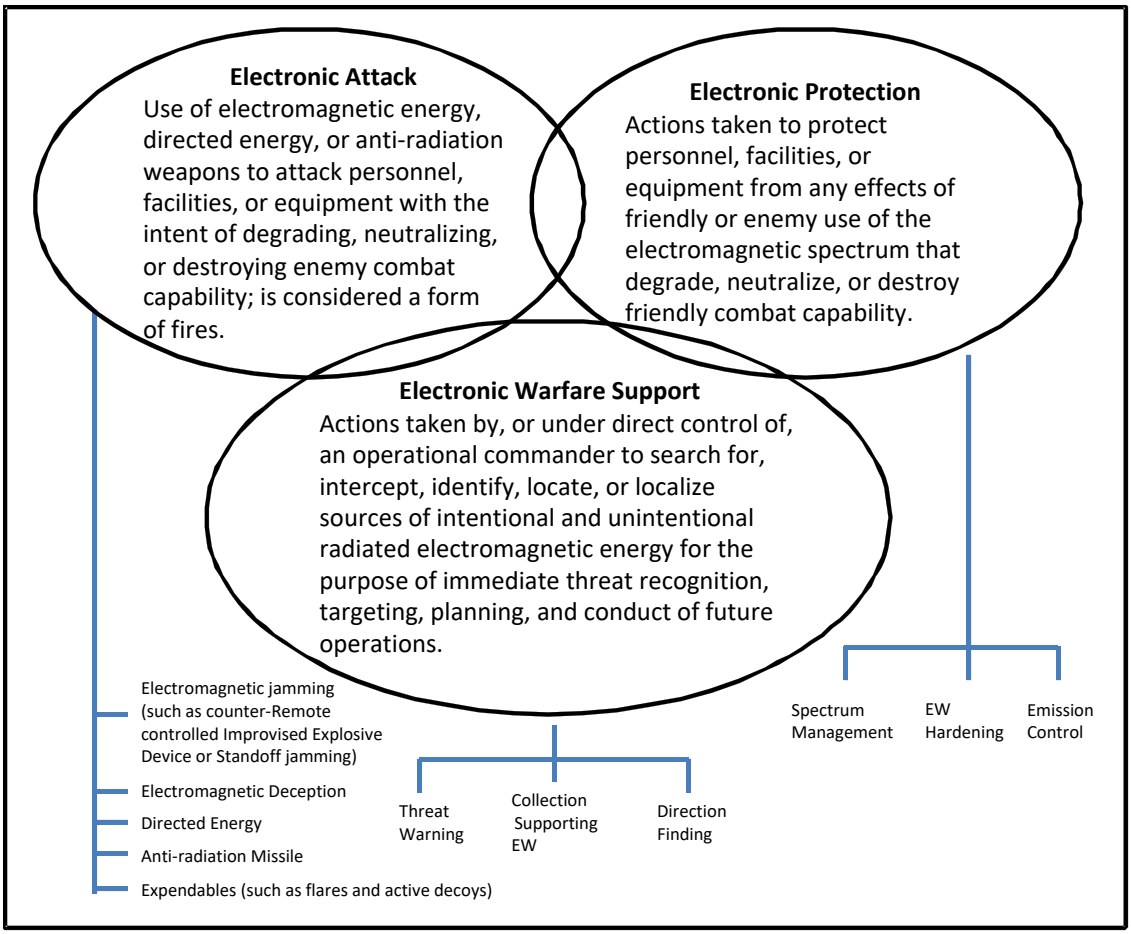

Figure 1. The Three Subdivisions of EW.

1.3 Evaluation Strategy Overview

The vulnerability evaluation (cybersecurity survivability evaluation) comprises multiple steps. The first steps are understanding the system and defining the scope of what is to be evaluated. Based on the AEC evaluator's understanding of the system, a vulnerability assessment needs to be performed to assign likelihood and consequences to potential threats. Risk levels and mission impacts will in turn be derived from the likelihood and consequence assessment. The AEC evaluator will develop the evaluation strategy and document the strategy in the SEP, Test and Evaluation Master Plan (TEMP), and Data Source Matrix (DSM). The risk assessment will also feed the design of the system testing and test plans.

The cybersecurity system testing will be defined in the TEMP, DSM and Operational Test Agency Test Plan (OTA TP) and will comprise developmental and operational test phases. Developmental test based assessments, Cooperative Vulnerability Assessments, will focus on identifying areas of vulnerability that could potentially compromise a system. Operational test based assessments, Adversarial Vulnerability Assessments, will take place sometime after the Cooperative Vulnerability Assessment.

The Cooperative Vulnerability Assessments will inform what specific vulnerable areas should be targeted during the Adversarial Vulnerability Assessment. Due to the complexity of systems that would be targeted by CEMA-related threats, the approach to the vulnerability evaluation should be iterative. The program office or system developer should be provided sufficient time between Cooperative Vulnerability Assessments or between developmental and operational test phases to address anomalies found during test.

The Adversarial Vulnerability Assessments will comprise approved test teams acting as attackers within the relevant operational environment.

Certain levels of functionality are delivered at each Milestone Decision, and a CEMA vulnerability assessment should be conducted for each milestone with available data to assess system maturity.

1.4 CEMA Policy, Acquisition Requirements, and Reference Documentation

The scope of CEMA assessments are captured in many policy references and procedural documents. Table 1 lists some pertinent documents for a CEMA evaluation. Each of them promotes information and guidance sharing throughout the system's lifecycle and a thorough review will equip an evaluator with the ability to fully understand the evaluation test measures and evaluator responsibilities throughout the program's development.

The Army provides EW doctrine, policy, and guidance reference documentation for EW planning, preparation, execution, and assessment in support of joint operations across the range of military operations. Each of the EW focused documents contains information and guidance for the overall evaluation framework and a thorough review will equip an evaluator with the ability to fully understand EW capabilities, operations, challenges, measures, and responsibilities.

It is important for an evaluation authority to be involved early in the system acquisition and development. Hardening of the system/platform against CEMA vulnerabilities is often easier and cheaper to incorporate early in the development process.

Table 1. Policy and Guidance Documents

Document	Important Information
Department of Defense Instruction (DoDI) 5000.02, Operation of Defense Acquisition System, 7 January 2015	• Policy for the management of all acquisition programs. • Authorizes Milestone Decision Authorities (MDAs) to tailor the regulatory requirements and acquisition procedures in this instruction to more efficiently achieve program objectives consistent with statutory requirements.
DoDI 5000.02 (DT&E)	• DT&E planning will resource and ensure threat-appropriate testing to emulate the threat of hostile penetration of program information systems in an operational environment. • Cybersecurity testing will include, as much as possible, activities to test and evaluate a system in a mission environment with representative cyber-threat capability.

	• Cybersecurity will ensure that each major developmental test phase or event in the planned test program has a well-defined description of the event, specific objectives, scope, appropriate use of M&S, and an evaluation methodology. • The evaluation methodology will be described in the TEMP at MS A and will provide essential information on programmatic and technical risks, as well as information for major programmatic decisions. • At MS B, the evaluation will include the framework to identify key data that will contribute to assessing progress toward achieving cybersecurity requirements. In addition, the evaluation framework will show the correlation/mapping between test events, resources, and decision supported. • The evaluation methodology will support an MS B assessment and an MS C assessment of cybersecurity. • All programs must have security controls implemented consistent with their system classification. Evaluation of the system to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction will be investigated.
DoDI 5000.02 (OT&E)	• Beginning at MS A, the TEMP will document a strategy and resources for cybersecurity T&E. At a minimum, software (SW) in all systems will be assessed for vulnerabilities. Higher criticality systems will also require penetration testing from an emulated threat in an operationally realistic environment during OT&E. • Appropriate measures will be included in the TEMP beginning at MS B and used to evaluate operational capability to protect, detect, react, and restore to sustain continuity of operations (COOP). The TEMP will document the threats to be used, which should be selected based on the best current information available from the intelligence community. • SW acquisition will be conducted and analyzed for operational risk to mission accomplishment covering all planned capabilities or features in the system. The analysis will include commercial and non-developmental items. • Testing of SW for any system should be supported through emulated hardware or virtual machines of digital device(s) on which the SW runs.
Director, Operational Test and Evaluation (DOT&E) Memo, Procedures for OT and Evaluation of Cybersecurity in Acquisition Programs, 1 August 2014	• DOT&E memo supersedes previously published guidance that described a “six-step” process and specifies a two-phase approach for operational cybersecurity testing in support of operational T&E for DoD acquisition programs. • Procedures apply to all oversight information systems, weapons systems, and systems with connections to information systems, including MDAP, MAIS, and special access programs. THE REQUIREMENT FOR OPERATIONAL CYBERSECURITY TESTING IS INDEPENDENT OF ANY REQUIREMENTS FOR CERTIFICATION AND ACCREDITATION. • A system is considered to encompass hardware, software, user operators, maintainers, and the tactics, techniques, and procedures used to carry out the concept of operations (CONOPS). • An operational environment includes other systems that exchange information with the system under test (system-of-systems to include the network environment), end users, administrators and cyber defenders, as well as representative cyber threats.
DOT&E Memo (Cooperative Vulnerability Penetration Assessment)	• This operational test shall be conducted by a vulnerability assessment and penetration testing team through document reviews, physical inspection, personnel interviews, and the use of automated scanning, password tests, and applicable exploitation tools.

	• The assessment should be conducted in the intended operational environment with representative operators including system and network administrators. This testing may be integrated with DT&E activities if conducted in a realistic operational environment, and approved in advance by DOT&E.
DOT&E Memo (Adversarial Assessment)	• This test phase should be conducted by an operational test agency employing a National Security Agency (NSA) certified adversarial team to act as a cyber aggressor presenting multiple cyber intrusion vectors consistent with the validated threat. • The assessment should be designed to characterize the systems vulnerability as a function of an adversary's cyber experience level, relevant threat vectors, and other pertinent factors. • Adversarial team should attempt to induce mission effects by fully exploiting vulnerabilities to support evaluation of operational mission risks. • Assessment should include representative operators and users, local and nonlocal cyber network defenders (including upper tier computer network defense providers), an operational network configuration, and a representative mission with expected network traffic.
DOT&E Memo, Test and Evaluation of Information Assurance in Acquisition Programs, 1 February 2013	• Independent Penetration Testing: Sharing system information and interconnections between the Cooperative cyber vulnerability assessment teams (blue) and the independent cyber penetration/exploitation teams (red) is acceptable. Shared information should not include specific vulnerabilities or system shortfalls. • Network Defense Analysis: Testing should quantitatively examine not only the inherent system network protections but also the network defense ability to detect penetration or exploitation, react, and restore. • Operational Effects Analysis: Testing should include an assessment of operational risk presented by vulnerabilities and shortfalls exploited by a representative threat, and the most direct way to assess that risk is to demonstrate and record relevant operational effects. When operational threat representative effects cannot be conducted on live-networks, alternate evaluation approaches should be employed and included in the test planning.
DoDI 8500.01, Cybersecurity, 14 March 2014	• Provides policy for DoD information and IT. The operational resilience will be planned, developed, tested, implemented, evaluated, and operated to ensure security posture of a system is sensed, correlated and made visible to mission owners, network operators, and DoD information enterprise. • Whenever possible, technology components will have the ability to reconfigure, optimize, self-defend, and recover with little or no human intervention. Attempts produce an incident audit trail.
DoDI 8510.01, Risk Management Framework, 12 March 2014	• Formally the Defense Information Assurance Certification and Accreditation Process (DIACAP), now replaced by the Risk Management Framework (RMF). • Manages the lifecycle cybersecurity risk to DoD IT, and directs visibility and procedural guidance for authorization documentation, acceptance, and decisions for the authorization and connection of IS's. • Informs acquisition processes for all DoD IT, including requirements development, procurement, and both DT&E and OT&E, but does not replace these processes. • Information protection requirements are satisfied by the selection and implementation of appropriate security controls. Security controls are

	implemented by common control providers, system managers, and risk based authorization decisions granted by the approving authority. • Test results will provide an initial assessment along with recommendations to eliminate discovered vulnerabilities or reduce their risk.
National Institute of Standards and Technology (NIST)	• http://www.nist.gov/
National Security Agency (NSA), National Information Assurance Partnership (NIAP)	• https://www.niap-ccevs.org/ • https://www.niap-ccevs.org/pp/
FM 3-36, Electronic Warfare In Operations, February 2009	• Provides Army doctrine for EW planning, preparation, execution, and assessment in support of full spectrum operations.
Joint Publication 3-13.1, Electronic Warfare, 25 January 2007	• Provides joint doctrine for electronic warfare planning, preparation, execution, and assessment in support of joint operations across the range of military operations.
DoD Directive (DoDD) 3222.04, Electronic Warfare (EW) Policy, 26 March 2014.	• Provides EW policy, definitions, and responsibilities within the DoD for providing operational forces with EW capabilities to control the electromagnetic operational environment across the range of military operations.
Army Regulation 70-75, Para. 1-6 j.	• Provides regulation for electronic equipment, ensuring electronic equipment will be survivable to electromagnetic environment criteria and survivable in an electronic attack environment (including directed energy weapons [DEWs]).
Electronic Warfare and Radar Systems Engineering Handbook	• Provides technical concepts, formulas, equations, constants, conversions, characters, mathematical notation, and equations used for analyzing Radar systems, electronic attack (jamming) scenarios, and electro-optical systems.

1.5 National Security Agency (NSA) and CSS Architecture

Formal architecture documents the scope of what is being depicted and the standard terms and definitions used in the architecture. Architecture products should be selected based on who is using the products. For most programs, this will be the Milestone Decision Authority (MDA). NSA requires specific architecture views for system use cases. An evaluator should become familiar with all the architecture views to help understand and design system T&E. Refer to NSA/CSS Architecture Guidance, dated 5 February 2015, for further details on architecture requirements and uses for NSA acquisition systems.

1.6 Defense Evaluation Framework (DEF)

This document aims to provide a methodology for CEMA T&E planning within the acquisition lifecycle. "Shift Left," a term coined in the DEF, establishes evaluation early in the acquisition lifecycle to synchronize the scope of CEMA for evaluation. Understanding system development early in the development phases will provide a more thorough evaluation for operational testing later in the lifecycle by attaining necessary information for informed decisions. Shift Left

includes aligning systems engineering processes with the acquisition lifecycle and documenting these processes within the T&E strategy that will feed into the TEMP at each MS. Starting the T&E process earlier provides the Operational Test Agency (OTA) with an objective to track, collect, and identify areas of interest for a developing system. For purposes specific to cybersecurity, Figure 2 provides the DEF Shift Left approach and shifts items such as the RMF, Developmental Test (DT) and Operational Test (OT), and interoperability testing early into the acquisition lifecycle.

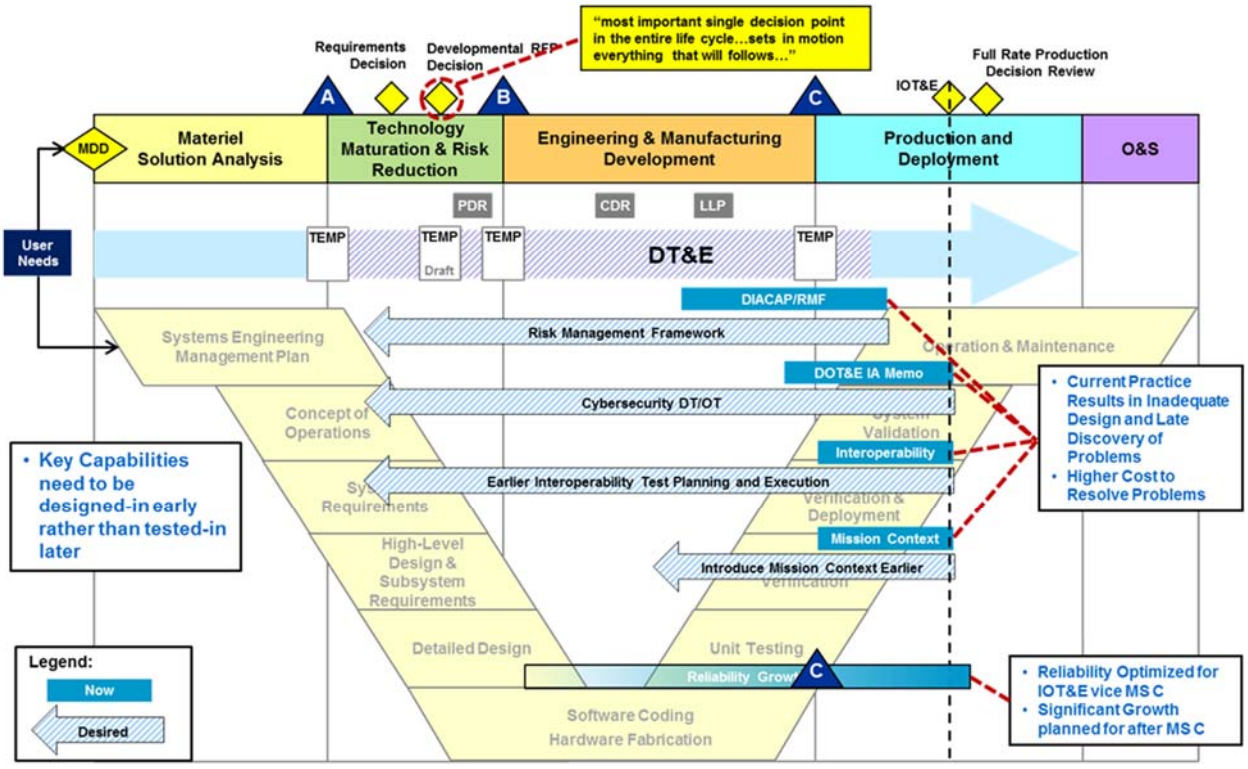

Figure 2. Cybersecurity Shift Left.

The following sections provide the CEMA process for the AEC T&E strategy development. Section 2 focuses on cybersecurity, and section 3 focuses on EMA. Each section addresses the process from the beginning of the program through test design.

2. CEMA T&E PLANNING

The T&E planning will follow the steps outlined in Figure 3. Each subsection outlined provides a means to develop and implement the T&E strategy for the system and builds upon each subsequent section. This process is used to inform documentation development from the ESR/CIPR, TEMP and SEP input, OTA TP, and analysis and evaluation reports.

The T&E planning for the EA and EP portions of EMA are discussed in this section and will also follow the steps outlined in Figure 3. Each subsection outlined provides a means to develop and implement the EMA T&E strategy for the system and builds upon each subsequent section. This process follows a model-test system improvement approach in which theoretical analysis, simulations, and predictions are compared with actual test results from DT and OT. The evaluator performs a technical assessment and documents all EMA findings, vulnerabilities, system impacts, Soldier impacts, and mission impacts and then makes the appropriate recommendations to improve the system. EMA theoretical analysis, simulations, and actual testing are used to determine (1) a system's operational response to the EA environment, (2) the enemy's ability to intercept, detect, identify, and locate radiated electromagnetic sources from the system, and (3) a system's ability to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of EW that degrade, neutralize, or destroy friendly combat capability. This process can be applied to various types of systems, such as Air Defense Radar, Optical Augmentation, Missile EO Countermeasures, and Communications.

Figure 3. The Cybersecurity Evaluation Process.

2.1 Understanding the System

The first step in the evaluation strategy planning process is to understand the functionality of the system and how the system operates. Understanding the stakeholder, system development, and requirements documentation will provide a more thorough understanding of the system's design, mission, and system-of-system integration. Collecting system information frequently, and early in the lifecycle, allows the evaluator to track any major design changes (between Preliminary Design Review [PDR] and Critical Design Review [CDR]), collect and review preliminary testing (manufacturer, demonstrations, lab), and begin to provide inputs for the T&E planning that will feed into T&E documentation. Additionally, early information and data collection may

expose initial vulnerabilities and allow for remedial updates as appropriate. This early assessment could make it easier for program offices to remedy anomalies earlier, cheaper, and more effectively.

An evaluator will need to identify information products—generation, use, storage, transmission, and destruction—and gather and review available documentation for the system. An evaluator also needs to identify the aspects of the system that are impacted by EW operations. This could include EA functions, employed Electronic Protection, and aspects of the system that potentially require EP. This requires an evaluator to be involved pre-MS A, ideally, and throughout the acquisition lifecycle to ensure an understanding of products used, their intended functions, and how they will be integrated within a system-of-systems environment.

Gathering DoD Architectural Framework (DoDAF) views (e.g., system and operational views), requirements documentation, and any manufacturer specifications will provide a foundation for the development of the evaluation strategy. These documents will outline mission dependencies, hardware (HW) and SW components, and any critical data exchanges and interfaces for the system.

This system understanding will be used to determine information products critical to, and how EW impacts, mission accomplishment. Table 2 provides relevant information for an evaluator to collect and understand during the development of the system.

Table 2. CEMA Relevant Documents and Resources

Key Documents	Description	Sources
FM 3-38 CEMA	• Overarching doctrinal guidance and direction for conducting CEMA	• http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_38.pdf
DOT&E Memo (August 2014)	• Guidelines for DT&E, OT&E, and TEMP input	• References
FM 3-36 Electronic Warfare In Operations	• Provides guidance on how the electromagnetic spectrum can impact operations and how friendly EW operations can be used to gain an advantage	• References
DoD Directive (DoDD) 3222.04	• Addresses Electronic Warfare (EW) policy definitions and responsibilities within DoD for providing operational forces with EW capabilities to control the electromagnetic operational environment across the range of military operations	• References
Army Regulation 70-75, Para. 1-6 j.	• Electronic equipment will be survivable to electromagnetic environment criteria and survivable in an electronic attack environment (including DEWs)	• References
EW and Radar Systems Engineering Handbook	• Provides technical concepts, formulas, equations, constants,	• References

	conversions, characters, mathematical notation, equations, and formulas for analyzing radar systems, electronic attack (jamming), and electro-optical systems	
DoDI 5000.02	• Acquisition Guidelines	• References
COTS, GOTS, and Free Open Source Software Certifications	• Driven by acquisition approach and technology choices • Tasks that a developer must accomplish to operate securely, such as NSA policy	• Program Management Office (PMO) • Manufacturer
Security Classification Guide	• Classification of program-related information	• PMO
Statement of Work, Initial Capabilities Document (ICD), CDD, and CPD	• Addresses capability gap, operational needs, and mission scenarios • Use of commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) products • RMF packages • Acquisition strategy and schedule • Contract specification documentation	• User (e.g., SOCOM) • PMO (Program Manager (PM), Chief Engineer, System Architect, Contractor Leads) • Manufacture
Concept of Operations (CONOPS)	• Examine system CONOPs to understand roles and responsibilities of system operators, administrators, and the computer network defense service provider (CNDSP)	• PMO
Technical Requirements	• Enables the capabilities defined in CONOPS and other operational documentation	• Army • NSA
DoDAF Views	• System View (SV-1/2/6) • Operational View (OV-1)	• PMO • System Architect • Lead Engineer (USG-KR)
Preliminary Design Review (PDR) and/or Critical Design Review (CDR)	• Insight into system development • Technical and operational requirements • Initial vulnerabilities and remediation	• PMO • Manufacturer
Interface Control Document (ICD)	• Communicates all possible inputs to and all potential outputs from a system for a user • Inputs and outputs of the system • Interface between two systems or subsystems	• PMO • Manufacturer
Systems Engineering Plan	• Submitted at each MS, beginning with MS A. • Describes overall technical approach, key technical risks, processes, resources, organizations, metrics, and design considerations	• PMO

	• Addresses integration with existing and approved architectures and capabilities. • Addresses SW risks; identification; tracking; and reporting of metrics for SW performance, process, progress, and quality; safety and security considerations; and SW development resources	
Program Protection Plan (PPP)	• SW vulnerability analyses tools will be used throughout the lifecycle and ensure remediation of SW vulnerabilities addressed in PPPs and test plans	• PMO
Validated Online Lifecycle Threat (VOLT)	• Determines the generation of the relevant operational threat environment	• Acquisition and intelligence communities
MS Schedule	• Planned T&E events	• PMO
Detailed Test Plans	• Provides information on how system is tested with results used in evaluation. Must have input into plans to ensure proper data is available for evaluation.	• ATEC or Test Facility

2.2 Bounding the Evaluation

2.2.1 Define the System Boundary

A system boundary defines the limits of the system for evaluation purposes and defines the transfer of information and signals. Using system and operational architectural views, development specifications, and requirements documents, a boundary can be defined. The evaluator should take into account the protection and trust across the network layers, such as application, session, transport, network, data links, and physical protection.

It may be beneficial to begin understanding how the information flows from the generation of data (sensors or user input) and how the information is processed (SW and HW) and collected, assessed, and disseminated (operators and users). COTS, GOTS, and previously fielded systems may be part of system under evaluation, or external interfaces in which the lines of transmission might need to be included. A system can be a hand-held device, tactical radio, or an enterprise network composed of multiple systems. Figure 4 provides an example boundary diagram for a generic system. Examples of system boundary diagrams for a tactical and enterprise system can be found in Appendix A and B.

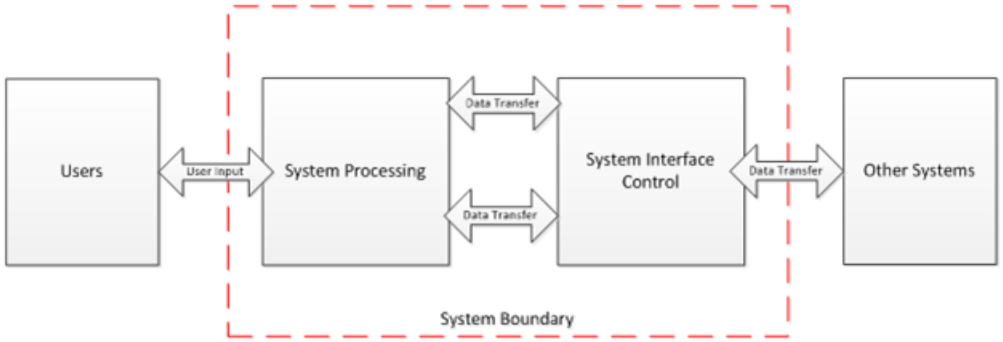

Figure 4. Cybersecurity System Boundary Example.

It may also be beneficial to understand what contingency protocols are in place for interruptions to data flow (e.g., a global positioning system [GPS]). An example of a system can be a hand-held device, tactical radio, air defense radar, optical, infrared (IR) guided missile with electro-optic countermeasures, radio frequency (RF) guided missile, or an unmanned air vehicle (UAV). Figure 5 provides an example boundary diagram for a generic system.

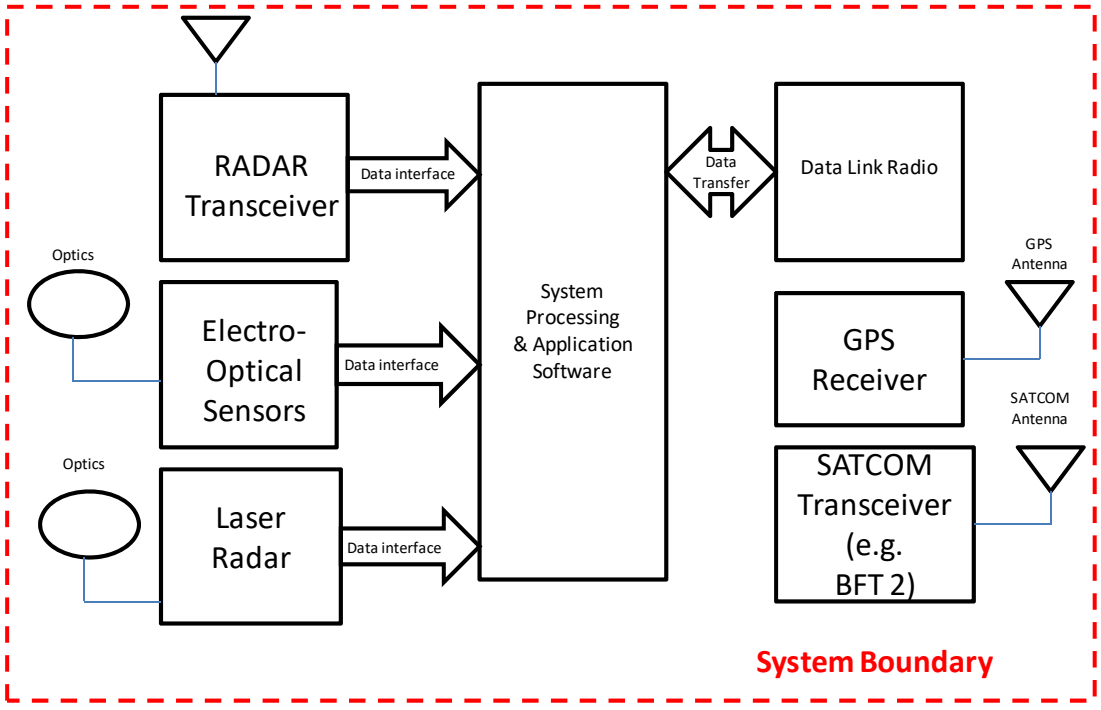

Figure 5. EW System Boundary Example.

After the boundary for a system has been defined, the evaluator can address the components that constitute the system, determining where the signals are generated and transmitted, including details on how the data are received, used, and transmitted. Details on how the data are received, stored, used, transmitted, and destroyed should be included. The evaluator should also investigate all physical means (e.g., cables, removable media and wireless) for data transmission and dissemination.

2.2.2 Defining System Components and Information

A complete system characterization may result in crossing subsystem boundaries. The boundary can include data transmission to interfaces from point to point, the transmission of data, or the receipt of data. The evaluator should also investigate interfacing systems, document each enclave or interface (and any intrusion detection SW or HW) and diagram all subsystems to capture all transmission.

The system can have HW and SW components, each with varying functionality and features. Review of the ICD and architectural views will provide the various SW and HW products used and their interface within the system and systems-of-systems. The evaluator should take into account how the key management, public key certificates, any biometrics, and cryptographic modernization functions are used within the system. Figure 6 shows a detailed boundary diagram, including different examples of how data transmission is considered part of the system.

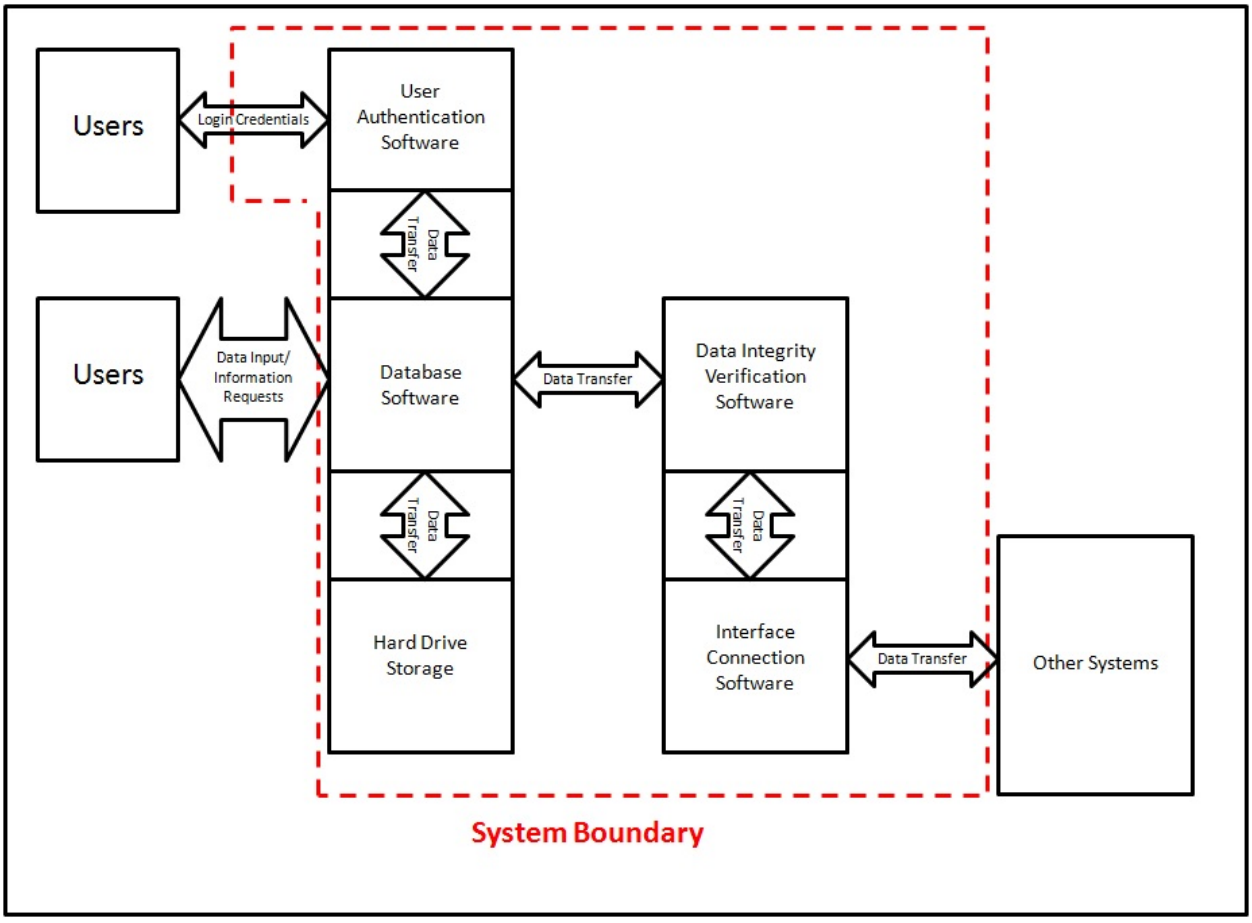

Figure 6. Detailed Cybersecurity System Components.

Now that the boundary and components of the system have been defined, the evaluator can address how and where the information flows. The evaluator should review data buses early in system development and when updates are available, as these provide a detailed description of

how the information is processed. Any ports and protocols intended for IS that traverse between DoD enclaves and DoD external enclaves should also be identified. All information gathered will aid the vulnerability assessments for the system.

2.2.3 Defining Electronic Signals Flow, Component Criticality, Function, and Potential Entry Paths for EA Energy.

The evaluator should also research any system functionality that can potentially serve in an EA capacity and should investigate the contingency protocols for data interception and interruption. This investigation may result in crossing subsystem boundaries. The evaluator should diagram all subsystems to capture all transmissions. The system can have HW and SW components, each with varying functionality and features. Review of the ICD and architectural views will provide the various SW and HW products used, and their interface within the system and systems-of-systems.

It is also necessary to understand the user's interaction with the system. Is the user there to monitor operation only or is the user there to detect issues and determine and implement fixes. Also critical to the understanding of the operational capabilities of a system are the definitions of the potential entry paths for the EW environments. These can be "front door" which include optical windows, antennas, or holes in a system skin. They can also be "back door" which include energy that couples on to a skin and is re-radiated to internal cables or components or finds an indirect path to internal electronics. Not all components are critical to the operation of a system and therefore, if they are susceptible to EA environments, may not cause operational issues within the system. Unfortunately, even a non-critical component that is in a front door path of a laser or HPM environment may provide incorrect information to a critical system causing operational anomalies. Therefore, understanding the normal operational capabilities and potential errors are necessary.

2.3 Designing Cybersecurity Tests and Experiments

The Cybersecurity OTA TP should outline the required data collection for specific test events and contains detailed information on data gathering event design, methodology, scenarios, instrumentation, simulation and stimulation, and all other requirements guiding the conduct of testing.

Table 3 outlines the representative data and metrics for cybersecurity assessments.

Table 3. Core System Protection Data and Metrics

Title	Measurement	Notes
Vulnerabilities	• Cyber vulnerabilities with descriptions and DISA severity codes.	Descriptions shall include the nature of the vulnerability, affected subsystem(s), and implications for system protect, detect, react, and restore capabilities. Include description of tools.

Intrusion/Privilege/ Escalation/Exploitation Techniques	Intrusion/privilege escalation/ exploitation techniques: • Specific technique employed • Starting point • Success/failure result • Time to execute, level of difficulty (low/medium/high) Starting point is the point internal or external to the system under test from which a scan or penetration attempt is initiated.	If technique is successful, state affected system(s). Level of grades: • LOW: technique can be executed by an actor without formal training or material support (e.g., a "script kiddie"). • MEDIUM: technique can only be executed by an actor with some formal training and material support but does not require a high-level actor. • HIGH: technique can only be executed by an actor with state-of-the-art training and ample material support (e.g., a nation state).
Password Strength	Number of passwords attempted to crack. Number of passwords cracked. For each cracked password: • Privilege level • Level of difficulty required • Reason for password weakness (e.g., default password, low complexity)	Can consider the use of tokens where appropriate. Include description of tools used.
Protect	Adversarial activities: • Description • Level of difficulty (low/medium/high) • Time to execute Success/failure.	Include starting position, nature of the technique(s) used, target system, and cyber objective (e.g., exfiltration).
Detect	Time for defenders to detect each intrusion/escalation of privilege/exploitation	For each detected event, include the means of detection (e.g., IDS alert).
React	Defense activities: • Description • Time elapsed • Success/failure Time for defenders to mitigate each detected intrusion/escalation of privilege/exploitation. White cards used: • Description Time issued	Include origin of response (e.g., user, system administrator, cyber defender) and nature of response (e.g., containment, quarantine, reporting).
Restore/Continuity of Operations	Time taken to restore mission capabilities after each degradation.	Includes assessment of ability of typical user operators to execute procedures.

	White cards used: • Description Time issued	Should describe restoration activities undertaken (e.g., restore from backup, failover to alternate site).
Mission Effects	Reduction in quantitative measures of mission effectiveness. Where direct measurement is not feasible, independent assessment of mission effects (minor, major, severe) using SMEs.	Should include performance parameters already being used to assess system effectiveness. Adverse effects could include specific mission-critical tasks or functions impaired and any resulting shortfalls in the confidentiality, integrity, and availability of critical mission data.
Account Management	• Separation of Duties • Non-Repudiation • Insider Threat Protection	Accounts are established only after screening users for membership, need-to-know, and functional tasks, and are disestablished promptly when they are no longer required.
Least Privilege	• User responsibilities • User rights	Accesses are granted to users following the principle of least privilege.
Identification and Authentication	• Password procedures • Key management • Encryption	Organizational users are uniquely identified and authenticated when accessing the system, including when using group accounts.
Content of Audit Records	Independent assessment of content using SMEs	Audit records contain sufficient information to establish the nature, time, location, source, and outcome of malicious events, as well as the identity of any individuals associated with such events.
Audit Review, Analysis, and Reporting	• Audit schedule • Notification methods • PPP	Audit records are reviewed and analyzed promptly for indications of inappropriate activity, and any findings are reported to cyber defenders.
Continuous Monitoring	• Intrusion detection and prevention methodology • Analytics • Information sharing	The system is continuously monitored for vulnerabilities, including regular assessments by cybersecurity test teams.
Configuration Settings	• Security focused configuration management • Information security • Organizational risk minimized while desired functionality is supported	The system is installed in accordance with an established baseline configuration following the principle of least functionality, and any deviations from this baseline are recorded.
Back, Recover, and Restoration	• Backup methodology • COOP	System data are routinely backed up and preserved, and a recovery and restoration plan for the system is provided.

Device Identification and Authentication	• Accesses explicitly identified • Authentication employment (e.g., passwords, tokens, biometrics, multifactor, or some combination thereof) • Local or remote access and methodology	The information system uniquely identifies and authenticates devices before establishing a connection.
Authenticator Management	• Identities are verified • Initial authenticator content established with sufficient strength • Maximum lifetime established • Reuse conditions • Authenticators changed when membership changes • Authentication location (e.g., endpoint vs. centralized)	The cryptographic strength, maximum lifetime, and storage methods for system authenticators (e.g., password, tokens) are compliant with organizational policy.
Default Authenticators	• Default authenticator content changed	System authenticators (e.g., password, tokens) are changed from their default settings.
Physical Access Control	• System storage methodology • Combat locks • Emplacement • Integration • Packaging • Guards (e.g., electronic, manned)	The information system, including data ports, is physically protected from unauthorized access appropriate to the level of classification.
Boundary Protection	• Whitelisting/Blacklisting • External communications monitored and controlled • Subnet usage • Interface management with boundary protection devices	The system monitors and controls data exchanges at the external boundary and at key internal boundaries, including firewalls or guard, IPS/IDS/HBSS.
Secure Network Communications	• Communication protocols • Transmission protocols • Encryption • Keys and hashes • Authentication protocols	Network communications are secure, and remote sessions require a secure from of authentication.
Update Managements	• Patch management • Update schedule • Hardware update management • System support • Malicious code protection updates	Security-related software and firmware updates (e.g., patches) are centrally managed and applied to all instances of the system in accordance with the relevant direction and timeliness.
Malicious Code Protection	• Protection mechanisms and entry and exit point • Scan schedules • Ability to block, quarantine, or remove malicious code or users • Ability to address false positives and potential impacts on system availability	Mechanisms for preventing the deployment of malicious code (e.g., viruses, malware) are installed, configured, and kept up-to-date.

391

2.4 Designing Theoretical Analysis, Simulations, and Laboratory and Field Tests

2.4.1 Theoretical Analysis and Simulations

The evaluator should design plans for theoretical analysis and simulations to gather predictions against operationally realistic EW. They should review data from prior testing, any design modifications, and use of surrogates to determine the system's expected performance in an EA jamming environment (e.g., determine signal levels from a jammer and the communications transmitter at the input of the receiver being jammed). Typically these effects can be predicted using the one-way radar equation, or the radio frequency propagation equation (see EW Radar Handbook), but the performance of the jammer depends on the relative received signal levels from the jammer and the communications transmitter.

The one-way radar equation can also be used to calculate free-space path loss as a function of range at a given frequency. Several other useful formulas and technical information related to EW analysis can be found in the EW Radar Handbook. It is highly recommended that the EW evaluator use this reference when performing theoretical analysis.

The power received from the transmitter and the power received from the jammer can be calculated based on parameters, such as transmitter power, signal wavelength, antenna gains, and propagation path-loss and can then compute the jamming-to-signal ratio (JSR). For jamming to be effective, two conditions must be met: the power received from the jammer must be greater than the sensitivity of the receiver, and the JSR must be sufficiently large. Particular effects also will depend on the jammers modulation. A rule of thumb for FM voice communications and data systems not using electronic protection techniques is: A JSR of 1 will lead to significant degradation of communications performance, and a JSR of greater than 2 will lead to an almost total loss of performance.

The GPS Interference and Navigation Tool (GIANT) is a many-vs.-many constructive and repeatable GOTS simulation tool that computes GPS and other navigation system performance and mission impacts in a benign or electronic combat environment. GIANT can be useful during operational assessments of company, or larger, elements or sensitive systems heavily dependent on positioning architecture.

2.4.2 Laboratory and Field Tests

The OTA TP and SEP should outline the required data collection and contains detailed information on data gathering event design, methodology, scenarios, instrumentation, simulation and stimulation, and all other requirements to support the system evaluation requirements. Historically, EW is not usually tested in an OT environment due to test participant safety but the EW environment may be simulated to assess operational capacity through validated and accredited models.

EW laboratory testing may use a Design of Experiments (DOE) approach. DOE is a method of data and information collection that uses statistics to evaluate the factors, conditions, and levels that control or affect the outcome of specific performance response variables. One or more

factors, conditions, and levels can be changed either one at a time or simultaneously during testing. These factors, conditions, and levels are the independent variables in the experiment, and the response variables are the dependent variables. The following questions may provide answers in a well-designed experiment.

- What are the key factors in a process?
- What is considered acceptable performance?
- What are the interaction effects in the process?
- What is the response to spoofing or jamming?
- What environment would bring less variation in the system response?

Table 4 contains a list of examples that represent EW response variables.

Table 4. EW Data Elements

Name	Description
Jammer-to-Signal (J/S) Ratio	Ration of the jammer power received at the input of the receiver to the communication transmitter power received at the input of the receiver
Message Completion Rate	Number of messages received/number of messages sent
Speed of Service (i.e., latency)	Message received time – message sent time
Packet delivery ratio	Number of packets received by a node/number of packets sent
Packet delay time	Time packets received – time packets sent
User transmission rate	
Radio throughput	Number of messages or bits per second that can be transmitted or received
Voice Quality	0–5 Likert scale scoring

The evaluator should conduct laboratory tests using DOE. The evaluator should witness and observe all EW laboratory testing as necessary and make detailed notes of what was done for future reference.

2.5 Documenting Evaluation Strategy

2.5.1 Evaluation Strategy Review (ESR) and Concept in Process Review (CIPR)

As part of the standard AEC ESR/CIPR process, the evaluator will need to present the system boundary for evaluation, initial list of CEMA threats, and the risk assessment for approval. The ESR will verify that all Key Performance Parameters (KPPs) and Critical Operational Issues (COIs) will be addressed. The CIPR will describe the proposed test events and the allocation of priority measures for the events. The CIPR will also outline the resource estimates for events and overall T&E costs. Any changes that come about through the CIPR process will be incorporated in the SEP and TEMP, as necessary.

The evaluation strategy will document all required testing resources and accompanying schedule, as well as metrics, measures, and data requirements for the TEMP, SEP, and OTA TPs. All

system testing should be tailored in an operational, mission context when applicable, possible, and affordable.

The operational test based cybersecurity assessment will consist of at least two assessments: the Cooperative Vulnerability and Penetration Assessment (CVPA) and the Adversarial Assessment (AA). The CVPA is to provide a comprehensive characterization of the cybersecurity status of a system in a fully operational context. If the system is sufficiently mature to engage in the AA, the evaluator should plan for both. The AA will use operationally realistic cyberspace based threats to engage the system and should use a NSA certified adversarial team employing a validated threat.

The evaluation of threat interactions should be system-specific and should be expressed in terms of operational effectiveness and survivability. Vulnerabilities could include shortfalls in the confidentiality, integrity, and availability of critical mission data.

The evaluation strategy that will feed the initial TEMP input, now required at MS A, will be derived from the ESR/CIPR and early draft SEP. The strategy along with resource requirements for testing, at each MS, will be included in the TEMP input. The SEP is a living document. Prior to each MS, the evaluator should review newly implemented system capabilities and threats to determine if new vulnerabilities have arisen and if established potential vulnerabilities have mitigated.

2.5.2 TEMP

The TEMP must define a CEMA T&E strategy that uses relevant data from all available sources, including information security assessments, inspections, components and subsystem-level tests, system-of-system tests, and testing in an operational environment with systems and networks operated by representative users and operators. The TEMP should also identify the anticipated CEMA threats for testing adequacy, lay out all expected testing, and is updated at each MS with greater detail.

The AEC TEMP input will follow the guidelines found in the ATEC Evaluator Handbook, DOT&E Memo dated 1 August 2014, and the DOTE TEMP Guidebook.

2.5.3 System Evaluation Plan (SEP)

The SEP will expand upon the ESR, CIPR, SEP, and TEMP input for the CEMA evaluation strategy and required data. The SEP will include any COI and COIC developed by the user and AIs developed by the evaluator for a complete evaluation of operation effectiveness, suitability, and survivability, as well as the methodology for addressing each issue. Each methodology will document how the evaluator will use the measures and data requirements associated with each issue to perform analysis in support of the evaluation. Table 5 provides an example of a cyber-focused COI, potential AIs, and measures for a system or system-of-systems.

Table 5. Cybersecurity COI, AIs, and Measures

COI: Is the system survivable when integrated and employed in a congested and contested operationally realistic environment? (NOTE: Each COI will have user-developed criteria for satisfaction of the COI)	
1.	**AI 1: How well do the system's cybersecurity capabilities protect the user's required data and information?**
a.	Adequacy of disk and file level encryption used for data-at-rest (DaR)
b.	Security of stored data
c.	Security of data transfer design
d.	Security of data processing
e.	Adequacy of encryption used for data-in-transit (DiT) and data-in-process (DiP)?
2.	**AI 2: How secure are access points for the system?**
a.	Effectiveness of virus protection
b.	Effectiveness of malware protection
c.	Effectiveness of firmware protection
d.	Timeliness of firmware updates pushed to the system
e.	Number and types of access points
3.	**AI 3: How will the system's cybersecurity detection measures support the ability of the user to identify specific attacks?**
a.	Adequacy of system produced audit trails and logs
b.	Effectiveness of system monitoring, analysis, and reporting
c.	Effectiveness of system responses to an intrusion or incident
d.	Adequacy of system notification to user or system administrator
e.	Effectiveness of IDS
f.	Effectiveness of firewalls
4.	**AI 4: How will the system facilitate the user and/or operator's ability to react to detected penetrations and exploitations?**
a.	Effectiveness of the system and/or user authentication schema
b.	Adequacy of account management for each authenticated user
c.	Adequacy of user and operator training
d.	Adequacy of schema to manage and update patches to the system
5.	**AI 5: How effective are continuity of operations and contingency plans?**
a.	Adequacy of system data backup
b.	Adequacy of system data backup protection
c.	Ability of the system to restore capabilities
d.	Time to reconstitute system operations or implement a work-around
6.	**AI 6: How effective is the disaster plan?**
a.	Assessment of the ability to render the system inoperable in case of imminent capture
7.	**AI 7: How effectively are the known vulnerabilities managed?**
a.	Ability of the system to manage known vulnerabilities
b.	Results of STIGS and SCANS
8.	**AI 8: How is the mission impacted by cyber vulnerability?**
a.	Impact to the mission by loss of data
b.	Impact to the mission by compromise of data and system authentication
c.	Impact to the mission by inability to access the system

e.	Ability of the user to perform mission tasks if the system cannot send information
f.	Ability of the user to perform mission tasks if the system does not receive requested information

Table 6 provides an example of an EW-focused COI and potential AIs and measures for a system or system-of-systems.

Table 6. EW AIs and Measures

1.	**AI 1: How well does the system survive in an operationally relevant EW environment?**
a.	Capability of the system to survive the effects of threat jammers (communications, GPS, multiple spot noise, wide-band noise, barrage noise, swept-carrier/spot noise, ground-based, airborne-based, frequency-follower and Digital Radio Frequency Memory (DRFM)-based jammers). (Laboratory and field test). Laboratory test potentially would have to be done closed loop, meaning RF and jamming signals would be injected into the receiver over coaxial cables.
b.	Message Completion Rate (MCR) in an electronic attack (EA) environment (radio-to-radio). (Laboratory and field test).
c.	Call Completion Rate (CCR) in an EA environment (radio-to-radio). (Laboratory and field test).
d.	MCR in an EA environment (networked radio). (Laboratory and field test).
e.	Call Completion Rate (CCR) in an EA environment (networked radio). (Laboratory and field test).
f.	Speed of service in benign and EA environment (network radio). (Laboratory and field test).
g.	Systems, subsystems, components, and functions degraded or damaged when exposed to EA by threat type. (Laboratory and field test).
h.	Mean time for each system, subsystem, component, and function to recover from the effects of EA by threat type. (Laboratory and field test).
i.	Subjective assessment of the ability of users to perform mission tasks in a jamming environment and their assessment of the level of degradation of the system while operating in such an environment.
j.	Capability of the system to counter spoofing threats, such as, GPS deception emitters, GPS spoofing, and communications deception emitters. (Laboratory and field test).
k.	Number of times that the system countered spoofing attacks by threat type. (Laboratory and field test).
l.	Mean time for the system to recover from a spoofing attack by threat type. (Laboratory and field test).
m.	Subjective assessment of the ability of users to perform mission tasks in a spoofing environment and their assessment of the level of degradation of the system while operating in such an environment.
n.	List and description of occurrences in which the system is intercepted, detected, identified, located and exploited by threat ES systems by threat type.
o.	Effectiveness of EP design.
p.	Probability of intercept vs. range in an ES sensor environment by threat type.
q.	Probability of correct identification vs. range in an ES sensor environment by threat type.
r.	Location accuracy vs. range in an ES sensor environment given detection, interception, and identification by threat type. Effects of return signal.
s.	Susceptibility to lasers, HPM, UWB, and EMP/HEMP.
t.	Use of chaff, flares, and decoys.

u.	Opposing force ES team's ability to detect the system's RF signals in an OT environment by threat type.
v.	Opposing force ES team's ability to intercept the system's RF signals in an OT environment by threat type.
w.	List and description of occurrences in which the system avoids interception, detection, identification, location, and exploitation as a result its EP capability by threat type.
y.	System RF, thermal, and optical signature measurements.

524
525

3. CEMA Evaluation

The evaluator needs to consider the 'who/how/why' uses of data and assess the impact of loss, compromise, or inability to access to information or systems when assessing mission impact. They should determine potential vulnerability of the system by first reviewing threat and system documentation and will need to look at both inherent sub-system vulnerabilities and external threats.

Threat documentation typically includes the VOLT and Army G2 analyses, but Subject-matter-experts (SMEs) should also be consulted to determine potential system vulnerabilities.

3.1 Cybersecurity Survivability

External threats will focus on actors, personnel categories who could attack the system, and tactics or attack postures that are used in CNO. This initial assessment will provide data on threats to address Likelihood and Consequence, which will determine the risk and drive required testing. Threats determined to have a consequence with a minimal mission impact will be noted but not tested.

3.1.1 Posture and Likelihood

After assessing potential vulnerabilities, the evaluator should review the findings and extrapolate beyond the results by assessing the likelihood of the threat being able to exploit system vulnerability. The likelihood of a threat being able to exploit a vulnerability can be assessed by first categorizing the threat. The evaluator should consult with cybersecurity experts as to whether there are any paradigms or trends among actors that will contribute to likelihood assignments. Table 7 lists an example of threat categories; experience level; and Tactics, Techniques, and Procedures (TTPs).

Table 7. Cybersecurity Threat Categorization

Threat Category		
Posture	Insider	• Consists of a User, Operator, or System Administrator • Legitimate physical and/or logical access to the system • Has all credentials for authorized access
Posture	Near-sider	• Visitors, cleaning crew • Has physical access but no credentials for authorized logical access
Posture	Outsider	• Foreign Government/Adversary, Hacker • No authorized physical or logical access • Engages from completely external vantage point • Connected to a network outside of the enterprise network perimeter firewall
Threat Experience Level		

Experience	Novice	• Typically uses open source tools and scripts that are ready "out of the box" without modification • No formal training
Experience	Intermediate	• Typically uses custom-developed tools and scripts • Formal training • Usually funded
Experience	Expert	• Typically uses custom advanced tool suites and techniques • Advanced training and highly capable • Formal CNO experience • Highly resourced
Threat Tactics, Techniques, and Procedures		
Tactics	Consult INTEL Community	• POAM Compliance • Hacker Methodology • System VOLT • Exploit system itself, depot level maintenance, supply chain, etc.

After a threat has been categorized, the evaluator must address the Likelihood, defined in Table 8, of a threat being able to exploit a system. The evaluator will develop the data inputs and justification for Likelihood ratings. For the Likelihood analysis, the evaluator must gather input from the ESR/CIPR, VOLT, SMEs, and any data currently available. The evaluator should consider consulting with the IPT for concurrence of the Likelihood rating.

Table 8. Likelihood

Likelihood	
1	Not Likely
2	Low Likelihood
3	Likely
4	Highly Likely
5	Near Certain

3.1.2 Consequence

The Consequence is defined by the impact of a particular threat on the system's function. The evaluator should establish early in system development what facets of the system are vital to defend in the event of an attack. Consequence will be used to prioritize evaluation issues and test requirements. Consequence ratings should include the potential to access another system or network if applicable. Given the fiscal constraints of the program, the assessment of consequence is a necessary step. The evaluator should consult with the Intelligence (INTEL) community to learn what types of threats pose the most detriment and what data a threat may try to gain if granted access to the system. The vital components that are required for the defense of the system should be categorized and prioritized. The evaluator will conduct the consequence analysis, but input will be derived from the user, PM, and evaluation community.

Table 9 lists the consequence categories and examples. It also provides a list of example questions to derive mission impact from the threat consequences.

583
584
585 **Table 9. Cyber Security Consequence Definitions**
586

Consequence Category	Definition	Example	Mission Relevance
Confidentiality (C)	Only those authorized to view information are allowed to access it.	• Classification levels • Required security clearance levels to access information • Encryption • Protecting access to other linked systems	• What are the impacts of unauthorized disclosure of information on the mission?
Integrity (I)	Information remains unchanged and no one has tampered with it.	• Antivirus software • Security policy and training (to minimize risk of malicious code, viruses, etc.) • Hashing	• What are the impacts of unauthorized modification, destruction of information, and misinformation on the mission?
Availability (A)	Information must be available for use by those allowed to access it.	• Protection against malicious code, hackers, denial of service attacks	• What are the impacts of loss of use of a system or information on the mission?
Authentication (AT)	Ensuring that users are actually who they say that they are. Can also be used for identifying devices and data messages.	• User name • Password • Tokens • Biometrics	• What are the impacts of lack of authentication or false authentication on the mission?
Non-Repudiation (NR)	A person cannot deny completing an action because there will be proof that he/she did it.	• Digital signatures	• What are the impacts of loss of Non-Repudiation if overridden?

587
588 The evaluator must rate the Consequence for each category using the definitions from Table 10,
589 considering consulting with the IPT for concurrence of the Consequence rating.
590
591 **Table 10. Cyber Security Consequences**
592

Consequence	
1	Minimal or no consequence to C, I, A, AT, or NR
2	Minor reduction in C, I, A, AT, or NR; little impact
3	Moderate reduction in C, I, A, AT, or NR; limited impact
4	Significant degradation in C, I, A, AT, or NR; may jeopardize survivability
5	Severe degradation in C, I, A, AT, or NR; will jeopardize survivability

593

3.2 EW Survivability

EW threats are generally found in VOLTs, or other threat documentation. Table 14 lists examples of threat categories and descriptions concentrated on optics, radar, and communication.

Table 11. EW Threat Categorization

Type	Description
Jamming	Spot, Infrared, Barrage, Sweep, Pulse, Cover Pulse, and Deceptive techniques.
Digital Radio Frequency Memory (DRFM)	A repeater technique that manipulates received radar energy and retransmits it to change the return the radar sees.
Deceptive Jamming	Uses techniques such as “range gate pull off” to break radar lock.
Electronic Warfare Support, and Electronic Reconnaissance	Detection, location, identification, and evaluation of electromagnetic radiations.
Thermal Imaging and Laser Systems	Provides target coordinates and pulse code.
High-Energy Laser	Near- and mid-IR chemical lasers using hundreds of kilowatts, allowing the ability to deliver beam folding optics to target.
Heat-Seeking and Imaging	Missile seeking weapons.
Electromagnetic Pulse (EMP)	A short burst of electromagnetic energy.
High-Power Microwave (HPM)	Emits highly focused energy, transferring energy to a target.
Ultra-Wide Band (UWB)	Uses UWB frequencies to engage and disrupt target.
Low Energy Lasers	Uses low GHz to deliver beam to target.

Once threats have been identified and defined, they must be accredited to be used in the T&E program. Accreditation is usually conducted under the coordination of an EW Threat Accreditation Working Group (TAWG).

The TAWG is established under the T&E Working Integration Product Team (WIPT) and conducted in accordance with AR 73-1 and DA Pam 73-1 to accredit threat representations for use in T&E. The ATEC threat coordinator, or evaluator, chairs the TAWG. The Deputy Chief of Staff (DCS), G-2 (DAMI-FIT) coordinates threat support. Membership to TAWG includes ATEC HQ (Threats), the PM, the Supporting Threat Manager (TM) and Foreign Intelligence Officer (FIO), testers, AEC, the DCS, G-2, the Threat Simulator Management Office (TSMO)/Targets Management Office (TMO), and threat representation developer (if different from TSMO/TMO).

Threat system accreditation identifies, analyzes, and documents the differences between the threat representation and the Headquarters, Department of the Army (HQDA) or Defense Intelligence Agency (DIA)-validated intelligence assessment of the actual threat system. Differences between threat representations and DIA-validated intelligence threats are documented and analyzed in threat representation accreditation reports issued by the TAWG. The Threat Integration Staff Officers (TISO) and Threat Analyst (TA) ensure the actual threat system data parameters are clearly laid out in the threat representation accreditation report. The TISO/TA assists in defining differences between the actual threat and the threat representation parameters and in defining the impacts of those differences on the test.

All differences affecting test issues should be noted as test limitations.

3.2.1 Likelihood

The evaluator must review the findings and assess the likelihood of the threat being able to exploit system vulnerabilities. Threat and intelligence documentation provide insights, but fielding plans, CONOPs, and SME assessments of nearby equipment should be leveraged whenever possible.

Electronic protection may reduce the likelihood of the threat being able to target and exploit system vulnerabilities. Examples of electronic protection activity is described in Table 12.

Table 12. Electronic Protection Activities

Electronic Protection Activity	Description
Electromagnetic Hardening	Consists of action taken to protect personnel, facilities, and/or equipment by filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of electromagnetic energy.
Electronic Masking	Controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electronic warfare support measures/signals intelligence, without significantly degrading the operation of friendly systems.
Emission Control	Selective and controlled use of electromagnetic, acoustic or other emitters to optimize command and control capabilities while minimizing transmissions for operations security.
Spectrum Management	Control of the electromagnetic spectrum to ensure that systems have the required frequencies available for proper operation.
Wartime Reserve Modes	Characteristics and operational capabilities that contribute to military effectiveness and are withheld for wartime or emergency use.
Electromagnetic Compatibility	Ability of systems and components to operate in their intended environment without operational degradation or interference. This includes the use of doctrines or TTPs which maximize operational effectiveness.

3.2.2 Consequence

The Consequence is defined by the impact of a particular threat on the system's function. The evaluator should establish early in system development what facets of the system are vital to defend in the event of an attack. This establishment will require consulting with the INTEL community to learn what types of threats pose the most detriment. The evaluator should then categorize and prioritize the critical components that require defense of the system. Table 13 lists the Consequence categories, as they may affect components, and examples.

Table 13. Consequence Categories

Consequence Category	Definition	Example
System Impact (Temporary)	Susceptibility of the system, subsystem, components, and functions to electronic attack. Technical impacts to subsystems, components, and functions are able to be restored to full operational capacity.	• Call completion rate able to be restored after X amount of time. • Message completion rates able to be restored after X amount of time. • Data transmission restored after X amount of time. • Subsystems, components, and functions able to be restored after X amount of time.
System Impact (Transient – Recoverable)	Susceptibility of the system, subsystem, components, and functions to electronic attack. Technical impacts to subsystems, components, and functions are not able to be recovered to full operational capacity.	• Call completion rate able to be recovered after X amount of time. • Message completion rates able to be recovered after X amount of time. • Data transmission recovered after X amount of time. • Subsystems, components, and functions able to be recovered after X amount of time.
System Impact (Permanent)	Susceptibility of the system, subsystem, components, and functions to electronic attack. Technical impacts to subsystems, components, and functions are not able to be recovered to full operational capacity.	• Complete loss of system, subsystems, components, and functions, and no ability to restore or recover the system.

3.3 Evaluating CEMA Risk and Mission Impact

Anomalies are likely to be found and the evaluator will need to present support for their evaluation with suggested mitigations. Risk matrices can be developed to address this need.

Each risk matrix (as shown in Figure 7) would be developed by the evaluator similarly to the latest version of MIL STD 882. This technique allows the evaluator to organize and present risk assessments for multiple anomalies while showing the benefits of suggested mitigations.

Examples of risk matrices are:

- Likelihood vs. Consequence for Confidentiality
- Likelihood vs. Consequence for Integrity
- Likelihood vs. Consequence for Availability
- Likelihood vs. Consequence for Authentication
- Likelihood vs. Consequence for Non-Repudiation
- Likelihood vs. Consequence for EW Threat 1
- Likelihood vs. Consequence for EW Threat 2

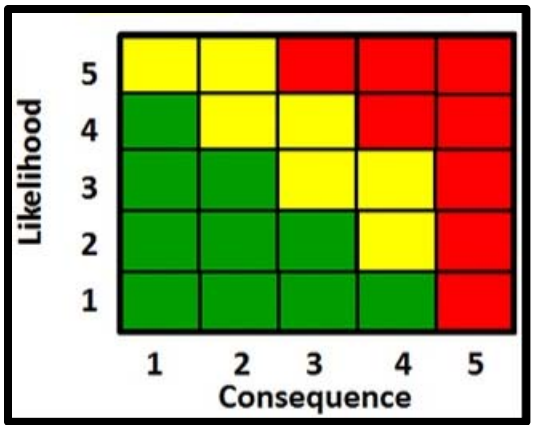

Figure 7. Example of Likelihood vs. Consequence Risk Matrix.

These matrices can be updated, or additional matrices can be created, for each evaluation report. They can be updated with additional information whenever available and can provide historical traceability as well as strategic direction for programs and evaluations.

APPENDIX A:
ACRONYMS

679 INTENTIONALLY LEFT BLANK

A	Availability
AA	Adversarial Assessment
AEC	U.S. Army Evaluation Center
AI	Additional Issue
AT	Authentication
C	Confidentiality
CCR	Call Completion Rate
CDD	Capability Development Document
CDR	Critical Design Review
CEMA	Cyber and Electromagnetic Activities
CIPR	Concept in Process Review
CNDSP	Computer Network Defense Service Provider
COI	Critical Operational Issue
COIC	Critical Operational Issue Criterion
CONOPS	Concept of Operations
COOP	Continuity of Operations
COTS	Commercial off the Shelf
CPD	Capability Production Document
CSS	Central Security Service
CVPA	Cooperative Vulnerability and Penetration Assessment
DaR	Data-at-rest
DEF	Defense Evaluation Framework
DEW	Directed Energy Weapon
DIACAP	Defense Information Assurance Certification and Accreditation Process
DiP	Data-in-process
DiT	Data-in-transit
DoD	Department of Defense
DODAF	Department of Defense Architectural Framework
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DOE	Design of Experiments
DOT&E	Director, Operational Test and Evaluation
DRFM	Digital Radio Frequency Memory
DSM	Data Source Matrix
DT	Developmental Test
DT&E	Developmental Test and Evaluation
EA	Electronic Attack
EMA	Electromagnetic Activity
EP	Electronic Protection
ES	Electronic Surveillance
ESR	Evaluation Strategy Review
EW	Electronic Warfare

FM	Field Manual
GIANT	GPS Interference and Navigation Tool
GOTS	Government off the Shelf
GPS	Global Positioning System
HW	Hardware
I	Integrity
IA	Information Assurance
ICD	Interface Control Document
IPT	Integrated Product Team
IR	Infrared
IT	Information Technology
JSR	Jamming-to-signal Ratio
KPP	Key Performance Parameter
MCR	Message Completion Rate
MDA	Milestone Decision Authority
MS	Milestone
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NR	Non-Repudiation
NSA	National Security Agency
OT	Operational Test
OT&E	Operational Test and Evaluation
OTA	Operational Test Agency
OTA TP	Operational Test Agency Test Plan
OV	Operational View
PDR	Preliminary Design Review
PM	Program Manager
PMO	Program Management Office
PPP	Program Protection Plan
RF	Radio Frequency
RMF	Risk Management Framework
SEP	System Evaluation Plan
SME	Subject Matter Expert
STIG	Standard Technical Implementation Guide
SV	System View

SW	Software
T&E	Test and Evaluation
TAWG	Threat Accreditation Working Group
TEMP	Test and Evaluation Master Plan
TTP	Tactics, Techniques and Procedures
UAV	Unmanned Air Vehicle
VOLT	Validated Online Lifecycle Threat
WIPT	Working Integration Product Team

680