Cyber Survivability Test and Evaluation Handbook

Version 4.0

24 OCT 2025

COSTELLO.EUGENE.D.1016366478

Digitally signed by COSTELLO.EUGENE.D.1016366478
Date: 2025.10.24 11:07:29 -04'00'

RECORD OF REVISIONS

Number of Change	Summary of Changes	Updated
1	This is the initial Cyber Survivability Test and Evaluation Handbook	26 MAY 20
2	Effective change to Checkpoint 1 requirements, elimination of Checkpoint 4, clarification of PPP analysis, reemphasis of CRM utilization, and clarification of CP2 delivery methods.	18 NOV 21
3	Content updated to for IEF and TEMP inputs, test planning lessons learned, scheduling and alignment with changes to higher policies and handbooks.	06 DEC 22
4	Added Post-Test Section, Business Rules, and updating language and references	24 OCT 25

Cyber Survivability Test and Evaluation Handbook

TABLE OF CONTENTS

TABLES

FIGURES

SECTION 1 - CYBER SURVIVABILITY

1.1 - INTRODUCTION

The purpose of the Operational Test and Evaluation Force (OPTEVFOR) Cyber Survivability (CS) evaluation is to determine each system's capability to survive and operate after exposure to cyber threats, which attempt to prevent completing operational mission(s) by destruction, corruption, denial, or exposure of data transmitted, received, processed, or stored.

In the role as OPTEVFOR's cyber competency, the 01D cybersecurity division supports all aspects of the cybersecurity Operational Test and Evaluation (OT&E) across all OPTEVFOR Warfare Divisions (WD) including VXs, VMX-1, and HMX-1. 01D leadership is comprised of the Director, Deputy Director, Operations Officer, Red Team Chief, and Systems Management Lead.

This handbook is a complement to OPTEVFOR test planning, execution, and reporting handbooks. It was created to assist the OPTEVFOR military, government civilian, and support contractor teams navigate through the cyber survivability evaluation methodology. This methodology defines a repeatable process for planning, executing, and reporting an evaluation of the System Under Test's (SUT) capabilities to Prevent, Mitigate, Recover, and Adapt (PMRA) in a cyber contested environment. When followed, this methodology provides the warfighter and acquisition stakeholders a solid understanding of the limitations and risks to the operational mission supported by the SUT.

The OPTEVFOR process for preparing cyber survivability test plans and reports is influenced by the complexity of acquisition programs. Consequently, test teams must tailor the approach to the needs of each program, working in collaboration with program offices, WD leadership, and OPTEVFOR competencies.

1.2 - POLICIES AND GUIDANCE

The requirement for OPTEVFOR to conduct cyber OT&E is derived from the following policies and guidance:

- OPTEVFOR INSTRUCTION 3980.2 (series), Navy OT&E Manual
- OPTEVFOR N00 Memo, *Direction to Establish and Maintain a Department of Defense Certified Red Team Capability to Support the Navy Operational Test and Evaluation Mission*, 28 March 2019
- Department of Defense (DoD) Cybersecurity Test & Evaluation Guidebook v2.0, February 2020
- DoD Cyber Operational Test and Evaluation Guidebook, February 2025
- Cyber Survivability Endorsement Implementation Guide, July 2022
- DoD Instruction (DoDI) 5000.02 (series), *Operation of the Adaptive Acquisition Framework* January 2020
- SECNAVINST 5000.2G *Department of the Navy Implementation of the Defense Acquisition System and the Adaptive Acquisition Framework* April 2022

This handbook implements DoD and Department of the Navy (DON) guidance and policies for cybersecurity OT&E. The following subsections describe policies and guidance that directly affect cyber OT&E execution.

1.2.1 - OPTEVFOR INSTRUCTION 3980.2 (series), Navy OT&E Manual

OPTEVFOR INSTRUCTION 3980.2 (series) identifies the role of OT&E in connection with the acquisition and procurement of naval weapons and warfare support systems. It prescribes policies for the planning, executing, and reporting of OT&E concerning new and improved systems. It provides policy and high-level guidance. Other documents, such as handbooks and best practices, provide the details of "how-to." Where appropriate, this manual links to those documents.

1.2.2 - OPTEVFOR Red Team (OPTEV-RT) Memo, 28 March 2019

OPTEVFOR N00 memo, Direction to Establish and Maintain a Department of Defense Certified Red Team Capability to Support the Navy Operational Test and Evaluation Mission, 28 March 2019 directs the OPTEVFOR Cyber OT&E Division, Code 01D, to establish and maintain a National Security Agency (NSA) certified red team. The memo designates 01D as the responsible division to coordinate execution resources to ensure OPTEVFOR follows DoD and DON policies and processes for red team operations. This memo will hereafter be referred to as the OPTEVFOR Red Team memo.

1.2.3 - DoD Cybersecurity Test and Evaluation (T&E) Guidebook v2.0, Change 1, February 2020

DoD Cybersecurity Test and Evaluation (T&E) guidebook promotes data-driven, mission-impact based analysis and assessment methods for cybersecurity T&E. It guides the assessment of cyber survivability, and resilience within a mission context by encouraging planning for tighter integration of traditional system T&E. This guidebook details a six-phase approach to conducting cyber T&E. Phases one through four are Developmental Testing (DT) led periods; phases five and six are Operational Test (OT) led periods comprised of a Cooperative Vulnerability and Penetration Assessment (CVPA) and an Adversarial Assessment (AA).

1.2.4 - DoD Cyber Operational Test and Evaluation Guidebook, February 2025

The Cyber Operational Test and Evaluation Guidebook amplifies the policies outlined in DoDI 5000.98 and DoD Manual (DoDM) 5000.99 with key guidance for details and procedures. It outlines the necessary cyber testing to inform evaluations of operational effectiveness, suitability, and survivability of systems under test (SUTs) and underscores the importance of operational test and evaluation (OT&E) in assessing a system's survivability and its capacity to prevent, mitigate, recover from, and adapt to adverse cyber-events. This guidebook supersedes, incorporates, and expands on guidance found within the rescinded Director of Operational Test and Evaluation (DOT&E) Memoranda "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs" (April 3, 2018) and "Cyber Economic Vulnerability Assessments," (January 21, 2015) and will serve as interim guidance until the release of the forthcoming joint developmental test and evaluation (DT&E) and OT&E guidance.

This guidebook's appendices include guidance and checklists designed for Operational Test Agencies (OTAs) and Operational Test Organizations (OTOs) to use in the planning of cyber T&E events. These appendices cover the following:

- Pre-OT considerations
- Cyber content of OT plans
- Cooperative vulnerability and penetration assessment (CVPA) data requirements
- Adversarial assessment (AA) data requirements
- Cyber economic vulnerability assessment (CEVA) requirements

1.2.5 - Cyber Survivability Endorsement Implementation Guide (CSEIG), July 2022

The CSEIG took the defined Joint Capabilities Integration and Development System (JCIDS) Manual system survivability key performance parameter pillars of susceptibility, vulnerability, and resiliency and transformed them into prevent, mitigate, recover, and adapt pillars, respectively. Those cyber survivability pillars became the PMRA construct for OPTEVFOR's cyber survivability evaluation. The CSEIG defines Cyber Survivability Attributes (CSAs) that are traced back to the PMRA pillars defined below:

- **Prevent** – Design requirements to identify, protect and harden weapon system's functions from adversary cybersecurity threats.
- **Mitigate** - Design requirements to detect and respond to cyber-events making it through defenses; enabling cyber operational resiliency.
- **Recover** - Design requirements to recover to a known good condition after a cyber-event; at a minimum, restore sufficient capability to complete the mission.
- **Adapt** – Enables a sustained capability to adapt to changes in adversary threat and vulnerabilities through processes such as DevOps. 01D does not anticipate the adapt pillar to impact our test execution.

The intent of the CSAs is to assist in the development of cyber survivability requirements that are testable and measurable. The CSEIG contributed to the development of the OPTEVFOR cyber survivability process because (1) it derives its authority from the JCIDS process, and (2) the guide captures a process for characterizing how a system can sustain non-kinetic "hits" and how they impact the system's mission. It is operationally relevant for warfighters to understand the capabilities and limitations of their system within a cyber-contested environment. This can be accomplished with or without defined CSAs. However, if a system does have CSAs, they shall be included as part of the evaluation to determine if a system meets its requirements.

1.2.6 - DoDI 5000.02, Operation of the Adaptive Acquisition Framework, 23 January 2020

DoDI 5000.02 describes the integration of cybersecurity T&E into the acquisition structure and through the system lifecycle. It further clarifies the roles of OPTEVFOR and DOT&E and the performance of both CVPA and AA.

1.3 - DETERMINATION OF CYBER OT&E SCOPE

The WD, with 01D support, will determine what level of cyber survivability OT&E must be conducted for each phase of test to meet policy and stakeholder requirements. OPTEVFOR director has final authority on all determinations.

1.3.1 - When Cyber OT&E is Required

Per DoDI 5000.89, cyber survivability OT&E is required for all US Navy acquisition programs that receive, process, transmit, store, or display digital data. Each WD is expected to engage the necessary stakeholders and policyholders to ensure the scope of test planning and test execution meets the WD's objectives and reporting requirements.

1.3.2 - Establishing an Adequate Scope of Test

Determining an acceptable level of cyber survivability OT&E is dependent on many factors that influence the overall resource requirements and scope of test. The level of acceptable testing for each phase of test is tailorable to the specific circumstances of the program. Testing scope may range from a full PMRA capabilities evaluation to a limited risk assessment depending on stakeholder priorities, resource constraints, and cyber survivability capabilities inherent to each phase of test for that program. To ensure adequate testing is conducted to meet stakeholder requirements, the following considerations are provided to stimulate discussion:

- Has cyber survivability OT&E been done? If OT has been done:
  - Has the Program Management Office (PMO) made any changes to the system to correct the identified deficiencies?
  - Have changes been made since the last cyber test that have introduced any new attack paths?
  - Have new cyber threats been identified since the last OT period?

If all questions are answered "No," but cyber survivability OT&E has been done before, then re-testing the system may not be necessary. If the system was evaluated as "Not Cyber Survivable", the result carries forward.

For programs with no previous cyber survivability OT&E, full IOT&E planning and execution is required. To assist in determination of scope consider, and be prepared to answer the following questions:

- What non-IP based attack surfaces will be a part of OT?
- Is a remote assessment in scope?
- Is there an expectation to attack System of Systems (SoS) components? If yes, describe.
- Is there an expectation to plug into SoS components? If yes, describe.
- Is there an expectation to observe mission impacts on SoS components? If yes, describe.
- Is the SUT geographically dispersed? E.g., separate rooms, buildings, or bases. If yes, describe.
- Is it desired for the test team to spoof, modify, or replay custom/proprietary messages?
- Is it desired for the test team to impact the SUT's mission in a specific way?
- Is it desired for the test team to test specific prevent, mitigate, and recover capabilities of the SUT?

- What classification level will the SUT/SoS be tested at, and what is the expected classification level of results?

Other items to consider are:

- For TS/SCI systems it is essential to understand who the authorizing official is and have ongoing communications with them. The OPTEV-RT is authorized to conduct testing on Navy TS systems, but not on National Security Administration TS systems, requiring external efforts.
- For programs involving Naval Nuclear Propulsion systems NAVSEA 08K must be involved in the test planning process from the beginning.
- For applications hosted within an environment that has had cyber survivability OT&E conducted, and the hosted application does not open new attack vectors, consider not testing the application and focusing on a reduced-scope evaluation of program protection.
- For systems identified as "agile", consider establishing the cyber survivability baseline on the first fielded configuration (i.e., full cyber survivability Initial Operational Test and Evaluation (IOT&E) effort), then conducting follow-on cyber survivability OT&E periods based on the scope of system and threat changes. DT should be conducting cybersecurity T&E phase 3 and 4 events on interim configurations and providing results to OPTEVFOR for situational awareness.
- For an Operational Assessment (OA), consider limiting cyber survivability execution to a vulnerability discovery period. The focus of this period will be identifying, validating, and documenting system deficiencies in the configuration evaluated during an Early Operational Assessment (EOA) or OA. If the SUT is in a state that precludes testing (e.g., system is incomplete, or system architecture will radically differ from OT&E configuration), consider requesting the PMO to lead a Cyber Table Top (CTT) with OPTEVFOR participation to identify and document potential risks within the system design that can be corrected prior to OT&E. However, it should be noted that CTT events are not OT events and should not be planned/executed in lieu of actual testing.
- For a Quick Reaction Assessment (QRA), engage the program resource sponsor early and attempt to include cyber survivability requirements in the QRA tasking letter. If the letter does not address cyber, DO NOT assume it does not apply. Contact the sponsor to clarify cyber survivability requirements pertinent to the QRA letter. QRA execution requirements should be streamlined, concise, cost effective and based on the resource sponsor's priorities. Consider executing a tailored CVPA to meet the QRA requirements and report on system deficiencies to prevent cyber-attacks.
- Operationally relevant cyber DT assists and CTT events are encouraged and can potentially reduce the scope of OT requirements. This is part of the overall OT strategy determination and shall be coordinated with all stakeholders including 01D.
- If there are external barriers to an adequate cyber evaluation, the WD and 01D will work together to establish a strategy to satisfy OPTEVFOR's test requirements prior to external coordination. Alternate courses of action may be available to meet test adequacy requirements while accommodating resource constraints through proper coordination

with 01D, the program resource sponsor, PMO, DOT&E (if oversight), and operational stakeholder commands.

- Ensure scheduling is completed in sufficient time to support test execution. See section 5.4 for further details regarding scheduling.

The above list of considerations is not exhaustive. Each program will have distinct aspects that require critical thinking to address stakeholder requirements to design and execute an adequate test. 01D is a major stakeholder in these decision-making processes and associated discussions to ensure the agreed upon strategy is adequate and executable by the OPTEV-RT.

SECTION 2 - CYBER MODELING AND SIMULATION (M&S)

Due to scheduling, safety, Fleet asset availability, or other uncontrollable factors, it is not always possible to conduct a fully scoped cyber test in the operational environment. If, after all options to schedule and conduct testing in the operational environment have been exhausted, it may be appropriate to evaluate the cyber survivability of the SUT using non-operational test assets (cyber M&S).

If cyber M&S is supporting a program's cyber OT&E strategy, the intended use and the data necessary to support OPTEVFOR's accreditation of the M&S should be captured during cyber survivability test planning. This can start as early as the development of a system's Integrated Evaluation Framework (IEF) and Test and Evaluation Master Plan (TEMP). The use and accreditation of M&S in support of Navy OT&E is governed by OPTEVFORINST 5000.1 (series), *Use of Modeling and Simulation in Operational Test*.

The need to adjust a test strategy to include cyber M&S may occur right before, or during, cyber test planning and after a program's non-cyber M&S strategy has been formally documented. In that case, a program will not be required to edit/create separate cyber M&S documentation. The cyber test planning process will serve as the vehicle to ensure the necessary stakeholder engagement and documentation is produced within the program's test plan. In any case where cyber M&S is used, there will be an OPTEVFOR accreditation decision made after the testing is complete but prior to the final report signature.

2.1 - RISKS ASSOCIATED WITH THE USE OF M&S

There are three primary risks of using cyber M&S as part of the OT&E strategy:

- Identifying system vulnerabilities that are only present within the modeled environment (i.e., a "false-positive"). False-positive findings lead to setbacks—resources are unnecessarily expended on validating them, and they create challenges for follow-on testing in the operational environment by representing incorrect initial information.
- Not discovering vulnerabilities that exist in the operational environment (i.e., a "false-negative"). If no follow-on testing activities are planned then a system vulnerability will go undocumented; if follow-on testing is conducted, the discovery of a "new" system vulnerability will cause additional test resource expenditures to validate the vulnerability and to develop test objectives.
- Schedule / cost risk associated with validating findings from M&S based testing in the operational environment. For example, assume the CVPA will be conducted in a lab and the AA will be conducted on the Fleet asset. Since there are always deltas between a lab and the operational environment, the team will expend additional time during the AA validating the CVPA results before proceeding with the AA test events. This will likely extend the AA and cause cost and schedule risk.

To mitigate these risks, it is critical for the Operational Test Director (OTD) to collaborate with cyber M&S stakeholders to:

- Establish the intended use of cyber M&S to support OT&E
- Determine the operational representation of the simulated or laboratory environment for OT data collection requirements

The effort to evaluate the M&S environment for the intended use should be completed by the Checkpoint (CP) -3 test planning milestone. All M&S environments must be accredited before declaration of end of test.

2.2 - USE OF CYBER M&S

Cyber survivability testing shall be conducted in an operationally representative environment that includes the system operators and technicians. The OTD and cyber test planner shall make every reasonable effort to test in the operational environment before considering the use of cyber M&S. Reasons to consider cyber M&S include:

- Risk to human life
- Irrecoverable equipment damage that would render the test unit incapable of meeting operational commitments
- Decertification
- Unmitigated operational security concerns
- Asset availability

M&S intended use is formalized in an M&S Requirements Letter signed by the WD A-Code. The requirements letter specifies how cyber M&S supports a program's cyber OT&E requirements and captures how the data collected will support the overall evaluation.

2.2.1 - Supplementing Use

If cyber M&S is supplementing cyber OT&E, then the intended use could be to conduct a risk reduction event to assess the test team's Tactics, Techniques, and Procedures (TTP) to ensure no adverse effect on the system. Additionally, supplementing use could enable vulnerability discovery to support execution of CVPA and AA in the operational environment.

2.2.2 - Substituting Use

If cyber M&S is substituted for cyber testing in the operational environment, then the intended use would be to discover vulnerabilities that impact a system's capability to support a mission. This approach introduces a significant amount of risk to test adequacy. The evaluation of a system's PMRA capabilities includes assessing how well system operators and technicians can maintain and recover lost mission capabilities in a cyber-contested environment. Lab and cyber range testing introduce artificiality that make it very difficult to ensure the human responses are authentic within a cyber M&S environment. Therefore, it may not be possible to evaluate a system's PMRA capabilities or make a cyber survivability determination.

The OTD shall consult with 01D on the use of cyber M&S during the test strategy development to ensure test adequacy prior to committing to the use of any cyber M&S. 01B is the lead competency division for M&S within OPTEVFOR and may be a further resource to the WD to determine the

viability of M&S as part of a program's cyber OT&E strategy. For oversight programs, DOT&E concurrence is also required for cyber M&S use.

2.3 - CYBER M&S ACCEPTABILITY

The key to effective use of cyber M&S in OT&E is understanding the differences between the M&S configuration / environment and the operational, fielded system. A program may use M&S to support both cyber and non-cyber aspects of the test program. Cyber M&S does not require a separate accreditation plan. The acceptability of cyber M&S hinges on the "width" of deltas between the cyber M&S configuration/environment and the fielded system; if the deltas are too wide, then the cyber test objectives may not be supportable. This comparison will identify differences in the following:

- System software versions (both operating environment and tactical applications)
- Commercial off-the-shelf (COTS) and Government off-the-shelf hardware versions
- System component-to-component interfaces or network topology
- SUT to SoS interfaces and data flows
- SUT internal data flows
- Program protection features (as applicable)

The PMO will provide a Verification and Validation (V&V) plan and report for the deltas above. At a minimum, the V&V report shall contain the following:

- A table showing all hardware, software, and interface components of the system in rows with the columns detailing the deltas between the modeled environment and fielded system
- A description of components of the fielded system that are not within the modeled environment and the associated impacts to the SUT's performance/behavior
- A description of simulated devices, interfaces, and data flows within the system boundary and between the SUT/SoS boundary — each item noted should include the associated impacts to the SUT's performance/behavior
- Whether or not program protection features are enabled in the modeled environment
- Program Manager (PM) recommendation to use the M&S to support cyber OT&E

2.4 - CYBER M&S ACCREDITATION

An accreditation recommendation will be made in accordance with OPTEVFORINST 5000.1(series), *Use of Modeling and Simulation in Operational Test*.

The accreditation letter (signed by OPTEVFOR) documents the M&S accreditation determination (i.e., fully accredited, accredited with limitation, not accredited).

2.5 - CYBER M&S TEST LIMITATIONS

Use of cyber M&S requires a test limitation to be included in the cyber survivability test plan. For consistency, the test limitation should be titled "Use of cyber M&S" and, along with the appropriate severity level, is considered OPTEVFOR's acceptance of the cyber M&S environment to support the stated test objectives.

The impact of the limitation should provide sufficient details to stakeholders regarding the risks of using M&S in the program's cyber survivability evaluation.

The mitigation shall depict the side-by-side comparison of the modeled environment and the fielded system to accurately characterize the deltas and capture the acceptability of the environment. This information should be easily incorporated from the PMO's V&V data provided as part of the test planning process.

Additional information regarding follow-on test events should also be included to provide stakeholders a clearer understanding of the overall risk.

The severity level of the limitation should be based on the acceptability analysis. As an example, if the modeled environment is a nearly identical representation of the fielded system and follow-on testing in the operational environment is scheduled as part of the test strategy then the limitation may be "minor". Conversely, if the modeled environment only supports limited vulnerability discovery because of wide deltas between it and the fielded system and follow-on test events are not scheduled, then the limitation should be at least "major".

2.6 - OTD RESPONSIBILITIES

It is the OTD's responsibility to ensure the cyber test planner or designated WD cyber Subject Matter Expert (SME) leading the cyber test planning effort has discussed the cyber M&S use with 01D and 01B. If the use of M&S and any associated limitations are determined at the time of TEMP development, the OTD ensures the limitation is documented in the TEMP. Regardless of the limitation within the TEMP, it is the OTD's responsibility to ensure the cyber test planner or designated WD cyber SME generates the "Use of cyber M&S" test limitation during the test planning process in coordination with 01D and that the documented limitation is carried through the test report. Lastly, the OTD ensures that the M&S V&V report is received prior to the cyber survivability test planning milestone CP-3.

SECTION 3 - CYBER SURVIVABILITY IEF GUIDANCE

01B is the authority on IEF development. This section is intended to provide high level guidance to the OTD to assist future test planning efforts as a program progresses through the test planning process. For IEF development, the OTD should use the OTD IEF Checklist. Much of this section contains content from the OTD IEF Checklist and IEF Template; some of that content has been modified to suit cyber survivability testing. The OTD should meet with the divisional 01D Exploitation Analyst (EA) and provide the EA with a basic overview of the SUT. This will ensure that 01D has the requisite information to support test design and proper test resourcing, and that the OTD and test team understand the expectations of the cybersecurity portion of the IEF. Specific guidance for cyber inputs to the IEF can be found in 01D Standard Operating Procedure (SOP) 2101.

01D shall be consulted after Touchpoint 1 products are refined to discuss:

- Defined SUT/SoS
- SUT concept of employment and concept of operations
- Mission Critical Subsystem Matrix (MCSM) / Mission Critical Software Function Matrix (MCSFM)
- Effectiveness Critical Operational Issues (COIs) and associated tasks
- System Validated Online Lifecycle Threat (VOLT) report
- Cybersecurity concept, including threats and defense
- Cyber T&E system information on-hand, and what is still required
- DT/OT alignment strategy
- OT cyber scope
- Augmentation requirements and other test resourcing

3.1 - CYBERSECURITY CONCEPT

The cybersecurity concept is described in section 1.3.3 of the IEF and should be as detailed as possible to include users, networks, threats, defenses, etc., to define why cybersecurity testing is relevant to the SUT. All threats listed in the subsection titled Cyber Threat Environment should have a corresponding defense concept listed under the title Cyber Defenses. If a threat has no corresponding defense concept, then this must be acknowledged. The acknowledgement should state that the SUT is limited in its capability to prevent, mitigate, and recover losses that impact its mission capability due to a cyber-attack. The cybersecurity concept section should NOT contain cyber DT or OT efforts, such as CTTs, CVPAs, or AAs which belong in the Cyber T&E Strategy (IEF Section 2) or Cyber Test Execution (IEF Section 3) sections as appropriate. If there are no cybersecurity concerns for the SUT, this would be included in the cybersecurity concept section as well. Examples are provided in the current IEF Template.

3.2 - IEF CYBER CRITICAL COMPONENT SELECTION

The Mission-Based Test Design (MBTD) process identifies the mission areas and provides an initial determination of the critical components. The critical components selected during MBTD are chosen from a suitability standpoint and serve as the foundation to define the initial cyber relevant terrain. In essence the goal is to make and refine the list of components that could conceivably be denied or degraded to directly cause an impact to the ability of the SUT to perform the mission(s). Some key elements to look for are the presence of Ethernet, Switches, and Universal Serial Bus (USB) interfaces within system components. Many times, these components are using some sort of embedded operating system and could be subject to cyber-attack. Also, look for key words in the system description such as processor, program, controller, terminal, multi-function, etc., which are often used by designers to indicate some kind of processing. Finally, consider any external systems that touch the SUT. Examples of this would include maintenance laptops, software updates, mission computer uploads, etc.

3.3 - MCSM AND MCSFM

The MCSM lists critical components within the SUT, like the Critical Components Breakdown (CCB) spreadsheet delivered with the cyber survivability test plan and should include any redundancies or duty cycles as applicable. The MCSFM lists SUT critical software functions but does not include software dedicated to the operation of hardware.

3.4 - DOCUMENTATION SUPPORT

Required documentation should be altered based on what is applicable to the SUT. For example, a list of removable media access ports is unrealistic for a platform level test. More references and documentation can be added as necessary. Information should be categorized into two groups: what is available prior to IEF signature, and what is outstanding at the time of IEF signature. The absence of information will lead to uncertainty in the MBTD process and could lead to a limitation to test which would be documented in the associated test plan.

3.5 - CRITICAL OPERATIONAL ISSUES (COI)

The cyber survivability COIs will mirror the effectiveness COIs. Suitability COIs may also be considered after a discussion with 01B and 01D support competencies. Cyber COI guidance for tasks and measures can be found in the 01B IEF Checklist. Cyber COI Data Requirements are found in the current cyber survivability test planning template.

3.6 - PLATFORM MISSION TASKS (PMT) VIEW ANALYSIS

Authoritative guidance for PMT views can be found in the current OTE Manual and Test Reporting Handbook and Capabilities Based T&E Implementation Guide. They are required in all OPTEVFOR test efforts. PMT view creation begins during MBTD when the SUT's missions are decomposed into subtasks which are linked to performance measures.

SECTION 4 - CYBER SURVIVABILITY TEMP GUIDANCE

Cyber survivability evaluation is part of a program's overall OT&E and should not be viewed as a separate requirement. As such, adequate resourcing for cyber survivability evaluation and stakeholder agreement shall be considered to plan and execute an adequate test. The TEMP, or any other OT&E resourcing document, is program management "owned" and relies on critical OPTEVFOR test design and resource inputs to ensure the approving authority is confident adequate DT and OT will be executed. It is critical for the OTD to ensure the necessary level of detail is included to adequately summarize the test strategy, scope of test, known limitations, and resourcing.

OPTEVFOR's cyber workforce consists of government and contractor employees and must rely on funding from the program office to plan, execute, analyze, and report on cyber survivability OT&E for each program. Therefore, it is imperative that the estimated costs to meet these requirements are coordinated with 01D using historical costs for similar systems as a basis of estimate. Additionally, if the cyber test planners are contractors funded by the individual program office, a cost estimate for the overall test planning support by the cyber test planner is required. Using the estimated costs, the OTD should ensure the PMO includes the cyber OT&E resource requirements in its T&E budgets during the TEMP development and review process. An Independent Government Cost Estimate (IGCE) based on the actual size and scope of the test will be provided by 01D to the OTD for text execution after test planning has commenced. An IGCE is an official document that 01D generates and provides to the WD to outline, test team travel funding, and funding delivery instructions. The 01D IGCE is described further in section 5.6.2. If cyber OT&E will be supported by other test teams or organizations, 01D is responsible for identifying the appropriate organization(s) and resourcing requirements to support the established scope of test. Once 01D and the external organizations determine availability to support testing, resourcing requirements will be provided to the OTD; the OTD will forward them to the PMO for future OT&E funding.

An IEF creation, Tailored IEF, or Master Test Strategy (MTS) update is typically driven by the necessity to provide inputs for a TEMP that is being created or updated. An OTD should be familiar with the MBTD process and be aware that an IEF provides content for a TEMP. Both of those documents drive what is later captured in a program test plan. These document relationships are important for an OTD to understand with respect to cyber survivability strategy development because he or she may be limited by the availability of a cyber test planner to assist them during MBTD and TEMP review and input. Depending on the availability of contractor support, government support, or active duty billets, there may not be a cyber test planner available prior to the beginning of test planning to assist the OTD with the IEF and TEMP effort. In these circumstances, the OTD should elevate the issue to their chain of command and request leadership support to identify an appropriate path ahead with consultation from 01B and 01D.

TEMP development is typically coordinated by the program office via a T&E Working Integrated Product Team (WIPT). While the WD and OTD are the primary OPTEVFOR members to the T&E WIPT, they are encouraged to liaise with 01D during TEMP development to ensure cyber OT&E requirements are appropriately captured in the TEMP. The following section of the cyber survivability handbook is not meant to provide an OTD explicit content for cyber survivability OT&E TEMP input since each TEMP is unique and tailored for the SUT. Rather, it highlights

items an OTD should look for in a draft TEMP with respect to a basic understanding of the technical aspects of the system, the DT strategy the PMO is intends to conduct, and what information needs to be produced and provided back to the PMO to adequately and accurately detail the cyber survivability OT strategy. For further information on TEMP development, please refer to the OT&E Manual. Detailed guidance for cyber TEMP inputs can be found in 01D SOP 2102

4.1 - ACTION OFFICER (AO) REVIEW AND INPUT

This stage of TEMP development involves interactive dialogue to formulate the initial scope of cyber OT&E, resulting in a first draft of the TEMP document for stakeholder review. The OTD uses the MBTD process, and an early understanding of the system architecture expected at fielding to guide the OT&E inputs and review. To optimize the fidelity of cyber OT&E content within the TEMP, the OTD is expected to:

- Provide the list of Required Information and Documents from section 5.5.2 of this handbook as TEMP content to enable the OTD, cyber test planner (if available), and 01D to understand the overall system architecture
- Facilitate discussions regarding DT and OT alignment, scope of test, and strategy between the PMO, WD, and 01D
- DOT&E involvement is encouraged for oversight programs
- Facilitate discussions among PMO, Systems Command Technical Authority leaders, and fleet release certification officials regarding system restoration or re-baselining requirements post-test

NOTE

Any associated planning, resource requirements, and execution are the responsibility of the PMO to conduct, secure, and manage (respectively). The funding requirements and any additional time required for restoration or re-baselining after an OT event must be accounted for in the TEMP OT resources.

- Review the draft TEMP to ensure the following questions are adequately addressed:
  - Is the cyber DT strategy fully summarized on the PMO's planned activities?
  - If the PMO desires to conduct joint, combined, or integrated testing that supports OT requirements:
    - Will DT led events have OPTEVFOR involvement? (if applicable)
    - Is resourcing captured in the TEMP to support the desired level of OPTEVFOR involvement in those events?
    - If ranges or labs are intended to be used, does the PMO intend to have the range/lab environment accredited by OPTEVFOR? (required for use in OT)
    - Will OPTEVFOR be permitted to review and comment on the test plans for execution of DT events?
    - If oversight, is DOT&E planned to be included in the events?

        - If combined testing with other programs, are both program test schedules identified?
- Provide the following inputs to the PMO for the OT portion of the TEMP:
    - Scope of test based on defined SUT, SoS, and cyber threat environment
        - What configuration is being tested for OT?
        - What limitations are known or what is at risk of becoming a test limitation?
        - What test tools and capabilities are required? (if beyond what the OPTEV-RT already provides, such as non-IP testing and/or special considerations)
        - What data from DT is expected to be used in OT&E? (if applicable)
- A general summary of the conduct of the CVPA that includes the following:
    - When and where it will take place?
    - How long it will be?
    - What resources are required? (outside of what the OPTEV-RT already provides)
    - What test assets are required? (e.g., ship, aircraft, maintenance devices, etc.)
    - What external SMEs are required? (e.g., contractor support, in-service engineering agent support, etc.)
- A general summary of the AA that includes the following:
    - When and where it will take place?
    - How long it will be?
    - What resources are required? (outside of what the OPTEV-RT already provides)
    - What test assets are required? (e.g., ship, aircraft, maintenance devices, etc.)
    - What external SMEs are required? (e.g., contractor support, in-service engineering agent support, etc.)
    - What threats are intended to be portrayed? (i.e., insider, nearsider, outsider)
    - What are the intended effects against the system? (e.g., degrade, deny, exfiltrate, etc.)
- Cyber OT funding requirements:
    - Planning support
    - Execution and reporting (may include a risk reduction event, augmenting test resources, and site visits)
    - Capability development (if required)
    - Lab/range (if required)

01D is available to support PMO discussions as well as support tailoring the TEMP inputs. All TEMP inputs shall be routed through the appropriate divisional EA within 01D for review of the potential test strategy and to assist with identifying resourcing deficiencies. All 01D comments

shall be adjudicated prior to the subsequent TEMP review stages. The OTD is expected to provide a Comment Resolution Matrix (CRM) along with the TEMP for 01D review.

4.2 - O-6 REVIEW

This stage of the TEMP review will formally capture all TEMP's stakeholder comments for AO adjudication prior to routing the TEMP for signature. There should not be significant changes to the cyber portions of the TEMP unless the program experienced significant changes to fielding, schedule, or system architecture since the AO review and input stage. The OTD is expected to:

- Ensure all OT inputs from the AO review and input stage have been correctly incorporated
- Ensure the overall DT and OT test strategy is up to date and accurately reflects the program's projected fielding configuration and delivery schedule
- Ensure the test resourcing is accurate and includes what was provided by 01D during the AO review and input stage
- Route the document through 01D for comments
- Identify any discrepancies that resulted from 01D review within the CRM and the executive summary in the electronic document router

When routing the TEMP through OPTEVFOR, the OTD shall ensure that 01D is included in the routing chain; this ensures 01D is able to provide a formal review and comments to the OTD and program office. 01D will provide critical comments based on the scope of test, resourcing, scheduling, execution, and limitations. Substantive and administrative comments will also be provided and should be addressed accordingly. The OTD is expected to provide the CRM along with the TEMP for 01D review.

This stage of TEMP review may lead to additional comment adjudication working groups to address critical comments held by various stakeholders of the TEMP. The OTD needs to be aware that changes to the TEMP may cause issues with red team availability, red team capability limitations, schedule delays, and test adequacy. 01D must be involved with any TEMP comment adjudication working groups that deal with the cyber T&E portion of the TEMP to ensure test execution is not affected.

4.3 - FLAG/GENERAL OFFICER OR SENIOR EXECUTIVE SIGNATURE

This is the final stage of TEMP routing. There should be no outstanding issues remaining with the TEMP. If there are unresolved critical comments that need to be adjudicated at the Flag/General Officer level, the OTD must ensure the division leadership and OPTEVFOR N00 have comprehensive understanding of the unresolved comments. Include 01D in the discussions for full support. At this stage, the OTD is expected to:

- Ensure all OT inputs from the O-6 review stage have been correctly incorporated
- Ensure the test resourcing is accurate and up to date

When routing the TEMP through iBOSS, the OTD is not required to select 01D if all critical comments have been adjudicated. However, the OTD should provide a brief status email to their EA stating the TEMP is in final signature phase and no outstanding issues remain. This status

should be further reflected within the executive summary that accompanies the TEMP within the electronic document router. If critical comments are still outstanding (regarding cyber T&E), the OTD shall contact their appropriate EA within 01D to arrange for a follow-on discussion of the status of the TEMP.

SECTION 5 - CYBER SURVIVABILITY TEST PLANNING

OPTEVFOR's cyber survivability test planning process and templates must be adhered to for all Navy-led OT&E regardless of what organization executes the testing. The OTD and cyber test planner shall implement the test planning process outlined in the following sections to ensure test team integration and delivery of an adequate cyber survivability OT plan. The desired approach for the cyber test plan is for it to be an enclosure of the overarching test plan for a program. However, a standalone cyber test plan may be required to accommodate unforeseen circumstances such as test schedule, asset availability, or limitation of the program funding for test planning. 01D SOP 2100 contains high level summaries of each major milestone in cyber survivability test planning.

5.1 - MISSION EFFECT TEST AND ANALYSIS

CS test planning and execution uses an adversarial mission effect approach to evaluate a system's cyber survivability. The test planning process used to support the evaluation is illustrated in Figure 5-1 below. The diagram is divided into blocks of time with the activities required during the timeframe depicted in a flowchart. Each block of time and required action is described further in the text below. The focus of this test planning process is to gather sufficient system information to characterize the attack surface, identify initial attack vectors, define test objectives, and ensure the necessary test resources are available. Documentation delivery is, historically, the biggest delay in getting to an adequate and informed test plan. **As a general guideline, test planning should start no later than 9 months prior to the expected test execution**. **For very large systems such as global enterprise systems (e.g., global communication systems) or surface platforms (e.g., FFG, DDG, LHA, etc.), the test planning process may need to start more than 12 months in advance**. The purpose of the extra time in the test planning process is to accommodate an increased level of effort for documentation delivery and analysis to enable OPTEVFOR participation in DT events that will contribute to the program's OT strategy. The cyber test planning process is owned by 01D as the cyber competency of OPTEVFOR. 01D EAs work with the assigned OTD to provide process oversight. The EA is responsible for the management and execution of the cyber test planning process.

Each cyber T&E test planning milestone is called a Checkpoint(CP) and represents the maturity level of the planning process up to a point in time. Some CPs culminate in a stakeholder brief/review while others culminate when all necessary stakeholders concur that the necessary exit criteria have been met. Regardless of how a CP is declared "complete", the overall cyber planning process is a technical focus on developing a test based on the mission relevant cyber terrain of the SUT and pairing a red team's capabilities to collect the necessary data requirements. The test planning process provides a vehicle for the test team(s) to participate in the process as the designated test execution stakeholder. This process was designed to be led by technical experts within the DoD cyber operations domain and ensure participating red team assets are prepared to conduct the evaluation.

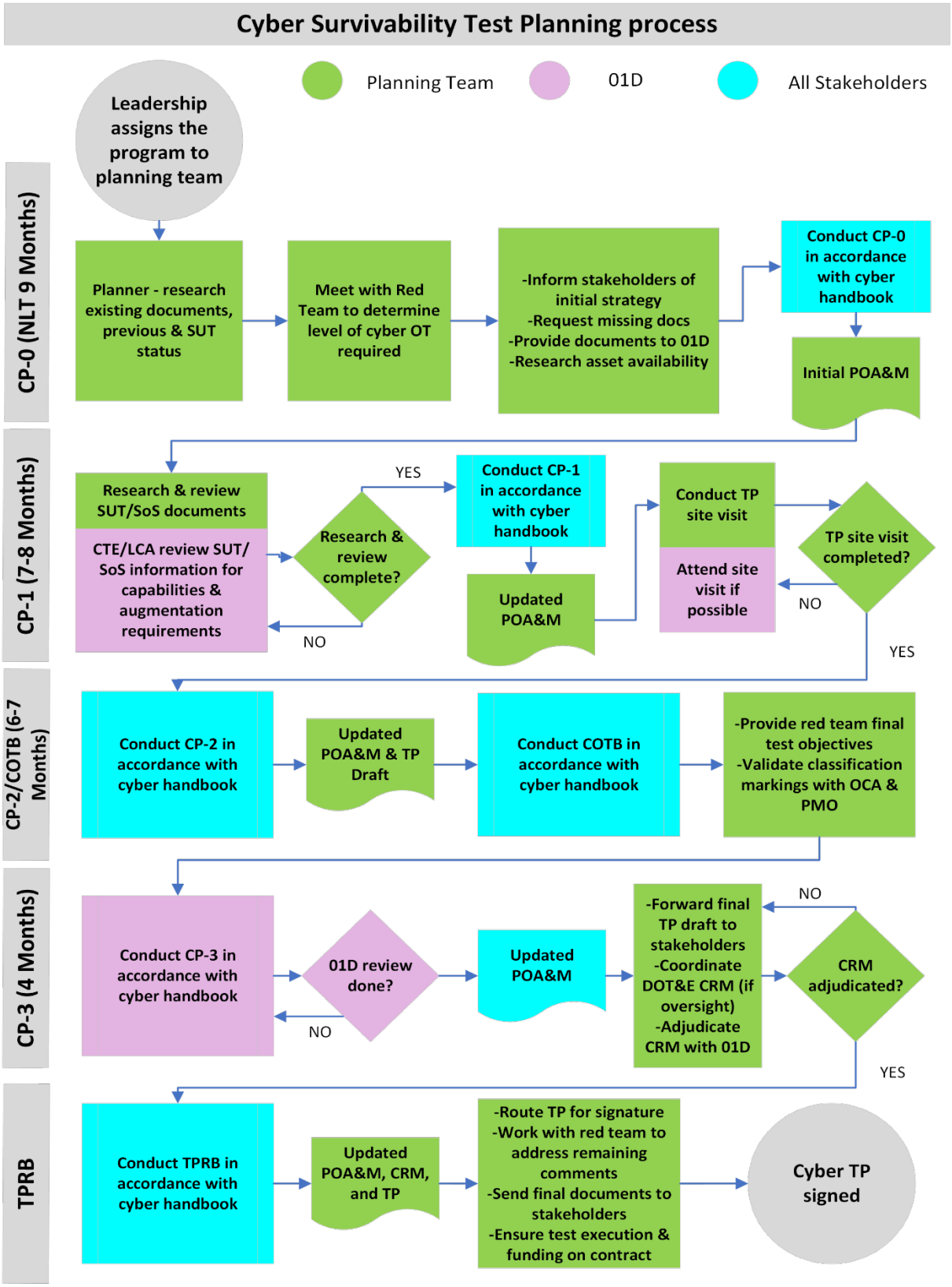
In the event external organizations are required to augment the testing (e.g., MIL-STD-1553 support), that organization should be brought into the test planning effort in the same manner as the OPTEV-RT and actively engaged throughout the process. 01D Operations is responsible for identifying, scheduling, and forwarding funding requirements of augmenting teams to the OTD.

It is the cyber test planner's responsibility to collaborate with the augmenting team throughout the test planning process and it is the OTD's responsibility to ensure the augmenting team's funding is delivered on time from the program office to support the testing.

The cyber survivability document templates can be found on OPTEVFOR's Unclassified SharePoint. The test plan template was developed to be used as a standalone test plan or as an enclosure or addendum to a master test plan. In the event a standalone test plan for the system is not used, all cyber survivability test plan content shall be in one document as an enclosure or addendum and not spread throughout the master test plan. This ensures the OPTEV-RT is provided all required information in a coherent and consistent format to execute test objectives.

Figure 5-1 is an overview of the test planning process.

Figure 5-1 Cyber Survivability Test Planning Process Overview



5.2 - ROLES AND RESPONSIBILITIES

An overview of the roles and responsibilities for test planning, execution, and reporting are provided in table 5-1 below.

Table 5-1 Roles and Responsibilities Overview

01D	Warfare Division
• Responsible for overall cyber test planning & checkpoint (CP) processes, acceptability of technical documentation, Plan of Action and Milestones (POA&M), and CP completion • Provide process, templates & tools for test planning • Lead Change Control Board to incorporate lessons learned and template modifications • Participate as a subject matter expert and a stakeholder • Collaborate and makes determination of cyber OT strategy & level of effort • Research advanced capabilities and augmentation requirements for non-enterprise information system-based programs • Identify source of augmentation and associated funding requirements • Schedule test teams in support of cyber test execution • Provide OPTEV-RT review and input for attack surface, vectors, test objectives, data requirements, and test cards • Support WD at TP site visit • Provide estimate of duration and personnel needs for test execution • Provide technical support for system/component off-limits discussions • Conduct pretest brief and coordination visit • Provide input for Test Plan (TP) • Lead DOT&E Comment Resolution Matrix (CRM) adjudication • Coordination with external entities with respect to red team resources and capabilities in accordance with 01D Standard Operating Procedure (SOP) 2104.	• Support 01D in test plan generation following the cyber survivability test planning process • Use OPTEVFOR published cyber templates and products • Warfare Division (WD) and cyber test planner complete CPs, follow POA&M, and write TP • Collaborate with 01D to determine cyber OT strategy • Cyber test planner communicate & inform Operational Test Coordinator (OTC) / Operational Test Director (OTD) and WD leadership on schedule and status • Cyber test planner coordinate/incorporate 01D input for TP • Cyber test planner conducts TP site visit • Cyber test planner supports system/component off-limits discussion and finalization • OTC/D lead Concept of Test Brief (COTB) with 01D support • Route final TP for signature • Support DOT&E CRM adjudication • Manage version control of test products post COI Evaluation Working Group (CEWG) and getting concurrence from 01D regarding technical changes to the same • OTC/D responsible for scheduling of fleet assets in support of test execution • (If applicable) Support 01D in coordinating with augmenting organization during test planning process

5.3 - OFF-LIMITS, NO EFFECT/NO STRIKE, AND TEST LIMITATIONS

Declaring a system or component off-limits means it may not be scanned, physically touched, accessed, manipulated, addressed, or be the target of any other action that could directly alter its state. The authority for making off-limits declarations rests with the program office, test asset owner, or a technical warrant holder. 01D may recommend an off-limits declaration be made based on its responsibility to execute the testing, and only 01D may accept an off-limits components list. However, only the authority who made the off-limits declaration can remove the designation. **If formally declared, an off-limits designation is absolute through the**

completion of test execution; no action of any kind can be taken against the designated system or component. In accordance with SECNAVINST 5000.2G, if a component or system is deemed off-limits, an alternate test strategy must be identified for evaluating the component or system to adequately capture and categorize cyber vulnerabilities within an operational context. The strategy is program office created and will need to be referenced with specific detail in the TEMP/MTS and may require a TEMP/MTS update.

There are four main justifications supporting an off-limits declaration, and it should be noted that some items being placed off-limits could create a limitation to test:

- Effects to real world operations (data spillage, interruption of services, etc.)
- Loss of life or personnel injury
- Irrecoverable effects to system or component (lack of spares is not an acceptable reason)
- Damage or destruction of surrounding environment

The proper authority shall provide the cyber test planner rationale linked to one or more of the justifications above in writing for each system or component being declared off-limits. An authority may have other justifications not covered in this handbook but, as a system authority, they reserve the right to make a declaration. A significant effort to reload or re-baseline items that are "one of" or obsolete should not be the sole reason for an off-limits designation, and a lack of spares cannot be the only reason for declaring an item off-limits. For efficiency, a digitally signed email from a government authority is sufficient to count as a formal declaration. During test planning, the cyber test planner is responsible for coordinating between 01D and the requisite authority for clarification of off-limits items. The test plan shall contain a list of designated off-limits items along with the associated rationale.

No effect/no strike means that the system or component is not targeted for exploitation during the test and no data is required to be collected off stated system/component. However, no effect/no strike components may still be involved during test execution as they may facilitate access, persistence, and/or lateral movement during test. Designating a system/component no effect/no strike does not necessarily require a test limitation if it is not foreseen to cause an impact to making the cyber survivability determination. Potential justifications for designation for no effect/no strike could be, but are not limited to:

- The system has been previously tested and not changed (may or may not be acceptable given the time since the last testing effort, and additional vulnerabilities known or additional adversarial capabilities)
- The system or component is outside scope of testing efforts
- The system or component must be traversed through to reach critical components

For each system listed on these two lists, the PMO must provide a justification for the entry and the IP addresses, hostnames, and other unique and persistent identifiers. A test limitation is necessary if data collection requirements are unable to be met for a particular part of the test to make a cyber survivability determination based on the scope of testing established in the test plan. A system or component that is declared off-limits may also drive the necessity to generate a test limitation due to an inability to collect data during test.

5.4 - CYBER SURVIVABILITY TEST PLANNING SCHEDULING RULES

The OPTEV-RT is a mission funded capability and a shared resource to support cyber OT&E execution requirements. To ensure equitable access to the red team and maximize the mission funding value, 01D must ensure programs seeking execution support adhere to the cyber operational test and evaluation scheduling business rules. This document details specific scheduling characteristics, processes and responsibilities to ensure the scheduling process supports the overall OPTEVFOR cyber T&E mission.

The most up to date document can be found on the OPTEVFOR SharePoint Online portal.

5.5 - PRE-TEST PLANNING

Pre-test planning steps must occur as soon as the program is initiated in the division. The focus is to gather and evaluate the system documentation to establish the program's T&E strategy. Gathering documentation is the most time-consuming task. Many of the documents required for test planning are not standardized and the information they contain varies greatly from program to program. Sometimes, technical information required to execute the test planning process is not under the control of the United States government and is held as proprietary vendor information that is not part of contract deliverables, which could result in a limitation to test.

As documentation is delivered to OPTEVFOR, it is imperative that the cyber test planner review it to ensure that it contains the required information prior to acceptance.

Sometimes, pre-test planning will start when the system's IEF and/or TEMP is being finalized. Early coordination between the OTD, cyber test planner, 01D, and PMO personnel is strongly recommended to ensure all stakeholders understand the overall cyber survivability T&E process. When determining level of effort for test plans, refer to section 1.3 of this document. Cyber test planners should consult and follow more detailed guidance provided in 01D SOP 2200.

5.5.1 - No Later Than 9 Months Prior To Test (12 Months for Platforms)

During IEF construction or pre-test planning the OTD/OTC are responsible for all test planning for their program. Test plan development tasks may be delegated to cyber test planner however the OTD/OTC retains overall responsibility. The OTD shall:

- Notify 01D Operations of upcoming testing requirements to provide the following information so 01D support personnel can be designated:
  - System name and Test and Evaluation Identification Number
  - Proposed dates for testing, if known
  - Type of support requested such as, but not limited to, IOT&E, OA, and DT Assists
  - Amplifying info or additional support being requested
- Coordinate with 01D Operations for estimate on test scope based on previous testing efforts and/or comparably sized systems
- Review latest OPTEVFOR published cyber templates available

- Identify asset availability with PMO
- Begin gathering the information needed for test planning, including compiling a list of contact information for each program stakeholder (including NAVSEA 08K for nuclear propulsion systems)
- In collaboration with 01D, identify if there is a need for augmentation of OPTEV-RT
- Check availability of the OPTEV-RT to support the projected test schedule (schedule will be confirmed by 01D)

The 01D Operations maintains an execution calendar that spans multiple fiscal years. In the event OPTEV-RT cannot support the asset schedule and external augmentation cannot be coordinated, 01D and WD leaderships will determine the prioritization of the programs and inform the OPTEVFOR Director. Early engagement with 01D is critical to ensure the timeline allows for external resource coordination as applicable.

5.5.2 - Required Information & Documents

The following is the list of documents and information that are required to begin test planning. These documents assist the test planner in the understanding of a system's attack surface and in the development of test objectives. This list should not be considered comprehensive. This list of documentation is also a living list that is modified with each handbook revision. As part of the pre-CP engagements, the cyber test planner and 01D representative will make sure the documentation request is accurate. Some of the required documents/information may not be readily available or may be significantly out of date. As test planning progresses through its various milestones, the cyber test planner may have additional requirements for information. When it is not possible to get all the information in the below list, the cyber test planner and 01D shall work together to determine if the level of documentation available is sufficient to proceed with testing. This determination will be made at CP-0 and updated at CP-1. The cyber test planner will document the missing information on the respective CP templates and meeting minutes.

- Detailed network architecture documentation (Note: This also pertains to all subsystems within the SUT):
  - IP Schema
  - Data flows
  - Physical and logical connections
  - External Interfaces
  - Virtual LAN configurations
  - Intrusion Detection System (IDS)
  - Intrusion Prevention System (IPS)
  - Network demilitarized zones
  - Proxies
- Technical manuals or interactive electronic technical manuals

- System baselines for all systems
- Internal and external interface descriptions
  - Interface addresses
  - Hostnames
- Software (including version and patch level)
- Sub-component make and model numbers
- Removable media ports
- Ports, protocols, and services details
- eMASS identification number
- Network switch, firewall, IDS, IPS, Proxy configuration(s):
  - Running Configurations
  - Access Control Lists
  - Rule Sets
- CTT and/or cyber risk assessment report(s)
- Assessment and Authorization process documentation
- Program Protection Plan (PPP)
- System Engineering Plan (SEP)
- Information Support Plan (ISP)
- Patch management process documentation
- System-specific cyber defense TTPs
- Classification requirements for cyber survivability test planning, data collection, analysis, and reporting including SoS and subsystems to include expected classification of results
- Interface Control Documentation / Software Interface Descriptions / Software Design Descriptions
- Cross Domain Interface list
- DT Plans and Results
- Previous OT Plans and Results
- System SME Point of Contact (POC) Information

When these documents are requested, the cyber test planner shall provide due dates and track them to completion. Late documentation delivery will cause the test planning process to be delayed and impact test plan signature as well as test execution. Documents that are acquisition milestone decision documents (e.g., PPP, ISP, SEP, etc.) shall be provided within 10 business days of a request. If requested documents and/or information do not exist, the program office may need to generate them, which may cause a delay in test planning. The cyber test planner will update the

Plan of Action and Milestones (POA&M) using 01D SOP 2203 as guidance and inform the stakeholders whenever documentation may delay the test planning process. Intuitively, if a SUT is installed on an operational asset, then it should be a reasonable expectation for the PMO to be able to provide the requested information.

5.6 - CHECKPOINT 0 (CP-0)

5.6.1 - CP-0 Preparation

Approximately 2 to 3 months prior to the expected date of CP-0, the WD Section Head assigns a cyber test planner to begin documentation collecting and analyzing documents. If not completed in the pre-test planning phase, the cyber test planner will review all the documentation to determine if it is sufficient to begin test planning. This must include any previous testing, including DT, as well as all the other documents listed in section 5.5.2. If the documentation does not exist or is not available, the cyber test planner shall note this as an area of concern.

Prior to the CP-0 review, the cyber test planner will meet with the 01D EA to determine the required scope of testing for the system using 01D SOP 2204; this will be used to inform all stakeholders and to maintain a consistent approach to cyber T&E. During the meeting, the cyber test planner will be expected to present a technical overview of the system including SUT and SoS descriptions, system architecture, and interfaces. See section 1.3.2 to facilitate this discussion. At the conclusion of this meeting, copies of all available documentation should be provided to 01D for inclusion in the OPTEV-RT's documentation.

The OTD will have to research test asset availability for both test planning, pretest brief and coordination visit, and the projected test dates. If specific dates are not known, the OTD should estimate the dates as closely as possible to ensure that the OPTEV-RT has sufficient availability on its execution calendar in accordance with 01D scheduling business rules. Overarching guidance for the CP-0 process for cyber test planners can be found in 01D SOP 2205.

5.6.2 - CP-0 Execution and Closeout

CP-0 is an administrative review focusing on an introduction to the SUT/SoS, schedule, budget, risks, and missing documentation. This milestone should be used by the cyber test planner and OTD as a venue to discuss the focus areas of the subsequent planning effort to solicit inputs on test scope resourcing requirements early per section 1.3.2. The cyber test planner will schedule the CP-0 review with the following entrance criteria:

- Cyber test planner compiled initial list of stakeholders. Identification of stakeholders is detailed further in 01D SOP 2201
- Cyber test planner received initial technical documents identified in the TEMP
- Cyber test planner reviewed delivered technical documents, prior test history, TEMP, and IEF
- Cyber test planner discussed cyber OT strategy and test planning focus with 01D
- Cyber test planner established initial documentation / information requirements for CP-1
- Test asset availability and schedule identified (if possible)

Insufficient system documentation may lead to an inaccurate estimation of the final scope of test and the associated OPTEV-RT level of effort at the CP-0 milestone. In this case, an estimate based on historical test data, if applicable, will be made by 01D and used as a placeholder on the execution calendar in the event of the execution date(s) not being known at the time. The estimate may reflect an increased level of OPTEV-RT support over what is finally determined later in the test planning process. This is an effort to avoid schedule conflicts due to an increased scope of test. At this point, it is important to identify the need for augmentation from outside test teams. If an outside test team is being used, include them in meetings and work with them for the entirety of the test planning process. Table 5-2 lists the necessary CP-0 attendees.

Table 5-2 CP-0 Attendees

Warfare Division	Director or Deputy Director, OTD or OTC, cyber test planner
01D	Director or Deputy Director, Operations Officer, EA, Red Team Chief or Deputy Red Team Chief
Program Management Office	PM or Assistant Program Manager (APM) or PMO T&E Lead
DOT&E (If Oversight)	AO

Additional information to be discussed:

- Cyber test planner provides an overview of previous cyber test (DT/OT), if any
- Cyber test planner reviews documentation requirements and identifies missing documents/information
- Cyber test planner provides details on declaring items off-limits in accordance with section 5.3
- Cyber test planner provides a documentation delivery timeline required to complete test planning
- Stakeholders review and confirm asset schedule
- 01D Operations discusses the funding requirement for test execution and tentative schedule
- Stakeholders determine if the test plan will be a standalone document or an enclosure
- Cyber test planner inquiries about PMO operational risk management and post-test system recertification concerns (if applicable)
- Cyber test planner begins discussions with PMO regarding off-limits systems and no effect/no strike components with justifications — see section 5.3 for more details
- Cyber test planner briefs areas of concerns and entrance criteria to CP-1

CP-0 exit criteria are listed as follows:

- Cyber test planner finalized POA&M for rest of test planning milestones

- Cyber test planner pulled current test plan template and began to tailor content for SUT
- Cyber test planner identified need for augmentation from outside test teams with 01D support

5.6.2.1 - Initial Government Cost Estimate (IGCE)

Once approved by the 01D Director or Deputy Director, 01D will provide an IGCE for test execution, typically prior to CP-2. The IGCE cannot be provided until a test scoping determination has been made. This requires that sufficient information is available to understand the location(s) of the test, the architecture of the SUT, SoS, and test strategy. In the event final test execution costs are required prior to CP-1, the WD will work with 01D and the necessary external stakeholders to expedite the collection of the necessary information.

5.6.2.2 - Comment Resolution Matrix (CRM)

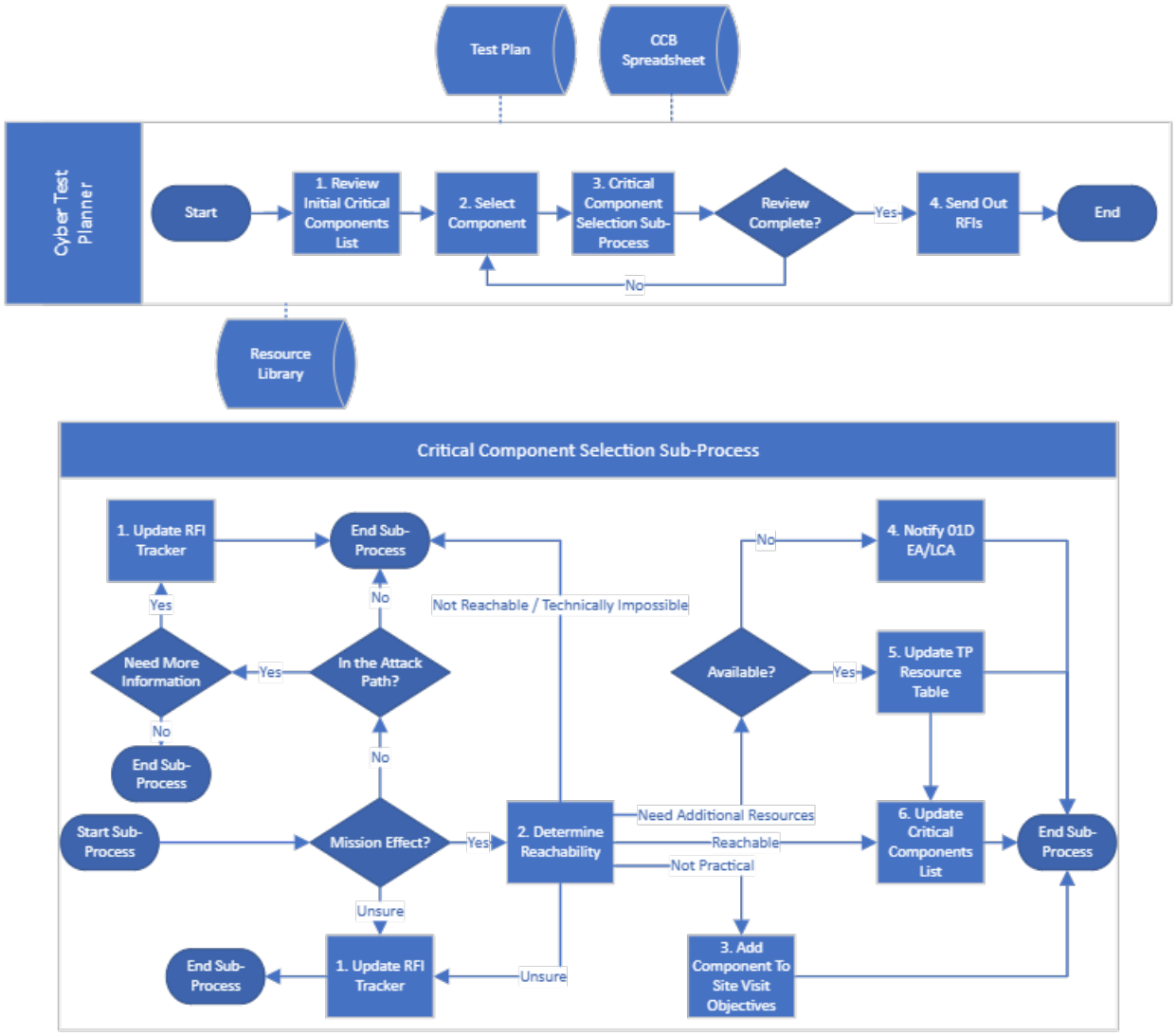
Upon conclusion of CP-0, the 01D EA representative will upload the initial CRM via the mission-based test and evaluation system. The CRM will be used throughout the test planning process to track formal test planning comments between 01D, the WD, and any other stakeholder involved. Critical comments left unresolved or any comment where 01D and the WD have an unresolvable difference will be escalated to 01D & WD leadership for resolution and may ultimately require flag level interaction. Unresolved comments during CP-0 through CP-2 may transfer over to unresolved issues in the test plan and may escalate in severity later in the process. Once CRM has been created, it is the responsibility of the EA to maintain the CRM. The EA, working with the cyber test planner will mark issues resolved with concurrence from the stakeholder who submitted the CRM comment. Once comments are resolved, they remain on the CRM for historical purposes. Detailed CRM guidance can be found in 01D SOP 2103.

5.7 - CHECKPOINT 1 (CP-1)

5.7.1 - CP-1 Preparation

CP-1 is a series of technical interchanges that begin immediately after CP-0. The cyber test planner will begin an in-depth analysis of the SUT using the documentation collected and begin the critical component identification process laid out in Figure 5-4 below. It is expected that this review will lead to more questions and additional information requests. For this reason, it is important to start the test planning process early and allow time between CP-0 and CP-1. Overarching guidance for CP-1 process flows can be found in 01D SOP 2210 and is supported by several other more specific SOPs detailed in their appropriate section.

Figure 5-2 Mission Critical Component Decision Flow Process



5.7.1.1 - Review Mission Areas

The cyber test planner must understand the mission(s) of the system and how it is employed by the warfighter to have a full understanding of why an adversary would want to conduct cyber operations against the system. The expertise of the cyber test planner will likely be from a cyber background, and they may have no experience/knowledge with the execution of the system's mission. Therefore, the goal is to provide the cyber test planner a solid understanding of how the missions are accomplished and how the system supports them. As the mission expert, the OTD is vital to this aspect of the test planning effort and must ensure adequate time is spent with their assigned cyber test planner to enable this critical exchange of knowledge. The cyber test planner needs to be able to determine how each subsystem and component contributes to the accomplishment of the missions during the architectural evaluation later in the process. The association of subsystems to missions contributes directly to the identification of critical components. Critical components will be identified in the CCB spreadsheet provided by the 01D EA. Further guidance for cyber test planners can be found in 01D SOP 2202.

5.7.1.2 - Identify Cyber-Related Functions

Cyber-related functions are defined as any activity or process used by the SUT, or SUT personnel, which could provide an adversary the opportunity to impact the system. The cyber test planner must think outside the box and look for things like supply chain, update procedures, and any other unique procedures for the SUT. A common example would be the system restoration or update procedures. Some questions to ask are:

- Is the device used to update or restore the system ever attached to the internet?
- Is the device stored securely between uses?
- Is the device wiped and reimaged prior to use?
- Is the update provided from an internet-based source?
- Is the update encrypted or provided with a checksum or hash?

5.7.1.3 - Determine Environmental Cyber Threats

The cyber test planner shall obtain the VOLT assessments to determine the potential threat actors that are operating in the environments where the system can be deployed or housed. For programs that will undergo a phased modernization of capabilities, it is important to consider the long-term employment concepts during threat assessment to ensure cyber testing is appropriately considered for each phase.

5.7.1.4 - Evaluate the System Architecture

When evaluating the system architecture, the cyber test planner using 01D SOP 2206, the knowledge of the mission, and the system documentation to determine:

- System interconnections and data flows
- Bottlenecks that could be used to block information exchange between components
- Presence of embedded operating systems
- Ingress and egress routes
- Locations for Critical Program Information (CPI)

The cyber test planner will be looking specifically for ways to impact the mission by denying, degrading, manipulating, or exfiltrating the data used by the system. The key is to begin determining the ways an adversary could affect the mission. This analysis leads directly to the development of the critical components list in the next step. Do not overlook the importance of open source intelligence by searching for COTS equipment information on the internet.

5.7.1.5 - Develop Initial Critical Components List

Critical components are those elements of the system that, if degraded, denied, or manipulated, would have a negative impact on the system's ability to support the mission. In this step, the cyber test planner will develop a list of initial critical components. This list is preliminary because it must be verified at the test planning site visit or through conversation with system SMEs. Experience has shown it is invaluable to sit with the SMEs and go through the initial critical components asking them, "What happens if the component was degraded, denied, or the

information was manipulated?" This information is documented in the CCB spreadsheet template provided by the 01D EA. The cyber test planner shall work closely with the EA to refine the CCB as they find and fill in information. It is better at this stage to over select than to under select. This will be refined through the CP-1 process and the test planning site visit. Refer to Figure 5-4 above for methods of determining critical components. More granular guidance for cyber test planners developing their critical components list can be found in 01D SOP 2207.

5.7.1.6 - Determine Interfaces

The cyber test planner shall look at interfaces to determine how an attacker could get a foothold on the system to begin working toward reaching the critical components identified in the previous step. These interfaces can be logical and physical. Examples of physical interfaces are a USB port, an Ethernet port, a compact disk, a serial port, a system reprogramming port, or a user terminal. The bottom line is that the cyber test planner must be creative.

Special attention shall be paid to external interfaces, specifically the interfaces to SoS components or external networks that could be used by an outsider to gain access to the system. The insider and nearsider threat typically require a trusted, or semi-trusted, person to become a bad actor.

5.7.1.7 - Determine Initial Attack Surface and Vectors

Now that the cyber test planner understands the interfaces and the critical components, they can use this information to map the attack path through the system using 01D SOP 2208. Attack surfaces are different places where an adversary can gain an initial foothold, whereas attack vectors are paths or means by which an adversary can gain access to the critical components.

The cyber test planner will trace the potential attack vector from the attack surface to the critical component. This path will sometimes pass through multiple components and network elements. In the next step, potential vulnerabilities will be identified through an analysis of the elements on the attack vector path and the critical components themselves.

5.7.1.8 - Determine Countermeasures

To adequately assess the mitigation capabilities of the system, the cyber test planner must research and document the inherent countermeasures within the system in accordance with 01D SOP 2209. If the system documentation does not provide the information, a separate request must be submitted to the PMO. Research for COTS components can and should be conducted open source on the internet. Common countermeasures include:

- Anti-tamper
- Firewalls
- IDS
- IPS
- Antivirus
- Host-based Security System
- Program protection mechanisms

If a system contains anti-tamper and it is to be tested, the OPTEV-RT must understand how to avoid triggering anti-tamper capabilities.

5.7.1.9 - Test Planning Site Visit

Once the mission and environment are understood, the cyber test planner may have additional information requirements. These shall be documented as site visit objectives and provided to the site or program office to address with the appropriate personnel during the test planning site visit. The test planning site visit shall not be ad hoc, it should be a well-organized event that facilitates a technical exchange between representatives from the Fleet, PMO, engineering support, and OPTEVFOR. Further guidance for Test Planning Site Visit planning, execution, and questionnaires to be filled out on site can be found in 01D SOP 2211.

Regardless of the additional information required, the cyber test planner must be able to accomplish the following objectives during the test planning site visit:

- Validate and record system interfaces relevant to insider, nearsider, and outsider access points
- Verify system architecture along with any relevant system processes and procedures germane to test objective finalization
- Determine SME support required for test execution
- Discuss off-limits requirements and solicit inputs from proper authorities
- Discuss pre-test risk reduction events and/or post-test system re-baselining requirements

5.7.1.10 - Test Objectives

Test objectives are a critical piece of the cyber OT&E process and shall be developed within an operational cyber warfare context. Each system undergoing cyber OT&E is distinct in its design, mission, and operational employment. With that distinction comes the applicable factors of an adversarial course of action to achieve desired effects against a specific SUT. Cyber OT&E objectives should not be based on red team TTP. Rather, they should be established on a holistic strategy, based on an operationally realistic adversarial perspective, to achieve access, gain persistence, move laterally within the system, and cause a desired operational effect. During test, the red team will choose how it executes test objectives based on red team TTP, capabilities, and vulnerability discoveries. Test objectives are operationally focused and linked to the effectiveness COIs for the associated SUT.

The cyber test planner, with technical support from the EA and supporting red team members, develops the test objectives based on the technical analysis and exchanges leading up to a CP-1. See current CS test plan template for further details on how to create and format objectives. The keys to logical, adversarial based test objectives are adequate technical information of the SUT and successful pairing of red team capabilities to desired system effects in an operational context.

Therefore, there is no set standard on the amount of test objectives for a particular system, only enough to capture a holistic evaluation based on relevant cyber threats to the system.

5.7.2 - CP-1 Execution and Closeout

CP-1 is a series of technical working group sessions and is considered complete when all the required objectives are met, and completion is provided in writing from the 01D Operations Officer. The entrance criteria for CP-1 are as follows:

- Cyber test planner receives and reviews technical system information and determines initial aspects of the scope of test:
    - Critical components
    - Interfaces / data flows / attack surface
    - Cyber threat emulation (insider, nearsider, and outsider)
- Cyber test planner begins PPA (disregard for platform tests)

CP-1 is an iterative research and analysis process for the cyber test planner to request documentation and review it to determine if it meets the information requirement(s) for test planning. The cyber test planner will lead the discussion for the technical working group session(s) and only schedule these sessions with the 01D EA and test execution team (OPTEV-RT or augmented) once the research and analysis is complete and the cyber test planner is fully prepared to lead the technical discussions. Technical working group session(s) can be held more than once if there are action items from the initial session; however, bandwidth/resource limitations for the participants and the test team(s) should be considered when scheduling these meetings. The cyber test planner provides the overview of the system architecture, nominated critical components, and the attack surface with an end goal to derive test objectives and resource requirements for the test team. The cyber test planner should be able to speak to the logic behind each critical component using provided documentation to point out ingress and egress routes. Program SME(s) participation is strongly recommended to provide system expertise and validate any assumptions made during system research and to answer questions during the working group meeting. Although a cyber test planner may not be a technical expert in a particular discipline (e.g., avionic data buses, industrial control systems, cloud-based systems, weapon systems, etc.):

- The cyber test planner needs to be able to bridge-the-gap with basic technical competency to engage with the selected test teams
- The cyber test planner needs to be able to understand test team capabilities/requirements and collaborate to develop test objectives that are relevant to critical components from an operational perspective and aligned to test duration available to the test team

The cyber test planner provides an initial assessment of the critical component(s) in the form of the CCB spreadsheet based on a component's functional support to the SUT mission and an evaluation of the level of effort for an adversary to target the component. As the number of critical components increases, so does the amount of time for test execution (usually).

For platform tests, the planning process scales up:

- Critical components become critical systems (or technical boundaries); criticality determination is still within the same perspective described above based on discussions around cyber test planner research contained in the CCB document.
- CP-1 shall focus on determining what platform systems are going to be "touched" by the test team and why (i.e., system prioritization). For the purposes of the CCB spreadsheet, focus on subsystems instead of individual system components.

The exit criteria for CP-1 are as follows:

- Clearly identify:
    - System attack surface
    - Attack vectors
    - Off-limits component list
    - Test objectives with OPTEV-RT input
    - Recommended initial connection points
    - Required special equipment needed by the OPTEV-RT
- Cyber test planner updated test planning POA&M as necessary
- Cyber test planner completed test plan site visit
- Cyber test planner completed CCB spreadsheet

Approval to move beyond CP-1 can be gained when all objectives are met and is formalized via email from the 01D Future Operations Officer.

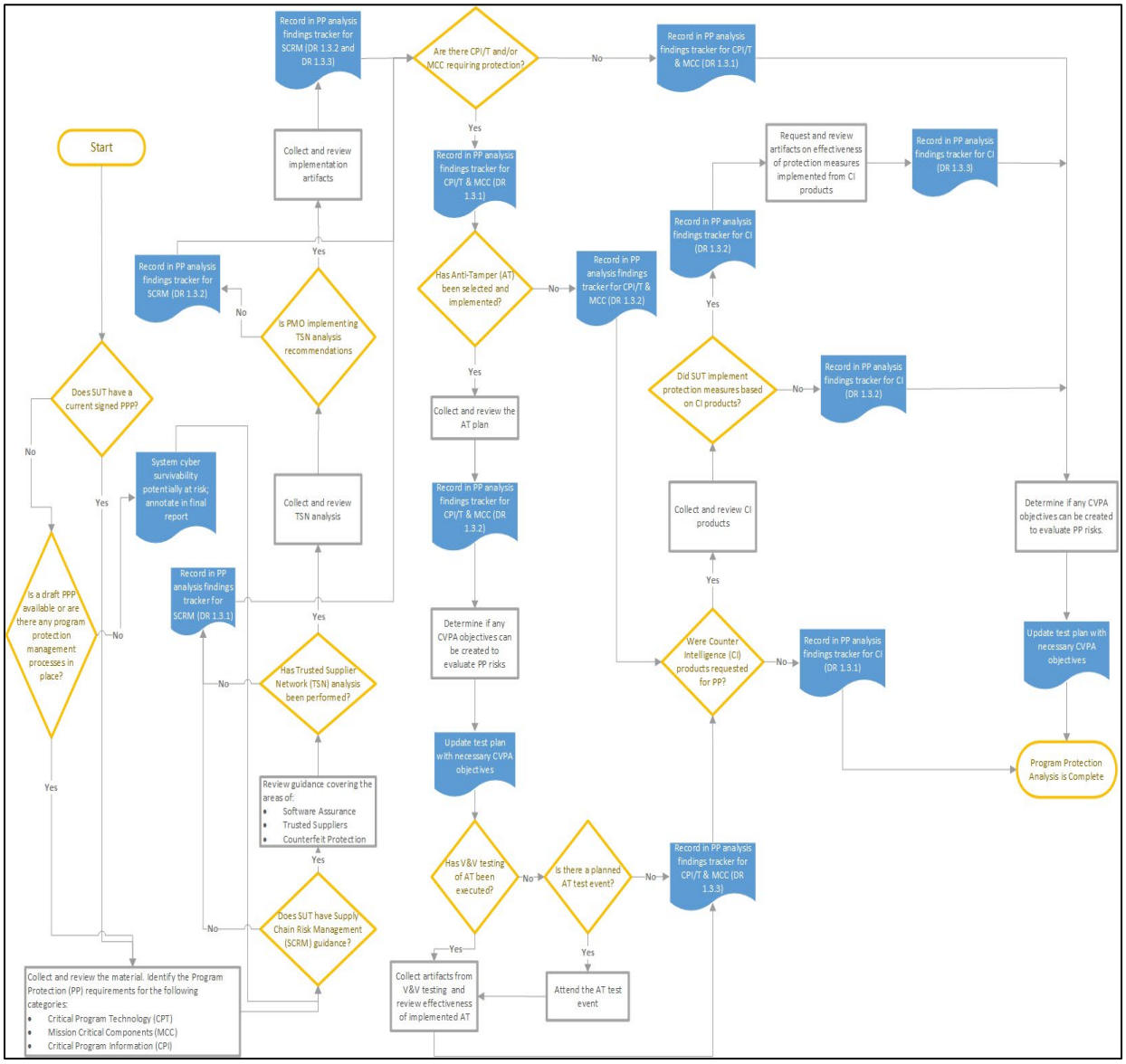
5.8 - PROGRAM PROTECTION ANALYSIS (PPA)

As soon as the cyber test planner receives the PPP, they should begin its analysis. These analyses are not required for platform level tests, and the cyber test planner should remove the Program Protection Analysis (PPA) data requirements from the test plan. The PPP documents the threats, vulnerabilities, and countermeasures selected to mitigate vulnerabilities and manage the risk of compromise of CPI and/or critical component technology. It also provides guidance for implementing, monitoring, and assessing the effectiveness of countermeasures. The PPP serves as a single point of reference for identifying all protection and security mechanisms being implemented by program personnel and associated contractors to protect DoD assets as required by DoD Instruction DoDI 5000.02 *Operation of the Defense Acquisition System,* DoDI 5200.39, *Critical Program Information (CPI) Protection within the Department of Defense* and DoDI 5200.44*, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN).*

The methodology for completing the PPA can be found in Figure 5-5 below. The result of the initial analysis shall be documented in the Program Protection Analysis section of the test plan template and may require additional requests for information. This can continue throughout the entire test planning process. The focus is to determine if the system has any residual risk to its cyber survivability from program protection implementation (or lack thereof). The cyber test planner is responsible for conducting this analysis and providing the data to the OPTEV-RT Lead for post-test data scoring. The process used for analysis is detailed in the cyber

survivability test plan template. The completed PPA is part of the entrance criteria to CP-2 to afford time to address residual risks prior to test execution.

Figure 5-3 Program Protection Analysis Flowchart



5.9 - CHECKPOINT 2 (CP-2)

5.9.1 - CP-2 Preparation

Beginning about 6 months prior to test the cyber test planner will begin final test planning. This phase begins once all requested system documentation and information have been delivered. This includes documentation requested during the test planning site visit. If documentation gaps noted during the initial documentation review remain unresolved, the WD in consultation with 01D must determine if test planning can proceed. Depending on the criticality of the documentation and its

impact to test adequacy, a test limitation may need to be documented in the test plan with stakeholder concurrence especially for oversight programs. Detailed guidance for cyber test planners regarding CP-2 execution can be found in 01D SOP 2212.

5.9.2 - Classification Verification

The OTD is responsible for ensuring the test plan and post-test documents are classified to the appropriate level according to applicable Security Classification Guides (SCG) with concurrence from the Original Classification Authority (OCA). The test plan developed for a SUT captures aspects of the system that, potentially, are of high value to an adversary since it outlines how the OPTEV-RT will attempt to degrade or deny a system using cyber capabilities. As derivative classifier, the cyber test planner shall follow the appropriate SCG while drafting the test plan. Prior to specifying potential attack vectors and associated vulnerabilities in the test plan, the cyber test planner shall request formal guidance from the OCA for the system to confirm the classification level of the test plan. Historically, SCGs contain vague derivative classification guidance regarding the existence of potential cyber vulnerabilities and related mission impacts. The cyber test planner will provide the OPTEV-RT with a list of classification levels for all systems within the SUT as they pertain to raw data, cyber vulnerability data, and post-test data analysis or aggregation. This ensures that the OPTEV-RT uses the appropriate classification handling procedures for data collection, on-test analysis, and post-test products. This list will need to be validated by the OCAs responsible for each system. Obtaining OCA classification confirmation prior to finalizing the test plan and distributing it will prevent accidental spillage and protects all parties from mishandling classified material.

5.9.3 - CP-2 Execution and Closeout

The focus of this CP is for the cyber test planner to present the results of the test planning site visit, and the new information gained. The cyber test planner will schedule the CP-2 review. The approved methods to deliver CP-2 briefs to meet the program's needs are:

- Formal brief in person or virtual
- In conjunction with Touchpoint-B or Concept of Test Brief (COTB)

The entrance criteria for CP-2 are as follows:

- Cyber test planner completed test planning site visit and collected remaining system information
- Cyber test planner engaged with test team(s) to update scope of test based on the site visit and additional information received:
    - Prioritized critical components
    - Finalized test objectives
    - Finalized off-limits components w/ PMO SME inputs
    - Finalized test limitations
- Cyber test planner satisfactorily completed their PPA (Not applicable for platform tests)

Table 5-3 lists the necessary CP-2 attendees.

Table 5-3 CP-2 Attendees

Warfare Division	Director or Deputy Director, OTD or OTC, cyber test planner
01D	Director or Deputy Director, EA, Red Team Chief or Deputy Red Team Chief, Augmenting Test Team (if applicable)
Program Management Office	PM or APM or PMO T&E Lead
DOT&E (If Oversight)	AO

This CP will be a working level review of the information from the site visit. The goal is to finalize:

- Attack surface / vectors
- Critical components
- Test objectives
- Limitations to test
- Off-limits items

Additional information to be discussed:

- Cyber test planner provided program/vendor SME(s) POC information
- 01D Future Operations confirmed receipt of pertinent SUT/SoS information (e.g., off-limits list, IP addresses, virtual local area networks, etc.)
- 01D Operations input for finalization of test objectives & go/no-go criteria for execution
- Finalized expectations and concurrence of external test team contributions and deliverables for final report (if applicable)

The exit criteria for CP-2 are as follows:

- All stakeholder inputs adjudicated satisfactorily
- 01D Operations schedules pretest brief and coordination visit and/or risk reduction event (if applicable)
- Cyber test planner continues to work towards completion of the TP with information from previous CPs
- Cyber test planner supports OTC/D to create COTB
- Finalize attack surface(s), vectors, critical components, off-limits components, and test objectives

5.9.4 - Refine Test Plan

The cyber test planner will continue to refine the test plan and update the POA&M with information gained during the test planning site visit and CP-2. Specifically, the cyber test planner will:

- Update and finalize the appropriate sections of the test plan
- Ensure all pertinent information is provided to the test team and that the test team has validated the information
- Prepare for COTB

Once CP-2 is completed, the focus of the remaining test planning process is to finalize the remainder of the test plan, get the necessary test execution funding in place, ensure test asset availability is solidified, and brief external stakeholders on the test.

5.10 - CONCEPT OF TEST BRIEF (COTB)

A SUT COTB will be conducted in accordance with OPTEVFOR INST 3980.2 (series), the OT&E Manual. Information collected and analyzed up to this point can be easily adapted to provide a very detailed COTB to internal and external stakeholders. The SUT COTB depicts how the cyber survivability evaluation contributes to the overall SUT evaluation plan (spanning operational effectiveness, operational suitability, and cyber survivability). For oversight programs, the COTB is required to be delivered to DoT&E no later than 180 days prior to test execution.

The cyber test planner will support the WD development of the COTB using the standard OPTEVFOR template provided on the OPTEVOR SharePoint. At a minimum, the following information regarding the system's cyber survivability test will be captured:

- Schedule
- Funding status
- Scope of test
- Test objectives
- Test limitations
- Test plan delivery date
- Stakeholder concerns

The cyber test planner shall use 01D and the WD's guidance to develop, schedule, and conduct the COTB. The cyber test planner shall coordinate the required technical support and COTB participation with 01D including any necessary travel requirements and/or 01D contractor support. Tables 5-4 and 5-5 lay out the required attendees for COTBs with the OPTEVFOR Director, and DOT&E (if applicable).

Table 5-4 OPTEVFOR COTB Attendees

Front Office	OPTEVFOR Director and Deputy Director

Warfare Division	Director or Deputy Director, OTD or OTC, cyber test planner
01D	Director or Deputy Director, EA, Red Team Chief or Deputy Red Team Chief

Table 5-5 DOT&E COTB Attendees

DOT&E	DOT&E AO
Warfare Division	Director or Deputy Director, OTD or OTC, cyber test planner
01D	Director or Deputy Director, EA, Red Team Chief or Deputy Red Team Chief

5.11 - CHECKPOINT 3 (CP-3)

5.11.1 - CP-3 Preparation

At this point in the test planning process (approximately 4 months prior to test) the cyber test planner should have the test plan in a signature-ready state (i.e., formatting complete, no missing information, etc.). This is the time for final reviews and test plan finalization. The cyber test planner should project at least 30 days to resolve remaining comments, conduct the test plan review board, and route the test plan for signature. Additionally, for oversight programs, DOT&E requires the final test plan 60 days prior to commencement of test. Overarching guidance for the CP-3 process for cyber test planners can be found in 01D SOP 2213.

5.11.2 - Test Cards and Data Requirements

Prior to completing CP-3, 01D will provide test cards and the final data requirements to the cyber test planner as input to the test plan. The cyber test planner will need to work closely with the OPTEV-RT and augmentees (if applicable) to ensure the input delivery timeline is confirmed to meet the CP-3 milestone.

5.11.2.1 - Test Plan Comment Adjudication

Before submission for CP-3, the cyber test planner needs to provide the draft test plan to the EA's for their review and comment. Once this has been completed and comments adjudicated it will be sent to the OPTEV-RT to ensure data is sufficient to be able to conduct a successful test, each of these reviews shall be allotted 5 business days for completion. Once 01D provides the test card and data collection requirement inputs to the cyber test planner, the cyber test planner shall distribute the test plan to the WD stakeholders for comment. Upon satisfactory resolution of all comments to this point and the document is in a signature ready state, the cyber test planner shall provide the signature ready document to the EA who in turn will provide it to the 01D ACOS for final OPTEVFOR comment. Upon attaining and resolving comments from the 01D ACOS and with permission from 01D the cyber test planner may finally distribute the test plan to DoT&E if

on oversight for their comment. The cyber test planner shall provide all stakeholders a desired date to receive comments to maintain the test planning POA&M. The cyber test planner is responsible for adjudicating all comments with 01D support. The cyber test planner shall communicate any updates that change the level of effort, test scope or the test execution section of the test plan with the WD leadership and 01D. 01D review of these changes is necessary to ensure test execution is not impacted.

The exit criteria for CP-3 are as follows:

- 01D Director or Deputy reviews the document and cyber test planner is provided updated running CRM as necessary
- Cyber test planner updated POA&M as necessary
- Cyber test planner finalized test plan

The final CP-3 approval authority for 01D is the 01D Director or Deputy.

5.11.3 - CP-3 Execution and Closeout

CP-3 is the final review of the test plan where the 01D Operations & EA representatives will review and provide final input for the 01D Director or Deputy. The cyber test planner shall provide a test plan that is ready for 01D Director level review at this time and allow 5 working days for test plan review. This CP is not a meeting but is used as a milestone to track document finalization progress.

The criteria for CP-3 closeout are as follows:

- Cyber test planner provided draft to 01D EAs for comment, and comments have been sufficiently adjudicated by cyber test planner
- OPTEV-RT and/or augmenting team comments adjudicated and/or documented in the CRM
- Cyber test planner received Program OCA concurrence on test plan classification marking
- 01D ensured test team inputs are captured correctly and that objectives are executable
- 01D ensured that test team comments are satisfactorily adjudicated and documents outstanding items in the CRM
- 01D provided test cards and final data collection requirements as input to test plan
- (If Applicable) Augmenting team will review test plan comprehensively and provide content back to cyber test planner

5.12 - TEST PLAN ROUTING

Once CP-3 is completed and all outstanding stakeholder comments have been adjudicated, the test plan is ready to be finalized and routed for signature. The internal OPTEVFOR document routing process will be followed.

5.13 - OTHER TEST PLANNING EFFORTS

This section covers other less common CS efforts including QRA, Cyber EOA, Verification of Correction of Deficiencies (VCD), and the Level of Test Determination (LTD) process (including the No-OT Concurrence process).

5.13.1 - Quick Reaction Assessment (QRA)

QRAs are conducted when rapid fielding of a system must be done to provide emergent capabilities to the fleet, or when the program desires a quick assessment of the cyber survivability of the new system. A QRA test plan is not developed using all the traditional CS test planning process and will only assess capabilities or attributes described in the tasking letter. Consider executing a tailored CVPA to meet the QRA requirements and report on system deficiencies to prevent cyber-attacks. The OTD needs to engage with the program resource sponsor early and attempt to include cyber survivability requirements in the QRA tasking letter. If the letter does not address cyber, DO NOT assume it does not apply. Contact the sponsor to clarify cyber survivability requirements pertinent to the QRA letter. QRA execution requirements should be based on the resource sponsor's priorities to keep the scope of the QRA streamlined, concise, and cost effective.

5.13.2 - Cyber Early Operational Assessment (EOA)

An EOA is conducted very early in an acquisition program's lifecycle often on subsystems and early prototype equipment for the purpose of forecasting risk. For cyber survivability, this may mean conducting a high level CTT based around the review of the SUT's design documentation. An EOA can be used to identify potential system enhancements early in the development lifecycle. Since EOAs occur so early in the acquisition process, it is essential to focus initially on the subsystem level. Decomposition of the system should be focused on functional capabilities vice technical. Input, output, and processing by subsystems should evaluated for potential exposure, denial, or manipulation of data.

5.13.3 - Verification of Correction of Deficiencies (VCD)

01C is the authority on VCDs, and the OPTEVFOR Test Planning Handbook Chapter 11 discusses VCDs in depth and is the authoritative document regarding their execution. From the Test Planning Handbook: "The purpose of a VCD is to confirm correction of deficiencies identified during IOT&E or Follow-on Operational Test and Evaluation (FOT&E). This evaluation applies to only those deficiencies the PM submits as having been corrected (or substantially mitigated). A VCD can occur through OPTEVFOR review and endorsement of corrective actions or, in some cases, through an end-to-end test of the complete system, depending on the complexity of the system and the extent of the corrections. Where retest of deficiencies is required, a VCD can occur as part of a formal FOT&E phase of test or as a specific stand-alone test limited to the verification effort. Stand-alone VCDs focus on deficiencies vice COI resolution. To resolve a COI that was previously evaluated as unsatisfactory or unresolved, a formal FOT&E phase of test is normally required. Typically, when the COI is unresolved or is resolved as unsatisfactory, deficiency(ies) prevented the full evaluation of the mission area, and additional testing beyond that required to address the correction of the deficiency(ies) may be required. However, with proper pre-test coordination and thorough test planning and sufficient resources, a VCD for a non-oversight program may be used to evaluate a previously unresolved COI, or to reevaluate a previously unsatisfactory COI. Stand-alone VCDs will use a test plan, produced using the test planning

process described in section 5, to guide the execution of the VCD. For programs on DOT&E oversight, the signed VCD test plan will be provided to DOT&E prior to execution." A VCD requires an OPTEVFOR signed test plan assigned to a phase of test. The WD should be in contact and work closely with their 01C representative during this process. The VCD test plan can be executed by an outside test team, but a Cover Sheet or Memorandum of Agreement signed by OPTEVFOR must be included to cover how the test is to be executed.

The following are the typical steps for the execution of a VCD as it relates to CS:

- WD receives VCD request in writing from the developing agency identifying specific deficiency(ies) that have been corrected
- WD with support from support competencies will determine testing requirements to ensure whether specific deficiency(ies) have been corrected or mitigated, and determine whether regression testing is required
- Draft the VCD test plan to include the following for EACH deficiency identified in the VCD request:
    - The deficiency(ies) to be evaluated
    - Cause and corrective action taken
    - Scope of VCD (number of days, regression testing, and other logistical concerns)
    - Test methodology (where appropriate, reference vignettes or test events from the previously approved OT plan or the IEF; describe any newly constructed vignettes)
- WD reviews and signs VCD test plan. Programs under DOT&E oversight must brief the test plan to the OPTEVFOR Director and a signed copy of the test plan will be forwarded to DOT&E prior to collecting VCD data

It is important to note that the conduct of a cyber VCD will not change a system from "Not Cyber Survivable" to "Cyber Survivable". It is recommended that the OTD, PMO, and the assigned 01D EA discuss VCD efforts prior to establishing a formal VCD request.

5.13.4 - Cyber Level of Test Determination

01B is the authority on conducting LTDs, and the LTD process is described in more depth in the OTE Manual. The LTD process may be used to assist in determining exactly what must be tested and how much testing is needed. The outcomes of an LTD can be: no OT, observation of DT by OT personnel, or formal OT. The WD will gather and scope information to be discussed with 01D support and be provided to the 01D Director for concurrence prior to the LTD decision meeting.

LTD considerations are like those of MBTD, and the following information must be considered:

- New or enhanced SUT capabilities
    - Example: The SUT was a missile that was previously designed for surface-to-air engagements has been modified to support a warhead for surface-to-surface engagements
- Hardware/Software configuration changes

    - Example: A computer system that upgraded from Windows 10 to Windows 11 might have a different set of vulnerabilities
- Changes in accessibility
    - Example: Changes to program policy that allow additional personnel access to the SUT for maintenance purposes, or a change in physical location of the SUT
- Previous testing
- CS testing already completed
- Future CS testing of the SUT

SECTION 6 - TEST EXECUTION

01D is responsible for coordinating execution resources to ensure OPTEVFOR follows DoD and DON policies and processes especially when it comes to red team operations due to real-world implications per *DoD Cyber Operational Test and Evaluation Guidebook, February 2025*. This includes coordination with DoD red teams, test teams, and external organizations for augmentation support. Augmentation may be required to deconflict OPTEV-RT's schedule or to partner with an external organization to conduct non-traditional tests such as radio frequency, hull, mechanical & electrical systems, and cross domain solution. The OPTEV-RT is authorized by the Navy Authorizing Official (NAO) to operate on Navy operational environments up to Top Secret (TS)/GENSER. However, the OPTEV-RT is limited to local, on-site testing (CVPA and AA) until 01D builds and accredits the necessary remote infrastructure. When applicable, 01D will coordinate the remote test execution support with another DoD Red Team organization that has both the NSA red team certification and NAO authorization. Without the credentials/authorization, an organization cannot conduct remote adversarial/red team activities on Navy operational environments. For TS/Sensitive Compartmented Information (TS/SCI) networks/systems, augmenting red teams must have NAVINTEL Designated Authorizing Official (DAO) authorization. The OPTEV-RT has authorization from the NAVINTEL DAO.

6.1 - FUNDING REQUIREMENTS

Cyber test execution and reporting are funded by the SUT PMO according to the TEMP and detailed in the test execution IGCE. OPTEV-RT is composed of a primarily contracted workforce (prime contractor with multiple sub-contractors). To ensure contractual requirements are met **funding for test execution must be delivered to Fleet Logistic Center Norfolk no later than 45 days prior to start of test.** Failure to have the funding delivered on time incurs a risk of test cancellation by 01D due to an inability to support contractor travel requirements.

6.2 - PRE-TEST BRIEF AND COORDINATION VISIT

The pretest brief and coordination visit takes place on the test asset approximately thirty days prior to test. Occasionally asset availability will force this visit just a few days prior to test execution. The pretest brief and coordination visit has four major objectives. First meet with site personnel, operators, subject matter experts and any other key individuals to discuss the upcoming test event. Second, the OPTEV-RT Lead will present the pretest brief to site personnel to outline expectations. Third, is to resolve any outstanding concerns of stakeholders. Concerns are often brought up for the first time during this visit. Finally, OPTEV-RT will review logistical information with the site and resolve any deltas for the test event. The logistical information OPTEVFOR Red Team will be looking for (but not limited to) items such as:

- Places to plug in
- Cable runs
- Work areas (Classified and unclassified)
- Logistics for getting equipment in and out of the test area
- Storage and command specific guidance for classified data

- Power
- Incident handling

6.3 - COOPERATIVE VULNERABILITY AND PENETRATION ASSESSMENT (CVPA)

The CVPA is a cooperative evaluation of the system's vulnerabilities in an operational context and provides reconnaissance of the system in support of the AA. The CVPA must be executed with full system access and in collaboration with the system SMEs funded by the program office. The OPTEV-RT or another qualified organization designated by 01D attempts to discover system vulnerabilities that impact the system's mission capabilities and the results support development of AA attacker storyboards. The CVPA is fully informed and supported by system owners, operators, and system engineering experts. The CVPA data supports the evaluation of the system's "prevent" capabilities within the PMRA construct.

The CVPA must be conducted in an operationally representative environment to reflect the system's intended operational environment. Ideally, CVPA and AA are conducted on the same test asset to avoid additional cost and increase in AA schedule. If circumstances make this infeasible, it may be required/desired to conduct parts of the test or the entire CVPA at Land-Based Test Site (LBTS) or labs. Such concessions are subject to the M&S accreditation policies conveyed by OPTEVFORINST 5000.1C and section 2 of this handbook. Historically, non-operational environments and test assets have increased the amount of time required to execute the follow-on AA period in an operational environment, because additional time is required to validate CVPA findings to ensure sufficient data was collected prior to the AA. The WD and 01D collaborate to determine the requirements for use of LBTS or labs during test strategy discussions. Once determined, the effort is coordinated with 01B and 01D as described in section 2 of this handbook and should be accomplished prior to CP-0.

6.4 - ADVERSARIAL ASSESSMENT (AA)

The AA evaluates a system's resiliency against cyber-attacks in an operational context by using realistic threat exploitation techniques in the system's intended operational environment. There are few exceptions to conducting this testing outside of the operational environment. Information gained during the CVPA is used to develop AA attacker storyboards, which portray adversarial threats from insider, nearsider, and outsider perspectives. In addition to the system's PMRA capabilities from both the system and operator perspective will be observed within the PMRA construct during an AA.

6.5 - EXECUTION METHODOLOGY

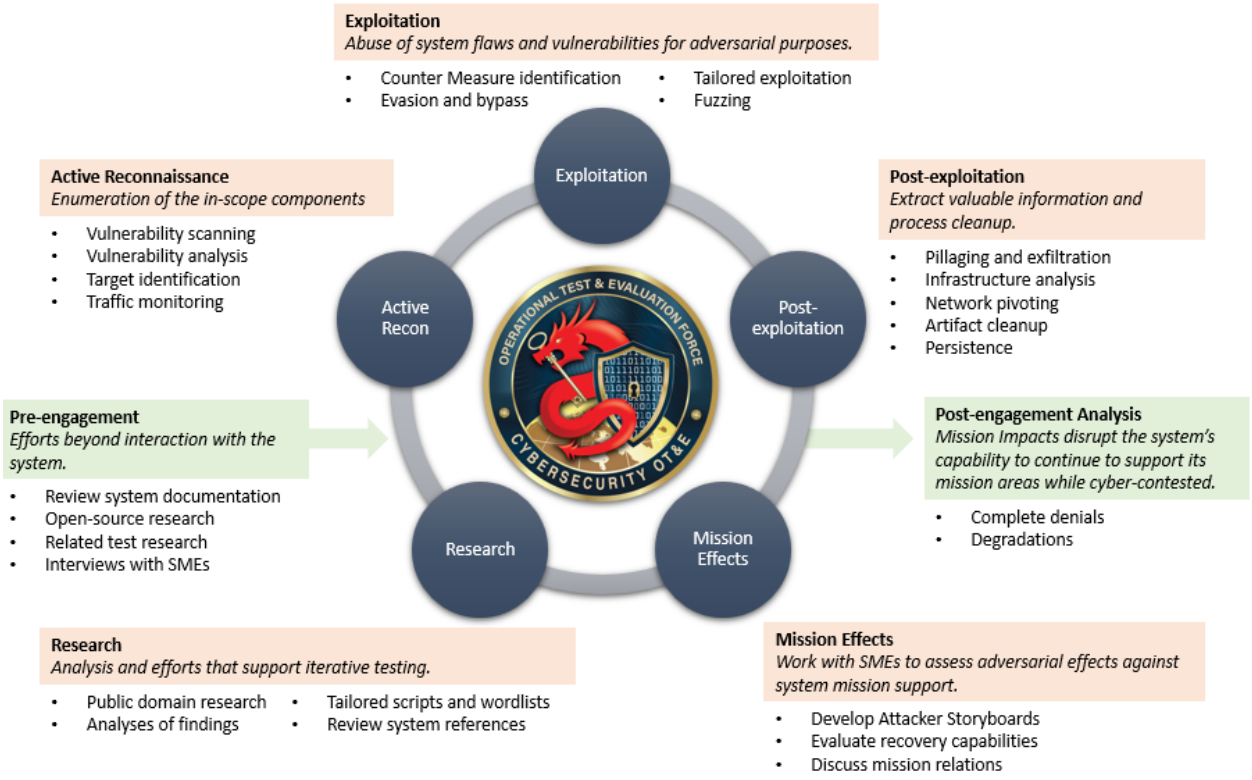
The OPTEV-RT conducts cybersecurity testing using a four-stage methodology: reconnaissance, scanning, exploitation, and post-exploitation. The result of this test cycle is mission impact, an effect that denies or degrades the system's capability to conduct its mission. Figure 6-1 provides a visualization of the methodology. The cyber test plan development process supports the research stage of the execution cycle for the OPTEV-RT.

During test execution, the OTD shall:

- Coordinate SME support on-site during scheduled test periods

- Collect data requirements during the execution of storyboards
- Oversee visitor control
- Oversee data collection, finalization, and reporting
- Review classification of data gathered during the test in accordance with applicable SCGs
- Oversee couriering or shipment of classified data to and from the test site
- Support OPTEV-RT or other executing organizations' Team Lead

Figure 6-1 Execution Cycle



Aspects of Figure 6-1 are described below:

- Pre-engagement: Efforts that take place prior to test, and prior to each day of testing, that typically do not involve working with the SUT.
- Active Reconnaissance: Exploration and enumeration of the available testing environment, to discern the cyber surface area and evaluate vulnerable targets.
- Exploitation: Targeted attacks to leverage or discover vulnerabilities, that include cooperative efforts with SMEs.
- Post-exploitation: Extract valuable information, maintain control of the machine for later use, and gain access to additional networks.
- Post-engagement Analysis: Reviewing and documenting the results of the engagement.
- Mission Effects: Working with the SME to develop attacker storyboards, evaluate recovery capabilities, and develop mission relations.
- Research: Efforts that take place each day of test, typically after-hours, that support ongoing test efforts.

SECTION 7 - POST-TEST PROCESS

The purpose of the cyber survivability Post-Test Iterative Process (PTIP) for IOT&E and FOT&E is to determine the cyber survivability of a SUT. Cyber survivability PTIP functions differently from effectiveness and suitability PTIP in that 01D leads the PTIP process until product turnover to the WD after the CEWG. The OTD and OPTEV-RT Lead will coordinate and manage the PTIP POA&M, ensuring enough time for test data shipping and uploading, internal 01D reviews, and the routine PTIP milestones.

The OTD has many responsibilities in the cyber survivability PTIP process including:

- Integration of cyber survivability products into the final report
- Generation of mission relation for deficiencies
- Generation of the content for the Director's letter
- Verify that the post-test documents are classified to the appropriate level according to applicable SCGs with concurrence from the cognizant OCA(s)

The OTD is encouraged to seek 01D support in test report finalization to ensure technical accuracy is maintained and consistent reporting is achieved across OPTEVFOR cyber survivability T&E reports.

7.1 - DATA RETURN

The post-test process begins when data is returned to OPTEVFOR and is uploaded to an IT system. If the test data is collateral Secret or below, the post-test products will be generated on OPTEVFOR's CLASS-NET. If the test data contains Sensitive Compartmented Information (SCI) or is TS, the post-test products will be generated on an 01D laptop. The entire PTIP process is more cumbersome when dealing with TS or SCI data; delays should be expected.

7.2 - CYBER SURVIVABILITY DATA SCORING BOARD

The purpose of the Cyber Survivability data scoring board is to qualify the data collected for OT. The scoring board should be completed within 30 days of data upload for system level tests, and 45 days for platform level efforts. Specific outcomes of the scoring board are (1) verify all data requirements were collected, (2) identify deviations to test, and (3) identify limitations to test. The OPTEV-RT Lead will lead execution of the scoring board.

7.3 - DELIVERY OF TEST DATA TO DOT&E

OPTEVFOR is responsible for supplying DOT&E with the data requirements defined in the *DoD Cyber Operational Test and Evaluation Guidebook, February 2025.* Data will be provided as soon as practical, but within 30 days of the completion of the applicable test event. The primary method for sharing Secret data is the 01D SharePoint on SIPRNet. For TS/SCI data, alternate arrangements will be made to transmit data via JWICS.

7.4 - 01D REVIEW BOARD

The 01D review board is an internal meeting with the 01D Director and/or Deputy to vet the draft report products for technical accuracy and consistency with 01D policy and is not part of the standard PTIP process. This meeting ensures the 01D Director concurs with the themes of the products prior to the System Evaluation Review Board (SERB) and alleviates potential re-work.

Due to the technical scrutiny established during the 01D review board, this review could result in significant changes to the draft report products; therefore, draft report products should not be distributed to external stakeholders until after the 01D review board has been completed.

For tests that are fully outsourced to other testing organizations the OTD will be responsible for conducting an 01D review board to ensure products meet quality standards.

7.5 - COI EVALUATION WORKING GROUP

The CEWG is intended to be a comprehensive review of each Cyber Survivability COI, including data analysis, deficiency sheets, and results paragraph. This is an iterative process and may take more than one meeting to accomplish.

Once the 01D Director approves the draft documents after the 01D review board, The OPTEV-RT Lead will provide drafts of the DAS, deficiency sheets, and results paragraph to the OTD two business days in advance of the first meeting.

The DAS, deficiency sheets, and results paragraph inputs brought to the CEWG by 01D are not final products. The OTD is responsible for incorporating the cyber inputs into the overarching final report products. The products initially brought to the CEWG by 01D will require WD input to the following sections:

- DAS:
    - Resources Table
- Deficiency Sheets:
    - Deficiency Numbering
    - Severity
    - Mission Relation
    - Conclusion
- Results Paragraph:
    - Cyber Survivability COI paragraphs
    - Deficiency Table

Up to this point, the OPTEV-RT Lead has maintained configuration control of the draft report products. The draft report products will be turned over to the WD upon completion of the CEWG. After the CEWG, the primary point of contact in 01D for the report will be the EA. Any changes to the technical meaning of the products will need to be reviewed by the 01D Director prior to the SERB. The OTD is also responsible for drafting the Director's letter, including the Cyber

Survivability paragraph. 01D encourages collaboration in this process and will support reviewing these products prior to the SERB.

7.5.1 - Cyber Survivability Deficiency

Cyber survivability deficiencies are unlike traditional effectiveness and suitability deficiencies which focus on a singular problem that causes a mission impact. The ability to impact a mission from a cyber warfare perspective typically requires multiple weaknesses or vulnerabilities to be chained together by an adversary. Therefore, 01D defines a cyber survivability deficiency as a weakness or chain of weaknesses that would allow an adversary to achieve mission impacts from a specific foothold.

Note: There is common confusion surrounding deficiencies and their relation to attacker storyboards executed during the AA. Attacker storyboards may only be executed for a subset of possible attack chains articulated in deficiency sheets to collect mitigate and recover data of the SUT under denial or degradation of a mission. Often, the mission impacts observed during AA may not be as severe as what is described in deficiency sheets because the OPTEV-RT will not engage in destructive testing.

Severity of Cyber Survivability deficiencies are determined in accordance with the OPTEVFOR Test Reporting Handbook, with additional considerations. Additional considerations for cyber survivability deficiency severity include, but are not limited to, the following:

- Physical Access – What, if any, layers of physical security would an adversary have to go through to achieve the same type of effect demonstrated on test?
- Credentials Required – Does the adversary require special credentials to achieve the level of access necessary? If vendor default credentials were used, are they publicly available? Was the password otherwise easily guessable (e.g., 1qaz2wsx!QAZ@WSX)?
- Knowledge Required – Would this attack require specialized knowledge of the target, or general operating system or service knowledge?
- Technical Complexity – Would this attack require custom development, or does it use publicly available code?
- White-carded Assumptions – What was white-carded while on test in relation to adversarial capabilities?

These items support severity determinations as they are related to credible enemy courses of action when weighed against the mission impact observed on test and the associated level of exploitation necessary.

7.6 - SYSTEM EVALUATION REVIEW BOARD (SERB)

The purpose of the SERB is for the 01D and WD Directors to review the PTIP products prior to presentation to the Director. The OTD should invite the 01DA, 01DB, 01D Operations Officer, EA, OPTEV-RT Lead, and OPTEV-RT Chief to support technical discussions at the SERB.

7.7 - EXECUTIVE SYSTEM EVALUATION REVIEW BOARD (E-SERB)

The purpose of the E-SERB is to inform the Director concerning SUT and SoS issues, COI assessment/resolution, overall conclusions, associated recommendations, and to gain the Director's concurrence on the same. The OTD should invite 01DA, 01DB, EA, and OPTEV-RT Chief to support technical discussions at the E-SERB.

APPENDIX A - ACRONYMS AND ABBREVIATIONS

AA	Adversarial Assessment
AO	Action Officer
APM	Assistant Program Manager
AT	Accelerator Team
CCB	Critical Components Breakdown
CEWG	COI Evaluation Working Group
COI	Critical Operational Issue
COTB	Concept of Test Brief
COTS	Commercial Off-the-Shelf
CP	Checkpoint
CPI	Critical Program Information
CRM	Comment Resolution Matrix
CS	Cyber Survivability
CSA	Cyber Survivability Attribute
CSEIG	Cyber Survivability Endorsement Implementation Guide
CTT	Cyber Table Top
CVPA	Cooperative Vulnerability and Penetration Assessment
DAO	Designated Authorizing Official
DAS	Data Analysis Summary
DMOT	Detailed Method of Test
DoD	Department of Defense
DoDI	DoD Instruction

DoDM	DoD Manual
DON	Department of the Navy
DOT&E	Director, Operational Test & Evaluation
DT	Developmental Testing
DT&E	Developmental Testing & Evaluation
E-SERB	Executive System Evaluation Review Board
EA	Exploitation Analyst
EOA	Early Operational Assessment
FOT&E	Follow-on Operational Test & Evaluation
IDS	Intrusion Detection System
IEF	Integrated Evaluation Framework
IGCE	Independent Government Cost Estimate
IOT&E	Initial Operational Test and Evaluation
IPS	Intrusion Prevention System
ISP	Information Support Plan
JCIDS	Joint Capabilities Integration and Development System
KPP	Key Performance Parameter
LBTS	Land-Based Test Site
LTD	Level of Test Determination
M&S	Modeling and Simulation
MBTD	Mission-Based Test Design
MCSFM	Mission Critical Software Function Matrix
MCSM	Mission Critical Subsystem Matrix
MTS	Master Test Strategy

NAO	Navy Authorizing Official
NSA	National Security Agency
OA	Operational Assessment
OCA	Original Classification Authority
OPTEVFOR	Operational Test and Evaluation Force
OT	Operational Test
OPTEV-RT	Operational Test and Evaluation Force Red Team
OT&E	Operational Test and Evaluation
OTA	Operational Test Agency
OTC	Operational Test Coordinator
OTD	Operational Test Director
PM	Program Manager
PMO	Program Management Office
PMRA	Prevent, Mitigate, Recover, and Adapt
PMT	Platform Mission Task
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPA	Program Protection Analysis
PPP	Program Protection Plan
PTIP	Post-Test Iterative Process
QRA	Quick Reaction Assessment
SCG	Security Classification Guide
SEP	System Engineering Plan
SERB	System Evaluation Review Board

SME	Subject Matter Expert
SoS	System of Systems
SS	System Survivability
SUT	System Under Test
T&E	Test and Evaluation
TEMP	Test and Evaluation Master Plan
TP	Test Plan
TS	Top Secret
TS/SCI	TS/Sensitive Compartmentalized Information
TTP	Tactics, Techniques, and Procedures
USB	Universal Serial Bus
V&V	Verification and Validation
VCD	Verification of Correction of Deficiencies
VOLT	Validated Online Lifecycle Threat
WD	Warfare Division
WIPT	Working Integrated Product Team