SOAR

STATE-OF-THE-ART REPORT (SOAR)
JANUARY 2025

CSIAC-BCO-2024-617

CYBERTEST AND EVALUATION OF DEFENSIVE CYBEROPERATIONS IN THE U.S. ARMY

By Tiffany Williams, Matt Friar, Olutoye Sekiteri, and Philip Payne
Contract Number: FA8075-21-D-0001
Published By: CSIAC

This Page Intentionally Left Blank

SOAR

STATE-OF-THE-ART REPORT (SOAR)
JANUARY 2025

CYBERTEST AND EVALUATION OF DEFENSIVE CYBEROPERATIONS IN THE U.S. ARMY

TIFFANY WILLIAMS, MATT FRIAR,
OLUTOYE SEKITERI, AND PHILIP PAYNE

ABOUT CSIAC

The Cybersecurity & Information Systems Information Analysis Center (CSIAC) is a U.S. Department of Defense (DoD) IAC sponsored by the Defense Technical Information Center (DTIC). CSIAC is operated by SURVICE Engineering Company under contract FA8075-21-D-0001 and is one of the three next-generation IACs transforming the DoD IAC program: CSIAC, Defense Systems Information Analysis Center (DSIAC), and Homeland Defense & Security Information Analysis Center (HDIAC).

CSIAC serves as the U.S. national clearinghouse for worldwide scientific and technical information in four technical focus areas: cybersecurity; knowledge management and information sharing; modeling and simulation; and software data and analysis. As such, CSIAC collects, analyzes, synthesizes, and disseminates related technical information and data for each of these focus areas. These efforts facilitate a collaboration between scientists and engineers in the cybersecurity and information systems community while promoting improved productivity by fully leveraging this same community's respective knowledge base. CSIAC also uses information obtained to generate scientific and technical products, including databases, technology assessments, training materials, and various technical reports.

State-of-the-art reports (SOARs)—one of CSIAC's information products—provide in-depth analysis of current technologies, evaluate and synthesize the latest technical information available, and provide a comprehensive assessment of technologies related to CSIAC's technical focus areas. Specific topic areas are established from collaboration with the greater cybersecurity and information systems community and vetted with DTIC to ensure the value-added contributions to Warfighter needs.

CSIAC's mailing address:

CSIAC
4695 Millennium Drive
Belcamp, MD 21017-1505
Telephone: 443-360-4600

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE January 2025	**2. REPORT TYPE** State-of-the-Art Report	**3. DATES COVERED**
4. TITLE AND SUBTITLE Cybertest and Evaluation of Defensive Cyberoperations in the U.S. Army		**5a. CONTRACT NUMBER** FA8075-21-D-0001
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Tiffany Williams, Matt Friar, Olutoye Sekiteri, and Philip Payne		**5d. PROJECT NUMBER**
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Cybersecurity & Information Systems Information Analysis Center (CSIAC) SURVICE Engineering Company 4695 Millennium Drive Belcamp, MD 21017-1505		**8. PERFORMING ORGANIZATION REPORT NUMBER** CSIAC-BCO-2024-617
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center (DTIC) 8725 John J. Kingman Road Fort Belvoir, VA 22060		**10. SPONSOR/MONITOR'S ACRONYM(S)** DTIC
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution Statement A. Approved for public release: distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Like the land domain, cyberspace must be defended. The U.S. Army has begun to deliver innovative and dominant cyberspace capabilities to cyberwarfighters (e.g., cyberprotection teams and regional cybercenters) based on mission and threat through Project Manager Defensive Cyber Operations (PM DCO).

This state-of-the-art report delves into the cybersecurity testing activities for defensive cyberoperations (DCO), which include discovery, vulnerability analysis, continuous monitoring, intel support, mitigation/remediation, event correlation, penetration testing, threat emulation, and malware analysis.

Key U.S. Department of Defense cybersecurity strategy and policies applicable to DCO are identified and defined. Additionally, this report explores the software tools and testing events used to establish the effectiveness and cyber-resiliency of the system under test. Lastly, three use cases detailing how PM DCO conducts cybertest and evaluation are presented.

15. SUBJECT TERMS
cybersecurity, test and evaluation, developmental test and evaluation, operational test and evaluation, attack surface, defensive cyberoperations, discovery, vulnerability analysis, continuous monitoring, intel support, threat emulation, malware analysis, ARCYBER

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
U			UU	48	Vincent "Ted" Welsh
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED			443-360-4600

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

ON THE COVER:
(Source: U.S. Army)

THE AUTHORS

TIFFANY WILLIAMS

Ms. Williams is a cybersecurity analyst for the SURVICE Engineering company, with technical experience in network security, event monitoring, incident response, vulnerability management, and test and evaluation of the U.S. Army defensive cyberoperations (DCO) systems. Some of her key contributions include conducting the assessment, evaluation, and reporting of DCO systems. She supported the planning and execution of notable tests and assessments and provided recommendations to the Department of Homeland Defense and Cybersecurity and Infrastructure Security Agency. Ms. Williams holds a B.A. in computer information systems from the University of Arkansas at Little Rock and is currently pursuing a master's degree in computer science.

JOSEPH MATT FRIAR

Mr. Friar works with the Cybersecurity & Information Systems Information Analysis Center (CSIAC) team as a research inquiry analyst. At SURVICE, he performs in-depth research relating to technology fields, such as cybersecurity and information systems. He also works with government clients to provide information-oriented solutions and answers to technical inquiries. He recently graduated from Stevenson University, acquiring a B.S. in computer information systems, with a specialization in software design. At Stevenson, Mr. Friar was a member of the Leadership Scholars Program and was an active participant in technology-related events on campus.

OLUTOYE SEKITERI

Mr. Sekiteri works with CSIAC as a research analyst, where he provides research efforts related to CSIAC's four technical focus areas, conducts data analysis to support U.S. Department of Defense (DoD) science and technology communities, and connects government clients with subject matter experts to aid in answering technical inquiries. He obtained a B.S. in information systems from the University of Maryland, Baltimore County (UMBC), where he is currently pursuing a master's degree in cybersecurity. At UMBC, Mr. Sekiteri worked as a research assistant for its Department of Information Systems, supporting a research project by recording emergency medical technician stress levels during interactive simulations.

PHILIP PAYNE

Philip Payne is the CSIAC technical lead. He comes from a rich background in cybersecurity with the Command, Control, Communication, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance Center, where he led a world-class Cross Domain Solution Lab. He was a key member of the Information Security Branch, which has made a myriad of contributions in the DoD cyberspace. At SURVICE, he served as senior cybersecurity engineer for the Cyber Research and Development team supporting the Data Analysis Center on early acquisition cybersecurity assessments for Army systems. Mr. Payne possesses a B.S. and M.S. in computer engineering from the Johns Hopkins University and Polytechnic University, respectively.

ABSTRACT

Like the land domain, cyberspace must be defended. The U.S. Army has begun to deliver innovative and dominant cyberspace capabilities to cyberwarfighters (e.g., cyberprotection teams and regional cybercenters) based on mission and threat through Project Manager Defensive Cyber Operations (PM DCO).

This state-of-the-art report delves into the cybersecurity testing activities for defensive cyberoperations (DCO), which include discovery, vulnerability analysis, continuous monitoring, intel support, mitigation/remediation, event correlation, penetration testing, threat emulation, and malware analysis.

Key U.S. Department of Defense cybersecurity strategy and policies applicable to DCO are identified and defined. Additionally, this report explores the software tools and testing events used to establish the effectiveness and cyber-resiliency of the system under test. Lastly, three use cases detailing how PM DCO conducts cybertest and evaluation are presented.

ACKNOWLEDGMENTS

The authors would like to thank Kelvin Bouldin and Lamar McNair as members of the Defensive Cyber Operations Army Test and Evaluation Command Systems team.

CONTENTS

CONTENTS, *continued*

SECTION 01 INTRODUCTION

Test and evaluation (T&E) efforts are critical to the U.S. Department of Defense's (DoD) overall acquisition process [1]. T&E activities have provided the data needed to present and validate functional, technical, and warfighting capabilities that span all domains of the DoD. T&E processes also provide the opportunity to identify, analyze, and address shortcomings within a system before making a final acquisition or fielding decision. Going through the T&E process provides decision-makers and hands-on engineers with enough insight to assist in managing and mitigating operational risk; measuring technical progress; and understanding and characterizing operational effectiveness, suitability, survivability, and lethality as a program's acquisition process progresses.

According to the DoD's *Cybersecurity Test and Evaluation Guidebook* [2]:

> The goal of cybersecurity T&E is to identify and mitigate exploitable system vulnerabilities impacting operational resilience of military capabilities before system deployment, to include safety, survivability, and security. Early discovery of system vulnerabilities can facilitate remediation and reduce impact on cost, schedule, and performance.

To facilitate cybersecurity T&E throughout the DoD, various organizations have been tasked with supporting the cybercapabilities and survivability of the U.S. Army's weapon systems, equipment, cybersecurity, information systems, and electronic warfare operations. The DoD has provided strategies and guidance on the development and testing of hardware and software used in these operations. Along with strategies, there are tools used to help support the DoD's overall T&E and cybermission. With the ever-changing and expanding landscape of cybersecurity, it is of great importance that personnel supporting the DoD are equipped with the correct processes, procedures, and tools to conduct risk mitigation and ensure the safety of cybermilitary operations and the Warfighter.

This state-of-the-art report first presents the main testing organizations within the U.S. Army. Section 2 identifies a key cybersecurity strategy applicable to defensive cyberoperations (DCO). Then the cyber-T&E activities used by DCO programs are defined. For each activity, the corresponding tools and analysis used by the U.S. Army Cyber Command (ARCYBER) are listed and identified. Lastly, three specific use cases are detailed, showing how Project Manager Defensive Cyber Operations (PM DCO) conducts cyber-T&E.

This Page Intentionally Left Blank

SECTION 02 KEY PLAYERS/ TESTING ORGANIZATIONS

There are many organizations that perform cyber-T&E. This report begins by identifying those key players within the Army. This section provides a brief description of some of the testing organizations relative to DCO.

2.1 U.S. ARMY TEST AND EVALUATION COMMAND (ATEC) ELECTRONIC PROVING GROUND (EPG)

ATEC plays a pivotal role in ensuring the operational effectiveness, suitability, and cybersurvivability of the Army's weapon systems and equipment [3]. As an independent evaluator, it is responsible for conducting rigorous testing, evaluation, and assessment of military capabilities to inform decision-making processes. All testing is done while adhering to a rigid set of military standards and validating the results produced by the command. ATEC operates through different locations and subordinate commands throughout the United States, with its headquarters located at Aberdeen Proving Ground, MD. Each test center focuses on different testing capabilities, such as aircraft systems, direct energy, and chemical defense, along with many others.

As a component of ATEC, EPG performs testing for command, control, communications, computers, cyber, intelligence, surveillance, and reconnaissance [4]. By providing T&E services in the areas of cybersecurity and information assurance, EPG can support the resilience of Army networks.

2.2 ARCYBER

ARCYBER is the supporting Army headquarters under U.S. Cyber Command (CYBERCOM) [5]. It directs and conducts integrated electronic warfare, information, and cyberspace operations as authorized or directed to ensure freedom of action in and through cyberspace and the information environment and to deny the same to U.S. adversaries. The command supports Army networks across the globe and develops both offensive and defensive cybercomponents for information networks within the DoD. It provides essential cybereducation and training to Army personnel to equip them with the knowledge required for cyberoperations. ARCYBER also collaborates with many organizations in the cybersecurity industry, intelligence community, and academia to ensure that the Army can adapt to the fast-paced world of cyberthreats.

2.3 ARMY CAPABILITIES MANAGER-CYBER (ACM-Cyber)

The role of ACM-Cyber involves overseeing and managing the development, integration, and sustainment of cybercapabilities within the Army. It plays a crucial role in identifying and prioritizing the Army's cyber-requirements and aligning them with strategic objectives. This includes working the acquisition and fielding of cyber-related systems, such as the DCO program discussed in this report.

2.4 U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND (CCDC) DATA ANALYSIS CENTER (DAC)

CCDC (also known as DEVCOM) DAC is responsible for the Cooperative Vulnerability Penetration Assessment (CVPA). The CVPA is a series of events designed to identify all significant vulnerabilities and the risk of exploitation of those vulnerabilities. Subject matter experts (SMEs) from CCDC DAC, in coordination with ATEC, conduct this assessment in an operational context, which is often an entrance criterion to operational testing. The CVPA may be integrated with other developmental test (DT) events. CCDC DAC also provides support to the Army through its technical focus areas of data science, cyber-resilience, operation research, and others [6].

2.5 THREAT SYSTEMS MANAGEMENT OFFICE (TSMO)

TSMO, under the Program Executive Office (PEO) for Simulation, Training, and Instrumentation, is responsible for overseeing and managing the development, deployment, and sustainment of threat systems that stimulate realistic adversarial capabilities during military testing and training exercises. ATEC coordinates with TSMO to act as the Red team during the adversarial assessment (AA). The AA assesses the ability of a unit equipped with the system to support its mission while withstanding cyberthreat activity representative of the enemy. The AA should be conducted in an operational environment and, if possible, during an operational test (OT).

2.6 ARMY CYBER INSTITUTE (ACI)

ACI is another organization that focuses on cyber-research and analysis [7]. Located at the U.S. Military Academy at West Point, ACI develops technical solutions by collaborating with military, government, and industry entities to help the Army combat the evolving cyberspace threats. ACI is researching the fields of cyberspace operations, cyberpolicy, and threat casting.

2.7 U.S. ARMY CYBER CENTER OF EXCELLENCE (CCoE)

CCoE is an organization within the Army that develops solutions within the areas of cyberspace operations, information services, and electronic warfare [8]. It contributes to the Army's capabilities by providing tactics, techniques and procedures (TTPs) related to cybersecurity systems. CCoE also collaborates with companies from the private sector and academia to bridge cyberknowledge gaps present in the military.

2.8 DEFENSIVE SUITE OF COMPLIMENTARY SYSTEMS (DSCS)

The DSCS was developed as an incremental, evolutionary acquisition approach that employs iterative development of software/hardware. It leverages four operational needs statements to establish the acquisition Category III or below programs, which have transitioned into nine programs of record (PORs) under the PEO Enterprise Information Systems and one under PEO Command, Control, Communications-Tactical (C3T). These 10 PORs are described as follows:

1. Cyberanalytics: A cyberthreat and vulnerability hunting capability that allows the cyberteams to rapidly ingest large volumes of structured and unstructured data, as well as correlate, perform analysis, and visualize the data to rapidly detect and illuminate adversaries and vulnerabilities.
2. Deployable Defensive Cyberspace Operations System (DDS): A multiconfigurable, deployable kit that is transportable by aircraft or other means to support deployed DCO missions.
3. Garrison Defensive Cyberoperations Platform (GDP): A prepositioned infrastructure (at installations) consisting of commercial-off-the-shelf (COTS) hardware and software

(proprietary and open source) and limited government-off-the-shelf (GOTS) hardware and software that enable cyberteams to remotely conduct DCO missions.

4. DCO Tool Suite: A set of software applications that are the fundamental tools enabling cybermission forces to perform DCO missions executed and managed on the DCO platforms.
5. Forensics/Malware: A capability to rapidly triage malware incidents; return impacted systems/services to full operations; detect, analyze, mitigate, and eradicate malicious activity (malware) on defended networked environments; and identify the root cause/ threat actor.
6. User Activity Monitoring: A software-based, scalable capability that proactively identifies and mitigates internal risks associated with unauthorized actions, including theft and misuse of critical or mission-essential data across all secured networks.
7. Counter-Infiltration: A capability that finds and quarantines threats that bypass defenses as counter-infiltration operations.
8. Threat Emulation: A capability that implements real-world threat TTPs against risk areas.
9. Castle Keep (CK): A strategy that develops new cybersecurity capabilities through development and integration of defensive cybersecurity solutions. CK develops the special security component of the capabilities detailed in the Land War Net Intelligence Community Directive to support the Army's intelligence warfighting function force generation and special security requirements [9].
10. Tactical Defensive Cyberspace Operations Infrastructure (TDI): A prepositioned infrastructure to provide robust computing resources within a tactical operations center or tactical command post. TDI is the only program in the DCO portfolio under PEO C3T.

This Page Intentionally Left Blank

SECTION 03 DOD CYBERSECURITY STRATEGY APPLICABLE TO DCO

Cybersecurity Test and Evaluation (CSTE) starts at the initiation of acquisition and continues throughout the entire life cycle of the software and hardware capabilities [2]. CSTE is a culmination of cybersecurity T&E activities, including vulnerability assessments, security controls testing, penetration testing, and adversarial testing. U.S. Department of Defense Instruction (DoDI) 5000.89 "Test and Evaluation" [10] provides guidance for mission-focused cyber-developmental test and evaluation (DT&E) to stakeholders involved with DoD systems. The information present in the document can aid engineers in measuring progress, identifying problems, defining capabilities, and managing risks when working on cyber-related programs. This also allows for the iterative development of survivable and resilient systems in cyberspace. Cyber-DT&E activities should be performed with the goal to evaluate a system's ability to prevent negative cyberspace events with operational mission impacts, detect anomalies, determine the cause of anomaly, mitigate future instances of a cyberspace event, and recover from an anomaly to ensure operational resilience. Testing results should be used to make informed decisions related to capability development, acquisition, risk acceptance, integration, requirements, and future testing procedures.

When planning cyber-DT&E events, the system developer contractor, integrated contractor, and government should be involved. Testing should be performed by test teams that are not working on the system itself and should be qualified as outlined in U.S. Department of Defense Directive (DoDD) 8140.01 "Cyberspace Workforce Management" [11] and DoDI 8585.01 "DoD Cyber Red Teams" [12]. The data used during testing events should originate from the system developer contractor, and monitoring efforts should be in place throughout the project life cycle, as described in DoDI 5000.79 "Defense-Wide Sharing and Use of Supplier and Product Performance (PI)" [13].

ATEC is involved in planning during the early stages of cybersecurity DT&E. To leverage a DT&E environment with the goal of satisfying operational test and evaluation (OT&E) requirements, evaluations must be demonstrated in an operationally realistic environment. The Cybersecurity Working Group (CyWG) identifies opportunities for testing events that satisfy both DT&E and OT&E objectives, if feasible. A successful evaluation also includes a mission-based cyber-risk assessment (MBCRA) when a significant change occurs with the mission, system, threat level, or operating environment. Examples can include any upgrades to the system software/hardware, new threat vectors (zero-day vulnerabilities), or deployment of DCO systems in a new operational environment. The MBCRA methodology prioritizes risk based on impacts to operational missions and the DCO system employed in the form of cyber-tabletop exercises. An MBCRA adds operational and adversarial test expertise to the evaluation, is developed during the DT&E phase, and is updated based on OT&E data collection, allowing stakeholders to make an informed decision on resilience and any remediation requirements.

Performance requirements must be measured when conducting cyber-DT&E, such as the fidelity of a system in contested cyberenvironments. The system must remain resilient during low bandwidth and disrupted situations. Cyber-DT&E activities must include realistic data and communication flows from the test team's evaluation and testing of the system. The capabilities to prevent, detect, contain, mitigate, and recover from mission effects must also be measured and verified. Effects of cyberspace attacks must be evaluated due to the possibility of cascading effects in both physical and cyberspace domains. Program managers (PMs) should be informed of technical cyber-risks from vulnerabilities and attack surface (AS) components found during testing, which could affect overall cybersurvivability.

"Purple team testing" should be utilized, which involves both cooperative and adversarial cyber-DT&E. This allows the testing team to detect potential methods to circumvent the system's security features. It is imperative to deconflict cooperative activities from adversarial activities to reduce risk of negative impacts during testing. The system should also be compliant with security technical implementation guides, as outlined in DoDI 8531.01 "Vulnerability Management" [14].

Stakeholders should stay up to date on changes to cybersecurity, cybersurvivability, and resilience risks from new software releases, emerging threat capabilities, new cyberspace attack techniques, and changes to existing technology. Changes to operational mission performance requirements, government supply chains, and software distribution channels should also be considered, as these factors could influence the requirements for new cybersystems under development. Making proactive changes to the project's scope could improve its cyberspace resiliency.

The DCO program team follows the cybersecurity policies and procedures, as detailed in DoDI 8500.01 "Cybersecurity" [15], DoDI 8510.01 "Risk Management Framework for DoD Systems" [16], DoDI 5000.89 [10], and Army Regulation (AR) 25-2 "Army Cybersecurity" [17] for the prototypes and PORs. The implementation of these policies by PM DCO helps safeguard DoD acquisition systems from cybersecurity-related risks throughout the system life cycle.

DoDI 8500.01 [15] defines the policy and procedures for cybersecurity. The policy is applicable to all DoD information technology (IT), while emphasizing operational resilience, integration, and interoperability throughout the acquisition life cycle. It references National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 "Security and Privacy Controls for Information Systems and Organizations" [18] for use in the DoD.

NIST SP 800-53 defines some of the following activities for CSTE stakeholders [18]:

- Conduct cybersecurity T&E throughout the acquisition life cycle.
- Ensure cybersecurity DT&E assessments are properly planned, resourced, integrated, and documented (e.g., a DCO simple acquisition management plan [SAMP]).
- Integrate CSTE with interoperability and other functional testing, such as the annual DCO cybersecurity CVPA and AA.

Acquisition programs like the DSCS must conduct an operational resilience evaluation during cybersecurity DT&E and OT&E. The system must be evaluated under realistic cyberconditions, with the ability to recover data while preventing and mitigating exploitations. The collection of data and reporting will support a fielding decision. These activities support the DCO objective of delivering high-fidelity cyberspace capabilities to the army, providing Warfighters with tools that give them the informational advantage.

The PM DCO team is responsible for coordinating periodic test exercises to demonstrate a program's ability to operate during loss of all information resources and connectivity, ensure systems can allocate information resources dynamically as needed, and sustain mission operations while addressing cybersecurity failures. Additionally, systems must be restored rapidly to a trusted state while maintaining support for ongoing missions.

DoDI 8510.01 [16] in accordance with NIST SP 800-37 "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy" [19] establishes policy, responsibility, and procedures for the maintenance of the Risk Management Framework (RMF) within DoD systems. The test community must integrate RMF with both DT&E and OT&E. The DCO infrastructure is currently categorized in DoDI 8510.01 [16] and Committee on National Security Systems Instruction (CNSSI) No. 1253 "Security Categorization and Control Selection for National Security Systems" [20]. The DSCS does not generate or consume personally identifiable information, personal health information, or law enforcement data. The DSCS security categorization is based on the implementation and may change over time as additional capabilities are added [16].

DoDI 5000.89 [10] provides T&E procedures for programs that are part of the adaptive acquisition framework. The policy applies to five of the six pathways found in the framework, which includes urgent capability acquisition, software acquisition, middle tier of acquisition, defense business systems, and major capability acquisition. The instruction explains the purpose of T&E, details the processes involved, and makes distinctions on how T&E can differ when applied to different offices. The *Test and Evaluation Enterprise Guidebook* [1] further expands on the policies found within DoDI 5000.89 [10].

This Page Intentionally Left Blank

SECTION 04 TEST TYPES

It is important to note that cybersecurity T&E is necessary and required by DoD policy, as well as both DT&E and OT&E. DT&E focuses on the process of generating knowledge to validate and support the capabilities and limitations of systems, subsystems, components, software, and materiel [1]. The knowledge and information are used to help provide program engineers, PMs, and decision-makers with information to measure progress, identify problems, characterize system capabilities and limitations, prepare for OT, and manage technical and programmatic risks throughout the program's acquisition life cycle [10].

DT&E assesses the maturity of technologies, system design, readiness for production, acceptance of government ownership of systems, readiness to participate in OT&E, and sustainment. DT&E activities start with the definition and development of capability requirements for the entity being tested. Identified conditions referring to test conditions that are controlled, uncontrolled, measured, or not measured are also defined. These requirements are created to ensure that important technical requirements are measurable, testable, and achievable and provide feedback showing that the tested system is performing properly [21]. DT&E activities continue throughout the development, delivery, acceptance, transition to OT&E, production, operations, and support. Overall, the DT&E program should do the following [22]:

- Verify the achievement of critical technical parameters and key performance parameters.
- Assess system specification compliance and the system's ability to achieve the thresholds prescribed in the capabilities documents.
- Provide data to the PM to enable root-cause determination of failures arising from tests and identify corrective actions.
- Provide information for cost, performance, and scheduled tradeoffs.
- Report on the program's progress to plan for reliability growth and assess reliability and maintainability performance for use during key program decisions.
- Identify system capabilities, limitations, and deficiencies.
- Assess system safety and compatibility with legacy systems.
- Stress the system within the intended operationally relevant mission environment to assess readiness for OT.
- Support all appropriate certification processes.
- Document achievement of contractual technical performance and verify incremental improvements and system corrective actions.
- Assess entry criteria for initial OT&E and follow-on OT&E.
- Provide DT&E data to validate parameters in modeling and simulation (M&S).
- Assess the maturity of the chosen integrated technologies T&E.
- Identify cybervulnerabilities within custom and commodity hardware and software on

components, subsystems, and systems so the program office can mitigate them early in the program's life cycle.

- Support cybersecurity assessments and authorization (A&As), including RMF security controls.

To evaluate DT adequacy, a PM uses the T&E strategy as the primary planning and management tool for the integrated test program. The documentation should describe a logical DT&E strategy, including:

- Decisions to be informed by the DT&E information.
- Evaluations to inform those decisions.
- Test and M&S events to be conducted to generate the data for the evaluation.
- Resources to be used and schedules to be followed to execute T&E events.

Developmental evaluations are accomplished most commonly using criteria the mission sets from the concept of operations/operational mode summary/mission profile, capability gaps, user requirements specified in the capabilities documents (initial capabilities document), capability development document, critical operational issues (COIs) and criteria, design measures contained in the technical requirements documents, and contractual performance specifications. The T&E strategy includes an integrated decision support key and evaluation framework that shows the correlation/mapping between decisions, capabilities to be evaluated, measures to be used to quantify the capabilities, and test and M&S events. The data collected during one test may result in multiple developmental evaluations being accomplished.

OT&E supports the evaluation of the operational performance of units equipped with systems operated under realistic operational conditions in an operationally representative threat environment (initial operational capability, plus 10 yr), including joint combat operations and system-of-systems concept of employment. Operational testing provides data required to enable credible evaluation of operational effectiveness, suitability, and survivability [10, 23, 24]. Ultimately, OT&E is trying to determine if T&E was performed adequately throughout the test life cycle and whether the results of such T&E confirm that the items or components tested are effective and suitable for combat.

To support OT&E efforts, in 2019, the OT community created a Director of Operational Test and Evaluation (DOT&E)-endorsed set of six core test principles: (1) Early Operational Testing Involvement, (2) Tailor to the Situation, (3) Continuous and Cumulative Feedback, (4) Streamline Processes and Products, (5) Integrated and Combined Collection/Test, and (6) Adaptive. The Six Principles of Test were adopted by the service OT agencies and the DOT&E to focus on delivering combat capability at the "speed of relevance." The principles apply to all acquisition types, technology demonstrations, and experimentation. The way T&E support quantity, speed to field, and increased performance is by testing earlier, faster, and smarter; discovering problems early; and reducing overall test-related costs. The efforts buy down costs, shorten development and production time, maximize the potential to move major decision points left, and support earlier fielding of combat capability. The six core test principles are detailed as follows [1]:

1. Early Operational Testing Involvement: Engage in programs as early as possible with acquisition partners and design integrated test events in an environment that can collect data once to answer the respective test objectives.
2. Tailor to the Situation: Empower test teams with flexibility to adjust their tests as needed to field capabilities as rapidly as possible. This gives teams the confidence to know they have the flexibility to tailor their test planning, execution, and reporting as needed.

3. Continuous and Cumulative Feedback: Ensure integrated testing provides timely feedback regarding the problems discovered throughout the life cycle of a program, especially in the earlier stages. Testing is a continuum, partnership, and communication between PMs and users that significantly reduces the chances of there being any surprises late in the testing process.
4. Streamline Processes and Products: Remove bureaucratic constraints from current processes to deliver combat capability to accrue warfighting advantages to the United States and its allies. As a new program comes online, test teams should have the flexibility to modify existing procedures. To enable fielding at the "speed of relevance," test teams must have the ability to streamline test processes and products to best meet the needs of the program.
5. Integrated and Combined Collection/Test: Have the goal to merge the primary test stakeholders (the T&E contractor/developer testers' contractor test [CT], DT, and OT) into one unified test team. As the program progresses through its acquisition life cycle, sequential testing is no longer conducted. Synchronized collection and data are pursued throughout acquisition stakeholder communities. All test events can be used at any point in the program to achieve CT, DT, and OT objectives in a collaborative fashion to the maximum extent possible—one team, one plan, one test.
6. Adaptive: With the push within DoD for rapid prototype fielding and today's ever-evolving technologies, the operational testing agencies must not be restricted by existing bureaucratic processes but must be allowed the freedom to change as the test proceeds to take advantage of learning during the test process.

Operational Assessments (OAs) are conducted by ATEC to provide an independent early assessment of the operational effectiveness and suitability of a capability. The OAs build upon the results rendered during DT and migrate test plans and procedures from system specification to operational mission verification and validation. The OA test plans and procedures further demonstrate verification and validation of COIs and measures of effectiveness (MOEs), in accordance with (IAW) an integrated test model. COIs are key operational effectiveness or suitability issues that must be examined in OT&E to determine the system's capability to perform its mission. COIs must be relevant to the required capabilities and of key importance to the system being operationally effective, operationally suitable and survivable, and representative of a significant risk, if not satisfactorily resolved. The MOEs should be broken up into different measures of performance (MOPs) that address how well the test entity is expected to satisfy each MOE. The MOPs should focus on measures that relate directly to operational performance characteristics. For example, measures can be based on resource utilization or the amount of time required to conduct a desired event [25].

Results from the OAs inform decision-makers on the maturity of the software/hardware in support of a deployment decision. The OAs are also leveraged as early analysis for the annual OT event. In addition to COIs and MOEs, cybersecurity and resilience are evaluated based on best practices for system software and hardware development, effective security controls and countermeasures, reliability of mission-critical assets, exposure to vulnerabilities, recovery time, and adequate user tools.

Simply put, the difference between DT&E and OT&E is that DT&E verifies the system is built correctly IAW the specification and contract and OT&E validates that the system can successfully accomplish its mission is a realistic operational environment [26]. In the cybercontext, these T&E activities and principles lay the groundwork for testing software/hardware systems that are previously, currently,

and will be fielded by the DoD. They also improve the safety, effectiveness, and survivability of the Warfighters tasked with using these systems. Table 4-1 depicts the difference between DT&E and OT&E.

Table 4-1. DT&E vs. OT&E

DT&E	OT&E
Measures Technical Performance	Measures Operational Effectiveness and Suitability
Leverages Technical Personnel	Leverages Operational Personnel
Holds DT&E Agency Responsible	Holds OT&E Agency Responsible
Has Prototype or DT Article	Has Production-Representative Test Article
Is Done in Controlled Test Environment	Is Done in Combat/"Real-World" Environment
Provides Preview for OT&E	Provides Feedback for DT&E
Has Heavy Contractor (Developer) Involvement	Does Not Allow System Contractor (Developer)

SECTION 05 CYBERSECURITY DT&E ITERATIVE PROCESS

At the time of writing this report, the Office of the Under Secretary of Defense for Research and Engineering was drafting the U.S. Department of Defense Manual (DoDM) 5000.UY titled *Cyber Developmental Test and Evaluation* [27]. That manual and the to-be-published accompanying guidebook will replace the *Cybersecurity Test and Evaluation Guidebook*, version 2.0 [2].

Each cybersecurity DT&E step includes analysis and planning activities for the subsequent actions and traces back to the DoDI 5000.02 "Operation of the Adaptive Acquisition Framework" [28] acquisition life cycle. The key initial step of the DT&E iterative process is planning, which involves developing a process that supports system design and development. Planning also considers the scope, test software/hardware, and opposing force skillset, and it relies on collaboration between the test team and engineering team during the early stages of system design and development.

The next steps involve preparation and execution, which comprise cybersecurity DT&E execution activities for the system. Test objectives and events are based on analysis and data collection during planning. The last two iterative steps involve the evaluation and reporting of cybersecurity OT&E activities. Cybersecurity operational testers provide the information needed to resolve operational cybersecurity issues, identify vulnerabilities in a mission context, and describe operational effects of discovered vulnerabilities.

5.1 PLANNING FOR CYBER-DT&E

The planning step examines the cyber-resilience requirements for developing an initial DT&E strategy. The CyWG, which reports to the T&E Working Integrated Product team, is responsible for performing all tasks throughout the entire process, and recommends a frequency (minimum annual testing for DCO) to conduct cybersecurity threat assessments throughout the system developmental life cycle. The CyWG consists of SMEs who foster the collaboration on cybersecurity and resilience between system engineering and T&E s teams. ATEC, ARCYBER, and ACM-Cyber are a few of the members among the group of SMEs. The CyWG ensures the integration between adversarial/vulnerability test teams and system engineers/developers. This allows stakeholders to design cyber-resiliency into the functional mission of the users of the DCO system. Additionally, this integration helps with system design by promoting a focus on mission capabilities, functional resiliency, safety, and cybersecurity threats.

The CyWG is responsible for integrating and coordinating all cybersecurity T&E and supporting the RMF A&A process. The information system security manager coordinates RMF A&A activities, and the remaining members of the CyWG ensure the successful implementation of the CSTE. The CyWG ensures requirements are testable, measurable, and achievable. The integration of RMF assessment activities with cybersecurity DT&E provides a wholistic evaluation of the

system's cybersecurity and resilience posture. Testers analyze architectures, system designs, and key interfaces to help refine cybersecurity and resilience requirements. Additionally, planning may be repeated and performed in parallel with preparation, depending on these changes and any testing results discovered during the execution.

An interim authority to test (IATT) is required if an operationally realistic environment or live operational data are required to support a functional DT&E or early OAs. The plan for an IATT includes developmental testing, security controls assessment, and assessment and compliance of the relevant security technical implementation guide. Prior to receipt of an IATT and part of the RMF process, verification of controls in a development laboratory and/or isolated test ranges is required unless testing is conducted in a closed-loop environment. Documentation of test objectives should include requirements for DT&E, OT&E, and RMF. Programs offices document and track remediation of all discovered vulnerabilities in a plan of action and milestones [2].

The planning step identifies vulnerabilities and avenues of attack an adversary may use to exploit the system. Additionally, the test team develops a plan to evaluate the mission impact. An AS can be described as different points in a system architecture where an attacker could gain entry to compromise a system [2]. The system's exposure to reachable and exploitable vulnerabilities (i.e., any connection, data exchange, service, removable media, etc.) can potentially subject the system to access from a threat actor. AS tasks can be characterized by identification, analyzation, and report documentation. Additionally, roles and responsibilities must be examined and mission dependencies must be mapped. AS analysis informs the system design and operation, cybersecurity risk and mission impact, and overall test planning. ASs are dynamic and can be amended throughout the testing life cycle.

5.2 PREPARING FOR CYBER-DT&E

The preparation step verifies cybersecurity and resilience while identifying vulnerabilities and needed mitigations. This informs system designers, developers, and engineers of needed cybersurvivability and resilience improvements to reduce risk on COTS and GOTS systems. COTS components may contain known vulnerabilities that are exploitable and documented in vulnerability databases, such as Common Weakness Enumeration, Common Vulnerabilities and Exposures, National Vulnerability Database, and Common Attack Pattern Enumeration and Classification. The preparation step identifies known cybersecurity system architecture, interfaces, and operational vulnerabilities. An appropriate mitigation or countermeasure associated with each risk is also identified. Technical parameters defined by the system engineer are evaluated and verified for operational effectiveness. After assessing the vulnerabilities, the team provides feedback to the CyWG for a resolution. The AS analysis feeds into testing efforts in the execution step of the iterative process, making the event a cooperative test.

5.3 EXECUTING CYBER-DT&E

This step provides characterization system status for cybersecurity and resilience in a fully operational environment. It also provides system reconnaissance in support of the AA. Cybersecurity OT&E assesses the ability of the system to enable operators with the execution of critical missions in an operational environment. The CVPA provides a comprehensive analysis and reconnaissance of system cybersecurity and resilience within a fully operational context.

Inputs to support the continuity of operations for a CVPA include the Authority to Operate; DT&E test results; mitigation plan; Operational Test Readiness Review; OT&E test plan; training materials; accreditation artifacts; and all relevant system

documentation, such as network architecture. The Operational Test Agency (OTA) team leads the testing and reporting for the CVPA because it is an OT&E event. The team also develops an analytical framework of issues, MOEs, suitability, and survivability. Data requirements and collection procedures, including instrumentation, recording of observations and actions, and surveys, are also developed. Additionally, the test design framework (length, scenarios, and vignettes) is designed and included in a report that addresses the collected data and evaluation results.

5.4 EVALUATING AND REPORTING CYBER-DT&E RESULTS

This step characterizes the operational mission effects to critical missions caused by threat-representative cyberactivity against a unit trained and equipped with a system, in addition to the effectiveness of defensive capabilities. The critical mission execution capabilities are evaluated, including tiered defenses, detection and response to cyberattacks, system survivability, and recovery. Near-sider, insider, and outsider threat postures are also evaluated. The AA is conducted before a full deployment decision and in support of OT&E. A minimum of 1–2 weeks of dedicated testing is recommended for the duration of the AA.

Coordination details of the AA are communicated through the CyWG and documented in the OT plan and reports. Planning includes the following resources to assess cybersecurity and resilience: an NSA-certified, CYBERCOM accredited Red team to act as the adversary; operationally representative hardware/software; and any additional resources required for CVPA, such as cybersecurity metrics, data requirements and collection, observation records, instrumentation, surveys, scenarios, and vignettes.

The AA produces a report that includes the assessment of effectiveness, suitability, and survivability of the system under test (SUT) and informs a fielding decision. Authorized tools used to assess cybersecurity and resilience should be removed from the SUT upon completion of the test.

This Page Intentionally Left Blank

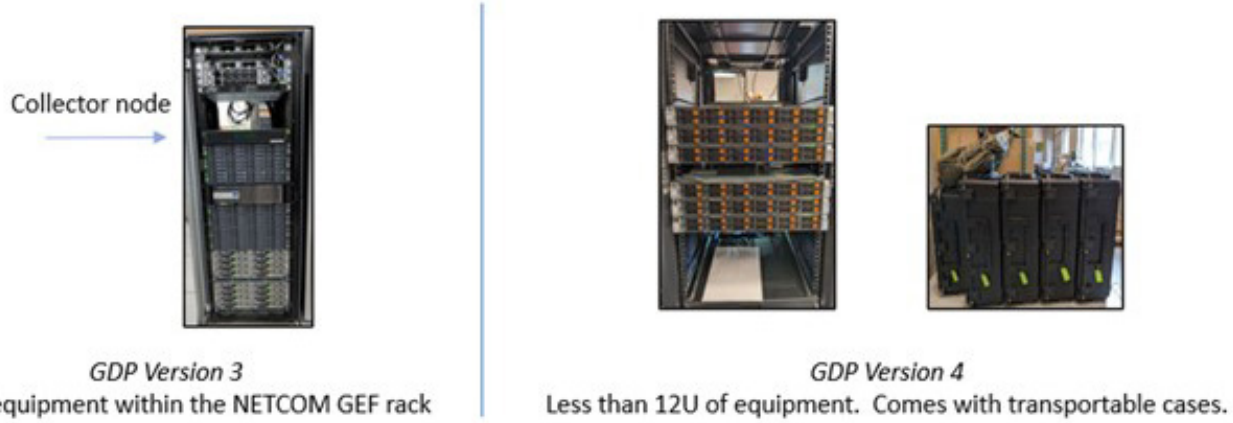
06 DCO CYBER-T&E ACTIVITIES

The DCO acquisition strategy is rapid and agile, with an evolutionary capability model based on a series of independent evaluations and associated risk performed by ATEC. To complement the agile acquisition testing strategy, documentation is streamlined with the creation of a SAMP. The SAMP creates a baseline and comprises a family of systems with an annex for each POR and addendum for each capability drop (CD). CDs describe the performance characteristics of a relatively small increment of a software or hardware solution necessary for partial deployment of the overall capability solution, generally derived from a requirements definition package.

Additionally, the SAMP covers the engineering, testing, and integration of software and hardware. Overall, it also documents the Army's DCO plan [29], defining the governance and execution strategy to acquire, integrate, test, field, and sustain the DSCS. The primary focus of the DCO program T&E methodology is to have the end user engaged throughout the testing life cycle to ensure the operational utility delivered, satisfying mission execution.

The DCO hardware components—the GDP and DDS platform—are the infrastructure-as-a-service (IaaS) elements of DCO (Figures 6-1 and 6-2, respectively). Additionally, the DCO IaaS is composed of the GDP and DDS hardware and software infrastructure upon which virtual machines operate as a platform as a service.

The DCO PORs are designed to preserve the Army's ability to utilize friendly cyberspace from enemy and adversary actions using the following cyber-T&E activities: discovery, vulnerability analysis (VA),



GDP Version 3
2-3U of equipment within the NETCOM GEF rack

GDP Version 4
Less than 12U of equipment. Comes with transportable cases.

Note: NETCOM = U.S. Army Network Enterprise Technology Command, GEF = Global Enterprise Fabric

Figure 6-1. GDP *(Source: PEO Intelligence, Electronic Warfare, and Sensors [IEW&S] [30]).*

Figure 6-2. DDS *(Source: PEO IEW&S [31]).*

continuous monitoring, intel support, mitigation/remediation, event correlation, penetration testing, threat emulation, and malware analysis. Sections 6.1–6.9 define each activity and provide examples of tools used by ARCYBER. Section 6.10 details additional ARCYBER DCO tools not specifically linked to one of the cyber-T&E activities described in Sections 6.1–6.9.

6.1 DISCOVERY

Discovery is the act of locating a machine-processable description of a web-service-related resource that may have been previously unknown and meets certain functional criteria [32]. It involves matching a set of functional and other criteria with a set of resource descriptions. The goal is to find an appropriate web-service-related resource. Discovery, in the context of Army cyberoperations, is the process of identification, mapping, and understanding an adversary's digital footprint, to include vulnerabilities and tactics. Additionally, Army cyberoperations encompass both passive and active reconnaissance techniques, with the intent of gaining actionable intelligence to support mission objectives.

Discovery enhances the Army's situational awareness by providing real-time insight into the cyberthreat landscape. Army cyberoperations can prioritize resources effectively by identifying high-value targets and critical vulnerabilities, as well as other potential attack vectors. Discovery also facilitates the collection of adversary attacks and TTPs for analysis and counteraction. The following lists example DCO tools employed by ARCYBER for discovery [33]:

- Red Seal: A software tool that analyzes an organization's network and automatically builds a model so operators can understand and continuously monitor the environment wholistically. It allows an operator to measure, benchmark, and set objectives to actively manage the digital resilience of the network and security infrastructure. It finds configuration errors and discovers unintended access paths. It is considered a security analytics platform that helps verify compliance with established operating standards, policies, and regulations. Additionally, it provides actionable intelligence for rapid response by identifying exposed assets and prioritizing actions. Red Seal enables integration with various cloud-based hardware and software technologies.
- Endgame: An endpoint solution-focused software application that prevents damage and loss from new attacks, stops ongoing attacks, and automates the hunt for the next generation of attacks. Endgame enables an organization to be more proactive with prevention, mitigation, and response using a single agent.
- Google Rapid Response (GRR): A client-server application used as a remote, live forensics tool for incident response. Initially, an agent is deployed on potential systems that need investigating. Once deployed, each system becomes a client and starts receiving messages from the front-end servers. Each message tells the client to run a specific client action and return the results to the server. A client action

is a familiar code that the agent knows how to execute (e.g., obtaining the list of files in a directory or reading a buffer from a file).

- BlueScope: A proprietary government software developed as a network discovery and enumeration tool suite to determine host integrity on a Windows network. It automates the collection of critical information from remote Windows hosts and manages host diagnostics, scans, and payload deployments. It supports file collection and analysis of data, using plug-ins and extensions. It adds hosts from an active directory (AD) and facilitates group policy analysis, to include enterprise-wide virus scanning. It performs domain name system (DNS) resolution and name deconfliction using AD and DNS entries. Additionally, it runs diagnostic tests to determine Window Machine Instrumentation connectivity, ping responses, and administrative capability. BlueScope consists of the Kinetic LINK (KLINK) Evaluation Suite, KLINK Analysis Suite, and Universal Serial Bus (known as USB) Detect.
- My Structured Query Language (MySQL) Workbench: A unified visual tool for database architects, developers, and database administrators (DBAs). It provides data modeling, structured query language development, and comprehensive administration tools for server configuration and user administration. It enables a DBA, developer, or data architect to visually design, model, generate, and manage databases. It includes everything a data modeler needs for creating complex entity relationship models, as well as forward and reverse engineering. MySQL Workbench also delivers key features for performing difficult change management and documentation tasks that normally require much time and effort.
- Network Visualization Suite: A mapping tool that connects hosts for network passive discovery and network traffic analysis. It utilizes developed protocols like the commercial tools Network Mapping (NMAP) and Scapy (a tool used to manipulate network packets written in Python). Additionally, Network Visualization Suite identifies multiple levels of systems, from network to computer and voice systems.

6.2 VA

VA is the formal description and evaluation of the vulnerabilities in an information system. It involves the identification and assessment of weaknesses in a system's security, helping to pinpoint potential entry points for attackers, which requires organizations to patch or mitigate vulnerabilities to strengthen the overall security posture and protect against potential cyberthreats. Additionally, VA is the systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. The following lists example DCO tools employed by ARCYBER for VA [34]:

- Red Seal: (See description in Section 6.1.)
- Nipper Studio: An advanced and detailed configuration auditing tool. It helps harden and secure vital network devices, such as firewalls, switches and routers. It provides detailed configuration reporting and quick, clear views of device settings. Additionally, Nipper Studio is agentless; it can audit offline, online, physically, and virtually, as well as in isolated systems. Tools can be scheduled or scripted and work on multiple platforms.
- Assured Compliance Assessment Solution (ACAS): An integrated software solution that is scalable to an unlimited number of locations. Its tiering ability enhances security with simplistic installation and ease of use. It can be deployed as an independent download without the need to procure and

install appliance devices. Its product suite provides the required automated network and application vulnerability scanning, configuration assessment, and network discovery. ACAS also generates reports and data with a centralized console and is security content automation protocol compliant.

- Burp Suite Pro: A software application with a suite of tools used to perform security testing of web applications. The integrated tools support the testing process in initial mapping, AS analysis, and vulnerability exploitation. It contains the following components: proxy interception (allows users to inspect and modify traffic between a browser and the target application), an application-aware "spider" used to crawl web content and functionality, a web application scanner for vulnerability detection automation, an intrusion tool that performs customized attacks, a tool used to manipulate and resend individual requests, and a sequence tool used to test random session tokens. Users can also use Burp Suite Pro to create customized plug-ins for penetration testing.

6.3 CONTINUOUS MONITORING

Continuous monitoring is the ongoing assessment of an organization's IT system to detect and respond to security threats. It helps identify changes in the environment, assess vulnerabilities, and ensure that security measures remain effective over time. With continuous monitoring, organizations can promptly address emerging threats, adapt to network changes, and maintain a proactive approach to cybersecurity. The following lists example DCO tools employed by ARCYBER for continuous monitoring:

- Security Onion (SO): An open-source network intrusion detection system (NIDS) and network security monitoring solution. The setup wizard allows operators to build an array of distributed sensors efficiently. It utilizes a rule-driven language, which combines the benefits of signature- and anomaly-based protocols. It provides a layer of defense that monitors network traffic for predefined, suspicious activity or patterns. Operators are alerted when suspicious traffic is detected. SO contains a domain-specific scripting language that enables site-specific monitoring policies. It is not restricted by detection type and does not rely on traditional signatures. Comprehensive logs are collected, and then an archive containing network activity is provided. It comes with analyzers for many protocols, enabling semantic analysis at the application layer. Additionally, it also contains an extensive application-layer state record about the network. SO interfaces with other applications for real-time data exchange.
- Wireshark: A software-based network packet analyzer that captures and displays network packets for troubleshooting issues with security; network protocol implementations; and any additional, pertinent network details. Tcpdump and WinDump are terminal-based applications that use command line scripts to analyze the network packet files. Wireshark imports packets from text files containing hexadecimal dumps of packet data. Additionally, it filters and displays packets with very detailed network protocol information using specific criteria.
- Endgame: (See description in Section 6.1.)

6.4 INTEL SUPPORT

Leveraging intelligence is often gathered through threat intelligence feeds or collaborative sharing to enhance the understanding of potential threats. This information helps organizations stay informed about the latest TTPs employed by cyberadversaries. Intel support enables proactive threat mitigation, allowing for the development of effective security strategies and the timely implementation of countermeasures to protect against evolving cyberthreats. Intel

support includes professional work involving the acquisition, receipt, evaluation and analysis, dissemination, and use of foreign intelligence and threat information having pertinence to research, combat and materiel developments, training and training developments, concepts, doctrine and doctrinal developments, T&E, readiness and sustainment, or employment of U.S. military forces and equipment. The following is an example DCO tool employed by ARCYBER for intel support:

- Emerging Threat Pro: A set of rules developed to detect and block advanced threats using existing network security appliances, such as next-generation firewalls and NIDS/intrusion prevention system. The firewall rules are updated daily. Additionally, Emerging Threat Pro covers more than 40 categories of network behaviors, such as malware command and control (C2), distributed denial of service attacks, botnets, exploits, vulnerabilities, supervisory control and data acquisition (SCADA) network protocols, and more.

6.5 MITIGATION/REMEDIATION

Mitigation involves taking actions to reduce or minimize the impact or severity of a security incident. Remediation refers to the process of resolving or fixing the root cause of a security issue after initial identification to contribute to an overall comprehensive cybersecurity strategy. The following lists example DCO tools employed by ARCYBER for mitigation/remediation:

- Sqrrl: A threat-hunting tool that enables organizations to target, hunt, and disrupt advanced cyberthreats. It combines link analysis, user and entity behavior analytics (UEBA), and multipetabyte scalable capabilities into an integrated solution. It reduces the time spent by an attacker in the system. Additionally, it enables effective threat hunting by detecting adversarial behavior faster and with fewer resources using machine learning (ML). As an incident response tool, Sqrrl enables operators to more efficiently investigate the scope, impact, and root cause of an incident.
- Red Seal: (See description in Section 6.1.)
- Endgame: (See description in Section 6.1.)

6.6 EVENT CORRELATION

Event correlation analyzes the relationship between various security events and alerts to identify patterns or connections that may indicate a potential security threat. It also helps security teams understand the context of individual events by linking them and providing a more comprehensive view of the security landscape. This allows cybersecurity organizations to detect complex attacks, reduce false positives within network traffic, and prioritize the severity of an incident, which leads to overall improvement in response time. The following lists example DCO tools employed by ARCYBER for event correlation:

- Splunk: A software application that collects and correlates data to identify potential problems in a network architecture and business procedures. It allows operators to collect and analyze data in a single pane, which enables data association from multiple data sources. Data ingestion is performed through unstructured data sources, such as log files. Splunk also ingests structured content from databases in real time. After data have been ingested, a comparison can identify potential issues that may not be diagnosed by analyzing log files from a single source.
- X Pack: An Elastic Stack extension that bundles security, alerting, monitoring, reporting, and graph capabilities into one manageable configuration package. The components are designed to work together seamlessly; however, a single operator can enable or disable the features as well.

- Elasticsearch, Logstash, and Kibana (ELK) Stack: An open-source software set of tools that provide real-time insights from a structured and unstructured data source. It makes searching and analyzing data easier. Elasticsearch provides the ability to move easily beyond a simple full-text search through its robust set of application program interfaces and query digital subscriber lines. Logstash retrieves data, such as logs and other time-based event data, from any system. It also scrubs the logs and parses all data sources into JavaScript Object Notation format. Logstash then stores it in a single place for additional transformation and processing. Kibana is a data visualization engine that allows the operator to interact with all data in Elasticsearch using custom dashboards.

6.7 PENETRATION TESTING

"Ethical Hacking" is a proactive cybersecurity practice involving identification and addressing vulnerabilities in a system or network. Penetration testing helps discover potential weaknesses in software, hardware, and networks. It provides insights into the severity and potential impact of vulnerabilities while prioritizing fixes. The assessment of effectiveness into existing security measures provides additional validation.

Penetration testing is a type of security testing where evaluators mimic real-world attacks to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability [35]. The following lists example DCO tools employed by ARCYBER for penetration testing:

- Burp Suite Pro: Allows operators to create customized plug-ins for penetration testing. (See additional details in Section 6.2.)
- Kali: An open-source software penetration testing, digital forensics, and security auditing Linux distribution. It is an operating system (OS) with over 600 testing tools, such as NMAP, John the Ripper, Wireshark, and Metasploit. It provides authorized users with the ability to scan selected systems, identify vulnerabilities, and exploit the identified vulnerabilities. Kali is capable of testing server and network vulnerabilities, performing web application assessments, and conducting social engineering.

6.8 THREAT EMULATION

Simulating real-world attacks evaluates an organization's overall security posture. Threat emulation (also referred to as adversary simulation) is an advanced form of testing where the attack TTPs utilized are based on documented, real-world criminal actions [36]. The difference between attack simulation and attack emulation is the word emulation means "to behave in the same way as someone else," while simulation means "to produce something that is not real but has the appearance of being real." When it comes to emulation vs. simulation in terms of cybersecurity, emulation duplicates while simulation replicates a real device. The purpose of both programs is to test a company's security and see how well it can defend against real-world attacks. Simply put, it is a rehearsal to measure an organization's security controls and posture. The following lists example DCO tools employed by ARCYBER for threat emulation:

- Kali: (See description in Section 6.7.)
- Cobalt Strike: A software tool used to assist Red teams with vulnerability assessments and cyberthreat emulation on networks. It includes a framework of tools used for multiple facets of cyberthreat emulation. Cobalt Strike

functionality includes, but is not limited to, reconnaissance, phishing, postexploitation, and reporting.

6.9 MALWARE ANALYSIS

Malware analysis is the process of dissecting and understanding malicious software to enhance threat detection, response, and oversecurity of the system [10]. Its role involves initial identification and detection; behavioral analysis for better understanding; impact assessment for potential risk and consequences; reverse engineering for code dissemination; understanding TTPs; containment of the malware to isolate infected systems; and, finally, postanalysis and reporting. The following lists example DCO tools employed by ARCYBER for forensics and malware analysis:

- IDA Pro: A software tool that combines an interactive, programmable, multiprocessor disassembler (application that explores binary programs with no available source code to create execution maps) coupled to a local and remote debugger and augmented by a complete plug-in programming environment. The debugger complements static analysis performed by the disassembler by allowing an operator to navigate malicious code. The debugger can bypass obfuscation and help obtain data that the more powerful static disassembler can then process more in-depth. IDA Pro can be used on multiple platforms, such as Windows and Linux.
- Encase Endpoint Investigator: A tool that performs remote, secure internal investigations without a disruption to day-to-day operations. Encase Endpoint Investigator is an effective tool for noninvasive scanning, searching, and data collection in an investigation.

6.10 ADDITIONAL ARCYBER DCO TOOLS

This section details additional ARCYBER DCO tools for the following: (1) C2, (2) the combination of Software Development and Operations (DevOps), and (3) Industrial Control Systems (ICS) and SCADA. These tools are not specifically linked to one of the cyber-T&E activities previously detailed in Sections 6.1–6.9.

6.10.1 C2

The following lists example DCO tools employed by ARCYBER for C2:

- Redmine: An open-source, web-based project management and issue tracking tool. It allows operators to manage multiple projects, such as project forums, time tracking, and role-based access control. Redmine also includes a calendar and Gantt charts to aid in visual representation of projects and deadlines.
- Mattermost Pro: An open-source, private-cloud chat-messing service for organizations. Mattermost Pro provides a virtual workspace for multiple projects, scalable to multiple operators.
- Nextcloud: A suite of client-server software for creating and utilizing file hosting services like Dropbox. Nextcloud is free and open source.

6.10.2 Software DevOps

The following lists example DCO tools employed by ARCYBER for Software DevOps:

- Confluence and Jira: Collaboration tools that provide operators the ability to create meeting notes, project plans, product requirements, and more using multimedia for dynamic content. While Confluence is designed for documentation, Jira allows project management and issue tracking.

- Atom: An open-source, web-based desktop application used to edit source code and text. It allows support for plug-ins written in Node.js and embedded Git control. It is based on Electron (formerly known as Atom Shell), a framework that enables cross-platform desktop applications using Chromium and Node.js. Atom is written in CoffeeScript and Less and can also be used as an integrated development environment.
- Git: An open-source, distributed version control system designed to efficiently handle small and very large projects. Git possesses ease of use with a small footprint to enable fast performance.
- PowerShell: A Microsoft task automation and configuration management framework, with a command line interface. The scripting language is built on the .NET Framework and .NET Core. PowerShell is now an open-source and cross-platform solution (initially a Windows component only).
- Python: A programming language with a syntax that expresses concepts in fewer lines of code than other languages. It supports object-oriented, functional programming, and procedural styles. Python features a dynamic system; automatic memory management; and a large, comprehensive, standard library.
- Ansible: An IT automation platform that makes applications and systems easier to deploy. Ansible allows operators to avoid writing scripts or custom code to deploy and update applications utilizing automation with no agents to install on remote systems.
- Docker: A software technology utilizing containerization. Containers are standalone, agile software packages that include all components needed to run an application. These components include, but are not limited to, source code, runtime, system library, and settings on a Windows or Linux OS.

6.10.3 ICS and SCADA

The following lists example DCO tools employed by ARCYBER for ICS and SCADA:

- GRASSMARLIN: Provides situational awareness for ICS and SCADA systems to maintain network security. GRASSMARLIN provides the ability to passively map and display an ICS or SCADA network topology while conducting device discovery, accounting, and reporting on mission-critical systems.

6.11 DCO CYBER-T&E ACTIVITY TOOLS SUMMARY

In summary, Table 6-1 shows all of the example DCO cyber-T&E tools employed by ARCYBER and the corresponding cyber-T&E activity aligned for reference.

Table 6-1. Example Tools for Each Cyber-T&E Activity

DCO Cyber-T&E Activity	Example DCO Tools Employed by ARCYBER
Discovery	Red Seal, Endgame, GRR, BlueScope, MySQL, Network Visualization Suite
VA	Red Seal, Nipper Studio, ACAS, Burp Suite Pro
Continuous Monitoring	SO, Wireshark, Endgame
Intel Support	Emerging Threat Pro
Mitigation/Remediation	Sqrrl, Red Seal, Endgame
Event Correlation	Splunk, X Pack, ELK
Penetration Testing	Burp Suite Pro, Kali
Threat Emulation	Kali, Cobalt Strike
Malware Analysis	IDA Pro, Encase Endpoint Investigator
C2	Redmine, Mattermost Pro, Nextcloud
DevOps	Confluence, Jira, Atom, Git, PowerShell, Python, Ansible, Docker
ICS and SCADA	GRASSMARLIN

This Page Intentionally Left Blank

07 DCO USE CASES

This section describes specific use cases detailing different cyber-T&E events conducted for PM DCO.

7.1 USE CASE #1: ICS AND SCADA SYSTEMS FOR DCO

DCO tools include the capability to protect and defend ICSs using the SCADA architecture [37]. SCADA systems specifically within the Army are used to monitor and control critical infrastructure, logistics, and defense systems. These systems manage operations in real time across a range of military applications, such as base infrastructure, utility management, and field operations, providing a centralized interface for operators to supervise large-scale automated processes. DCO includes planning and visualization software tools that generate, optimize, and verify different sequences of mechanical assembly using three-dimensional computer-aided-design models. The DCO tools and program also provide a user-friendly graphical user interface (GUI). Cyberdefenders operating the GUI have the capability to detect, monitor, and track anomalies with ICS and create a dynamic visualization of the SCADA architecture.

Specifically, Tenable.ot, SO, and Nozomi Networks were assessed during a DCO OT for their technical and functional capabilities, IAW the performance characteristics stated in the DCO Tool Requirements Definition Package. The ICS and SCADA system for the DCO program are designed to detect zero-day exploitations. Zero-day exploits target vulnerabilities that are not publicly known, rendering them difficult to detect using traditional security mechanisms. Tenable.ot, SO, and Nozomi Networks are ICS and SCADA software solutions that enable global DCO forces to monitor and track anomalies and enrich network packet information, among other capabilities. They also provide collaboration between IT and operational technology, which is critical to reducing the security gaps surrounding highly connected industrial control systems.

Nozomi Networks is the first software component used for DCO and provides visibility into operational technology by focusing on real-time monitoring, asset discovery, and anomaly detection essential for zero-day exploits. Nozomi Networks builds a behavioral baseline of normal operations across a human machine interface (HMI), programmable logic controller (PLC), and SCADA network by tracking normal communication patterns and activities. An HMI is the interface through which human operators interact with a control system, allowing operators to issue commands and monitor system performance in real time. HMIs can visualize data and processes, such as temperatures, pressure, and valve positions, in a power plant or a weapons system in the military. PLCs process input signals from sensors and execute logic or control instructions to operate machinery based on input. Output commands can control motors; valves; and other types of industrial automation, such as robotics, assembly lines, or process controls in utilities. During the Stuxnet malware attack in 2010, PLCs used in Iran's nuclear enrichment

programs were targeted and exploited. Specifically, the Siemens Step 7 PLC's logic was manipulated to cause damage to centrifuges while reporting normal operations to the HMI and delayed detection even further. This anomaly detection software can detect deviations from the normal baseline and command patterns between the HMI and PLCs, such as unexpected PLC reprogramming, described in the Stuxnet attack.

The second component is vulnerability management software used for DCO testing that manages weaknesses in ICS and operational technology environments, providing insight in the system's risk posture. The software discovers and assesses vulnerabilities in IT systems, including HMI and any connected devices that interface with the SCADA network. Risk scores based on known vulnerabilities and misconfigurations are provided for each asset to prioritize systems that are more likely to be targeted by a zero-day exploit. Misconfigurations in ICS and SCADA systems, such as open ports or weak credentials, can increase the AS for zero-day exploits and must be continuously monitored.

The third and final component is a platform for intrusion detection, network security monitoring, and log analysis. Use of these specific tools allows for deep packet inspection and anomaly detection, suspicious traffic patterns, and the close monitoring of communication protocols. These tools also watch for suspicious signatures or behavior, such as unexpected data flows between HMI and PLCs or unusual traffic from external sources, which can contribute to the detection of zero-day exploits. Host detection is an additional capability and log analysis. The solution aggregates and correlates logs from various sources and any unusual event patterns from the two preciously mentioned security tools. The combination of the three security components for DCO creates a comprehensive detection mechanism for zero-day exploitation in ICS and SCADA systems.

Members from the Cyber Protection team within ARCYBER in Fort Gordon, GA, served as operators for an assessment and user feedback on the effectiveness of these tools and operational utility. The testing environment consisted of a single HMI and multiple PLCs. Attack simulations were performed and captured in a network packet file to be examined. Remediation steps to enhance security posture included encryption, system hardening, access control mechanism, and network segmentation. The results of this event were proprietary. However, examples of attacks on ICS and SCADA systems within a military environment can include:

- Weapons Systems (e.g., artillery and missile systems): Where HMIs are used to monitor targeting data and weapon status, as well as control firing operations for real-time feedback to the operator.
- Infrastructure and Base Operations: Where automation of essential services (e.g., power generation and water supply) are controlled by PLCs.
- Air Defense Systems: Where operators use HMIs to track aerial threats and manage radar systems.
- Vehicles (like tanks): Where operators are provided with control over the vehicle's system.
- Unmanned Vehicles (e.g., ground or aerial drones): Where HMIs are used for remote control.
- Logistics and Supply Chain: Where PLCs control automation of the supply chain to manage inventory and equipment status.

Upon completion of the OT, an assessment report was provided to all stakeholders to support a fielding decision.

7.2 USE CASE #2: CYBERSECURITY VULNERABILITY AND PENETRATION TESTING FOR DCO

The CVPA is designed to identify confirmed cybervulnerabilities and potential cyber-attack vectors" [3]. A CVPA was executed by the CCDC DAC on a tactical software program within the DCO program [38]. The DOT&E published the "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs," dated 3 April 2018 [39]. This assessment was conducted IAW those guidelines. DAC conducted a CVPA of the tactical system in support of PEO C3T and ATEC, serving as the OTA. During the assessment, cybersecurity and resiliency of the systems were characterized in operational-representative context and provided reconnaissance of the SUT in support of an AA. "The data results were disseminated among stakeholders to implement mitigations to improve resiliency. The assessment was conducted in a cooperative manner between the SUT technical team, network defenders/ operators, and DAC, as applicable.

The TDI capabilities eradicate advanced cyberspace threats and vulnerabilities. Operators are provided with the ability to automate deployment of DCO tools on tactical hardware. The TDI can be accessed by local cyberdefenders and remotely by cyberprotection teams augmenting the local defender staff.

Results of the CVPA are considered proprietary. However, the following cybersecurity task and activities are typical during a CVPA. During the Reconnaissance phase, network discovery is performed by running vulnerability scans and network traffic is captured and analyzed. The Penetration phase confirms whether the vulnerabilities identified during Reconnaissance are exploited from three postures:

1. Near-Sider: An adversary that has gained physical or logical access to the target system without granted credentials.
2. Insider: An adversary with legitimate access to a target system.
3. Outsider: An adversary without legitimate physical or logical access to the target system.

Based on the functionality and configuration of the SUT, only near-sider and insider were tested during this event. The objective is to compromise mission-critical operations and degrade the target system's performance and impact to confidentiality, integrity, and availability. At the final phase, a physical inspection for tampering on the SUT is performed and personnel interviews are conducted to identify any additional strengths and weaknesses. DAC provides a daily status meeting in addition to an emerging results brief on the final day of testing. An assessment results matrix is distributed within 30 days of the event to appropriate stakeholders.

7.3 USE CASE #3: USER ACTIVITY MONITORING FOR DCO

The User Activity Monitoring Cloud software (UAM-C) is a cloud-based solution that was evaluated by ATEC system's team in 2020. UAM-C consists of an endpoint collection tool (EPCT) and UEBA tool within Gabriel Nimbus (GN). GN is the Army's segment of the Big Data Platform. UAM-C leverages ML on GN to analyze user data while detecting malicious insider threats and calculating system behavior, such as policy violations within a classified environment. Specific test cases performed during the event included:

- Event Data Monitoring: Continuous monitoring ensures data, ingestion, collection, and retention within GN using the UEBA and EPCT.
- Monitoring Windows Activity by Terminated Accounts: User activity by terminated employees could indicate possible misuse or an operational gap in the decommission process. A security policy details UAM-C's ability to

detect an inactive status on a Windows account tied to a successful logon event code.

- Abnormal Network Access: A spike in the number of occurrences that access new network objects could indicate snooping or reconnaissance activity. UAM-C detects activity from established baselines within a specific window.
- Excessive Login Failures: An abnormal occurrence of login failures could indicate infiltration of a user account. UAM-C monitors specific event codes for this activity, with further investigation for users with incorrect login types.
- Privilege Escalation: User activity escalates privilege on a local account.
- Registry Key Modification: Registry edit attempts may indicate malicious activity on the endpoint. Increased usage of the registry edit command is monitored compared to the established baseline.
- Beaconing: A traffic beacon to malicious sites could indicate communication with a C2 server. UAM-C can act as a traffic analyzer to perform specific checks against proxy traffic to detect anomalous domains and user agents and domains generated by algorithms.
- Data Exfiltration: Uploads greater than or equal to 1 MB to storage sites may indicate data exfiltration.
- Suspicious File Activity: Accounts with no interaction to any valid user data ingested can be detected using UAM-C.

The UAM-C solution addresses the mission need to detect and deny malicious activity of trusted insiders with access to classified information. It provides operators with a common picture of an insider threat risk profile across the network and overall organization.

08 CONCLUSIONS

The rate at which malicious cybertools are being created is alarming, and keeping critical networks from becoming compromised is a crucial challenge as new cyberthreats are developed. Different organizations within the Army are providing support by using their capabilities to help the military gain an advantage in cyberspace operations. These organizations include ATEC, ARCYBER, and CCDC. To meet the growing demand for innovative solutions in cyberspace operations, the Army collaborates with industry, academia, and government entities.

The Army uses acquisition strategies to build new cybertools in an efficient manner, employing rapid and flexible development projects. The DSCS and the DCO acquisition strategies ensure that cybersecurity software and hardware can be created in an efficient manner while staying compliant with Army regulations. Additionally, the SAMP establishes guidelines that new cybersoftware and hardware products can follow to ensure proper integration into existing systems. Throughout the development life cycle, testing will be conducted on new systems to determine the maturity of the technology and help dictate deployment decisions.

Tracking notable cyber-T&E activities during the acquisition process is also crucial to the development process. For DCO, the Army focuses on the following activities: discovery, VA, continuous monitoring, intel support, mitigation/ remediation, event correlation, penetration testing, threat emulation, and malware analysis. DCO follows specific T&E based on DoDI 5000.89 [10], which helps shape the design, planning, and execution of new cybersecurity systems. With current acquisition processes, the Army will continue to pursue its mission to develop resilient cybersecurity technology to secure military networks and systems.

This Page Intentionally Left Blank

REFERENCES

1. Office of the Under Secretary of Defense for Research and Engineering, Office of the Director, Operational Test and Evaluation. *Test and Evaluation Enterprise Guidebook*. OSD T&E-GB-08.02, Washington, DC, https://www.test-evaluation.osd.mil/Portals/120/Documents/TE%20Enterprise%20Guidebook/TE%20Enterprise%20Guidebook%208.02.pdf?ver=uqBTY9tLbZTH1oSOQgRmUg%3D%3D, 19 August 2022.
2. U.S. Department of Defense. *Cybersecurity Test and Evaluation Guidebook*. Version 2.0, Change 1, Washington, DC, https://www.dau.edu/sites/default/files/Migrated/CopDocuments/Cybersecurity-Test-and-Evaluation-Guidebook-Version2-change-1.pdf, 10 February 2020.
3. U.S. Army. "ATEC: U.S. Army Test and Evaluation Command." https://www.atec.army.mil/index.html, accessed on 15 November 2024.
4. U.S. Army. "EPG: U.S. Army Electronic Proving Ground." https://www.atec.army.mil/epg/index.html, accessed on 15 November 2024.
5. U.S. Army Cyber Command. "ARCYBER Homepage." https://www.arcyber.army.mil/, accessed on 18 November 2024.
6. U.S. Army. "DEVCOM Analysis Center." https://www.army.mil/DAC, accessed on 18 November 2024.
7. Army Cyber Institute. "Army Cyber Institute at West Point." https://cyber.army.mil/, accessed on 15 November 2024.
8. U.S. Army Cyber Center of Excellence. "U.S. Army Cyber Center of Excellence (CCoE) Homepage." https://cybercoe.army.mil/Home/Schools/Cyber-School/, accessed on 18 November 2024.
9. Program Executive Office Intelligence, Electronic Warfare, & Sensors. "PM DCO." PEO IEW&S, https://peoiews.army.mil/pm-dco/, accessed on 18 November 2024.
10. Office of the Under Secretary of Defense for Research and Engineering, Office of the Director, Operational Test and Evaluation. "Test and Evaluation." DoDI 5000.89 Washington, DC, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500089p.PDF, 19 November 2020.
11. Office of the U.S. Department of Defense Chief Information Officer. "Cyberspace Workforce Management." DoDD 8140.01, Washington, DC, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001p.pdf, 5 October 2020.
12. Office of the U.S. Department of Defense Chief Information Officer. "DoD Cyber Red Teams." DoDI 8585.01, Washington, DC, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/858501p.pdf?ver=0J4GT4-ji4H0Dd7mOa173w%3D%3D, 11 January 2024.
13. Office of the Under Secretary of Defense for Acquisition and Sustainment. "Defense-Wide Sharing and Use of Supplier and Product Performance Information (PI)." DoDI 5000.79, Washington, DC, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500079p.PDF, 15 October 2019.
14. Office of the U.S. Department of Defense Chief Information Officer. "Vulnerability Management." DoDI 8531.01, Washington, DC, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853101p.pdf, 15 September 2020.
15. Office of the U.S. Department of Defense Chief Information Officer. "Cybersecurity." DoDI 8500.01, Version 2.0, Change 1, Washington, DC, https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/850001_2014.pdf, 7 October 2019.
16. Office of the U.S. Department of Defense Chief Information Officer. "Risk Management Framework for DoD Systems." DoDI 8510.01, Washington, DC, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf, 19 July 2022.
17. Headquarters, Department of the Army. "Army Cybersecurity." AR 25-2, Washington, DC, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN37506-AR_25-2-003-WEB-4.pdf, 4 April 2019.
18. National Institute of Standards and Technology. "Security and Privacy Controls for Information Systems and Organizations." NIST SP 800-53, Revision 5, U.S. Department of Commerce, Washington, DC, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf, September 2020.
19. National Institute of Standards and Technology. "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy." NIST SP 800-37, Revision 2, U.S. Department of Commerce, Washington, DC, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf, December 2018.
20. Committee on National Security Systems. "Security Categorization and Control Selection for National Security Systems." CNSSI No. 1253, National Security Agency, Fort Meade, MD, https://www.dcsa.mil/portals/91/documents/ctp/nao/CNSSI_No1253.pdf, 27 March 2014.

REFERENCES, *continued*

21. Defense Acquisition University. "Critical Operational Issue." DAU, https://www.dau.edu/glossary/critical-operational-issue, accessed on 15 November 2024.
22. U.S. Department of Defense. "Section 04: Test Types." *DT&E Program: Defensive Cyber Operations Single Acquisition Management Plan*, version 1.8, Washington, DC, 12 July 2018.
23. Office of the Law Revision Counsel of the U.S. House of Representatives. "Operational Test and Evaluation for Defense Acquisition Programs." 10 U.S.C. § 4171, U.S. Government Publishing Office, Washington, DC, https://uscode.house.gov/view.xhtml?req=10+USC+4171&f=treesort&fq=true&num=7&hl=true&edition=prelim&granuleId=USC-prelim-title10-section4171, 2018.
24. Office of the Law Revision Counsel of the U.S. House of Representatives. "Major Systems and Munitions Programs: Survivability Testing and Lethality Testing Required Before Full-Scale Production." 10 U.S.C. § 4172, U.S. Government Publishing Office, Washington, DC, https://uscode.house.gov/view.xhtml?hl=false&edition=prelim&req=granuleid%3AUSC-prelim-title10-section4172&f=treesort&fq=true&num=0&saved=%7CMTAgVVNDIDQxNzE%3D%7CdHJlZXNvcnQ%3D%7CdHJ1ZQ%3D%3D%7C7%7Ctrue%7Cprelim, 2021.
25. Schmidt, R. F. "Software Requirements Analysis Practice." *Software Engineering: Architecture-Driven Software Development*, ch. 8, pp. 139–158, Cambridge, MA: Elsevier, https://www.sciencedirect.com/science/article/abs/pii/B9780124077683000082, 30 April 2013.
26. Defense Acquisition University. "Test Types." DAU, https://www.dau.edu/acquipedia-article/developmental-test-and-evaluation-dte#:~:text=The%20difference%20between%20DT%26E%20and,is%20a%20realistic%20operational%20environment, accessed on 18 November 2024.
27. Office of the Under Secretary of Defense for Research and Engineering. "Cyber Developmental Test and Evaluation." DoDM 5000.UY, unpublished draft, Washington, DC, 2024.
28. Office of the Under Secretary of Defense for Acquisition and Sustainment. "Operation of the Adaptive Acquisition Framework." DoDI 5000.02, Washington, DC, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.pdf?ver=2020-01-23-144114-093, 23 January 2020.
29. U.S. Department of Defense. "DCO Cyber T&E Activities." *Defensive Cyber Operations Single Acquisition Management Plan*, version 1.8, Washington, DC, 12 July 2018.
30. Program Executive Office—Intelligence, Electronic Warfare, and Sensors. "PM DCO: Garrison Defensive Cyberspace Operations Platform." PEO IEW&S, https://peoiews.army.mil/wp-content/uploads/2023/10/GDP.png, accessed on 15 November 2024.
31. Program Executive Office—Intelligence, Electronic Warfare, and Sensors. "PM DCO: Deployable Defensive Cyberspace Operations System." PEO IEW&S, https://peoiews.army.mil/wp-content/uploads/2023/10/DDS.png, accessed on 15 November 2024.
32. World Wide Web Consortium Working Group. "Web Services Glossary: Discovery." W3C, https://www.w3.org/TR/ws-gloss/, accessed on 18 November 2024.
33. National Institute of Standards and Technology. "Glossary: Discovery." NIST, https://csrc.nist.gov/glossary/term/discovery, accessed on 18 December 2024.
34. National Institute of Standards and Technology. "Glossary: Vulnerability Analysis." NIST, https://csrc.nist.gov/glossary/term/vulnerability_analysis, accessed on 18 November 2024.
35. National Institute of Standards and Technology. "Technical Guide to Information Security Testing and Assessment." NIST SP 800-115, Section 5.2, U.S. Department of Commerce, Washington, DC, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf, September 2008.
36. Goodwin, S. D. "Threat Emulation vs. Penetration Testing: Understanding the Differences." Wolf & Company, P.C., https://www.wolfandco.com/resources/insights/threat-emulation-penetration-testing-understanding-differences/, accessed on 18 November 2024.
37. U.S. Army Evaluation Center, Survivability Evaluation Directorate. "Use Case #1." Aberdeen Proving Ground, MD, April 2023.
38. U.S. Army Combat Capabilities Development Command Data Analysis Center, Cybersecurity Experimentation and Analysis Division. "Use Case #2." White Sands Missile Range, NM, September 2022.
39. Office of the Secretary of Defense. "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs." Memorandum, Director of Operational Test and Evaluation, Washington, DC, https://www.dote.osd.mil/Portals/97/pub/policies/2018/20180403ProcsForOTEofCybersecurityInAcqProgs(17092).pdf, 3 April 2018.

BIBLIOGRAPHY

Defense Acquisition University. "Cyber DT&E." DAU, https://www.dau.edu/sites/default/files/2024-02/Cyber%20DT%26E%20Webinar%20Q%26A.pdf, accessed on 18 November 2024.

Deloitte Touche Tohmatsu Limited. "Cyber 101." Deloitte, https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-july2017.pdf, July 2017.

National Institute of Standards and Technology. "Security Requirements for Cryptographic Modules." FIPS PUB 140-3, Gaithersburg, MD, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf, 22 March 2019.

U.S. Air Force. "Air Force Operational Test and Evaluation Center." https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104538/air-force-operational-test-and-evaluation-center/, accessed on 18 November 2024.

CYBERTEST AND EVALUATION OF DEFENSIVE CYBEROPERATIONS IN THE U.S. ARMY

Tiffany Williams, Matt Friar, Olutoye Sekiteri, and Philip Payne

CSIAC-BCO-2024-617