Cyber Survivability Test and Evaluation Handbook

Version 3.0

06 Dec 2022

COSTELLO.EUGENE.D.1016366478

Digitally signed by COSTELLO.EUGENE.D.1016366478
Date: 2022.12.06 13:42:18 -05'00'

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

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, and stored.

In the role as OPTEVFOR's cyber competency, the 01D cybersecurity division supports all aspects of the cybersecurity operational test and evaluation across all OPTEVFOR warfare divisions 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, execution, and reporting that communicate the System Under Test (SUT) prevent, mitigate and recover capabilities. When followed, this methodology provides the warfighter and acquisition stakeholders a solid understanding of the limitations and risk 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 their particular program, working in collaboration with program offices, Warfare Division (WD) leadership, and OPTEVFOR competencies.

1.2 - POLICIES AND GUIDANCE

The requirement for OPTEVFOR to conduct cyber Operational Test and Evaluation (OT&E) derives 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 and Evaluation Guidebook v2.0, April 2018
- Director, Operational Test & Evaluation (DOT&E) Memo, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs," 03 April 2018
- Cyber Survivability Endorsement Implementation Guide, January 2017
- 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. 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 conducted in connection with the acquisition and procurement of naval weapons and warfare support systems. It prescribes policies for the planning, conduct, 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 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 cybersecurity, 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 with the final two phases (five and six) being the Operational Test (OT) led Cooperative Vulnerability and Penetration Assessment (CVPA) and Adversarial Assessment (AA) periods.

1.2.4 - DOT&E Memo, 03 April 2018

Director Operational Test and Evaluation (DOT&E) published the updated "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs" memorandum in April 2018. This memo directs an Operational Test Agency (OTA) to conduct cybersecurity CVPA and AA events for their respective service's acquisition programs on DOT&E oversight. The OPTEVFOR cyber survivability planning process aligns to the requirements of this memo. This memo requires the collection of data and analysis of a system's capability to:

- Prevent cyber attacks
- Mitigate the effects of a cyber-attack
- Maintain a mission capability
- Recover lost mission capabilities to support follow-on mission requirements in a tactically relevant timeframe.

This construct is referred to as Prevent, Mitigate, and Recover (PMR).

1.2.5 - Cyber Survivability Endorsement Implementation Guide (CSEIG), January 2017

The Joint Capabilities Integration and Development System (JCIDS) Manual was updated on 18 December 2014 to add non-kinetic effects as a key element of the mandatory System Survivability (SS) Key Performance Parameter (KPP). The CSEIG took the defined JCIDS SS KPP pillars of susceptibility, vulnerability, and resiliency and transformed them into prevent, mitigate, and recover pillars, respectively. Those cyber survivability pillars became the PMR construct for OPTEVFOR's cyber survivability evaluation. The CSEIG defines Cyber Survivability Attributes (CSAs) that are traced back to the PMR pillars. The intent of the CSAs are 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 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 should be included as part of the evaluation to determine if a system is meeting its requirements.

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

DoDI 5000.02 describes the integration of Cyber Security T&E into the acquisition structure and through the system lifecycle. It further clarifies the roles of OPTEVFOR (see section 5.2) 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 in order to meet policy and stakeholder requirements.

1.3.1 - When Cyber OT&E is Required

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 planned and executed meets the necessary reporting requirements and their needs.

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 for the program. Testing scope may range from a full PMR 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. In an effort to ensure minimally adequate testing is conducted at an affordable cost to meet stakeholder requirements, the following considerations are provided in order 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," consider not re-testing the system. If the system had been evaluated as "Not Cyber Survivable", the result carries forward.

- 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 & 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. In the event that 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 operational test 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 it should be coordinated with all stakeholders including 01D.
- When external barriers to an adequate cyber evaluation are identified, and prior to external coordination, the WD and 01D should work together to establish a strategy for satisfying OPTEVFOR's test requirements. 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.

- For programs with no previous cyber survivability OT&E, full IOT&E planning and execution is required.
- Ensure scheduling is completed in sufficient time to support test execution. See section 6.2 for further details.

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

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 full scope 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 "go back" and 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 result in resources being unnecessarily expended validating the vulnerability and creates challenges for follow-on testing in the operational environment due to 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 the 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 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 should be conducted in an operationally representative environment that includes the system operators and technicians. Operational Test Directors (OTDs) and Cyber Test Engineers (CTEs) should 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 Warfare Division 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, an intended use could provide for conducting a risk reduction event to assess the test team's tactics, techniques and procedures 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 substituting 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 system's PMR capabilities includes assessing how well system operators and technicians are able to maintain and recover lost mission capabilities in a cyber-contested environment. Lab and cyber range testing introduce artificiality that makes 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 PMR capabilities and make a cyber survivability determination.

The OTD should 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 warfare division to determine the viability of M&S as part of a programs 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. For cyber M&S, the acceptability criteria is how "wide" the deltas between the cyber M&S configuration / environment and the fielded system can be while still supporting the cyber test objectives. This comparison will identify differences in the following:

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

The PMO will provide a Verification & Validation (V&V) Plan and report for the deltas above. At a minimum, the V&V report should 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 SUTs 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 SUTs 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 (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 should depict the side by side comparison of the modeled environment and the fielded system in order 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 in order 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 the environment and fielded system and follow-on test events are not scheduled, then the limitation should be at least "major".

2.6 - OTD RESPONSIBILITIES

The OTD is responsible to ensure the CTE or designated warfare division 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, the OTD is responsible to ensure the CTE or designated warfare division 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 SURVIVABILITIY 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 located here: Y:\OT&E Production Library\IEF. The majority of this section contains content from the OTD IEF Checklist and IEF Template modified to suit cyber survivability testing. The OTD should meet with their divisional 01D Lead Cyber Analyst (LCA) to provide a basic familiarization of the SUT to ensure that 01D has the requisite information to support test design, and so the OTD and test team understand what is expected for the cyber security portion of the IEF. The CTE or WD will develop the initial cyber security related inputs, working with 01D for clarification and review.

01D should 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 (COI's) 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

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 no associated defense exists to be paired with a threat, then an acknowledgement must be made that the associated defense does not exist and include a statement saying the SUT is limited in its capability to prevent, mitigate and recover losses to a mission capability resulting from 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 most current IEF Template.

3.2 - IEF CYBER CRITICAL COMPONENT SELECTION

The Mission Based Test Design (MBTD) process identifies the mission areas and makes 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 is 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, similar to the Critical Components Breakdown 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

This paragraph contains critical information for cyber OT planning. 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 divided between information available prior to IEF signature from information still required. 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

The CS 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 (DRs) 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 or 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 SURVIVABLITY 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 in order 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 details are 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 the program office funding 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 warfare division CTEs are contractors funded by individual program office, cost estimate for the overall test planning support by the CTEs is required. Using the estimated costs, the OTD should ensure the PMO includes the cyber OT&E resource requirements in their 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 testing 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 warfare division to outline the required contractor man-hours, test team travel funding, and funding delivery instructions. The 01D IGCE is discussed further in section five. 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 to be forwarded to the PMO for future OT&E funding.

An IEF creation, Tailored Integrated Evaluation Framework 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 development because he or she may be limited by the availability of a CTE 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 CTE 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 warfare division 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 particular system

under test. 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 intending to conduct, and what information needs to be produced and provided back to the PMO in order to adequately and accurately detail the cyber survivability OT strategy. For further information on TEMP development, please refer to the OT&E Manual

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 effort 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 5.4.2 of this handbook as TEMP content in order to enable the OTD, CTE (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, warfare division, 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 restore 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, do they intend to have the range/lab environment accredited by OPTEVFOR (required for use in OT)
    - Will OPTEVFOR be provided the ability to review and comment on the test plans being executed for DT led 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 to becoming a test limitation
        - What test tools and capabilities are required (if beyond what the OPTEVFOR Red Team already provides such as non IP testing and or specialized considerations)
        - What data from Developmental Test and Evaluation (DT&E) is planned 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 OPTEVFOR Red Team 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 OPTEVFOR Red Team 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 surveys)
    - 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 LCA within 01D for review of the potential test strategy and to assist with identifying resourcing deficiencies. All 01D comments should be adjudicated prior to the subsequent TEMP review stages. The OTD is expected to provide a comment resolution matrix along with the TEMP for 01D review.

4.2 - O-6 REVIEW

This stage of the TEMP review will formally capture all TEMP stakeholder's 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 Comment Resolution Matrix (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 comment resolution matrix along with the TEMP for 01D review

This stage of TEMP review may lead to additional comment adjudication working groups in order 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 are dealing 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 has 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 O6 review stage have been correctly incorporated
- Ensure the test resourcing is accurate and up to date

When routing the TEMP through the iBOSS, the OTD is not required to select 01D if all critical comments have been adjudicated. However, the OTD should provide a brief status e-mail to their LCA 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 LCA within 01D to arrange for a follow-on discussion of the current status of the TEMP.

SECTION 5 - CYBER SURVIVABILITY TEST PLANNING

OPTEVFOR 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 CTE shall implement the test planning process outlined in the following sections ensuring 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.

5.1 - MISSION EFFECT TEST AND ANALYSIS

The cyber survivability 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 nine 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 early start 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 LCAs provide process oversight to the assigned OTD who is responsible for the management and execution of the test planning process.

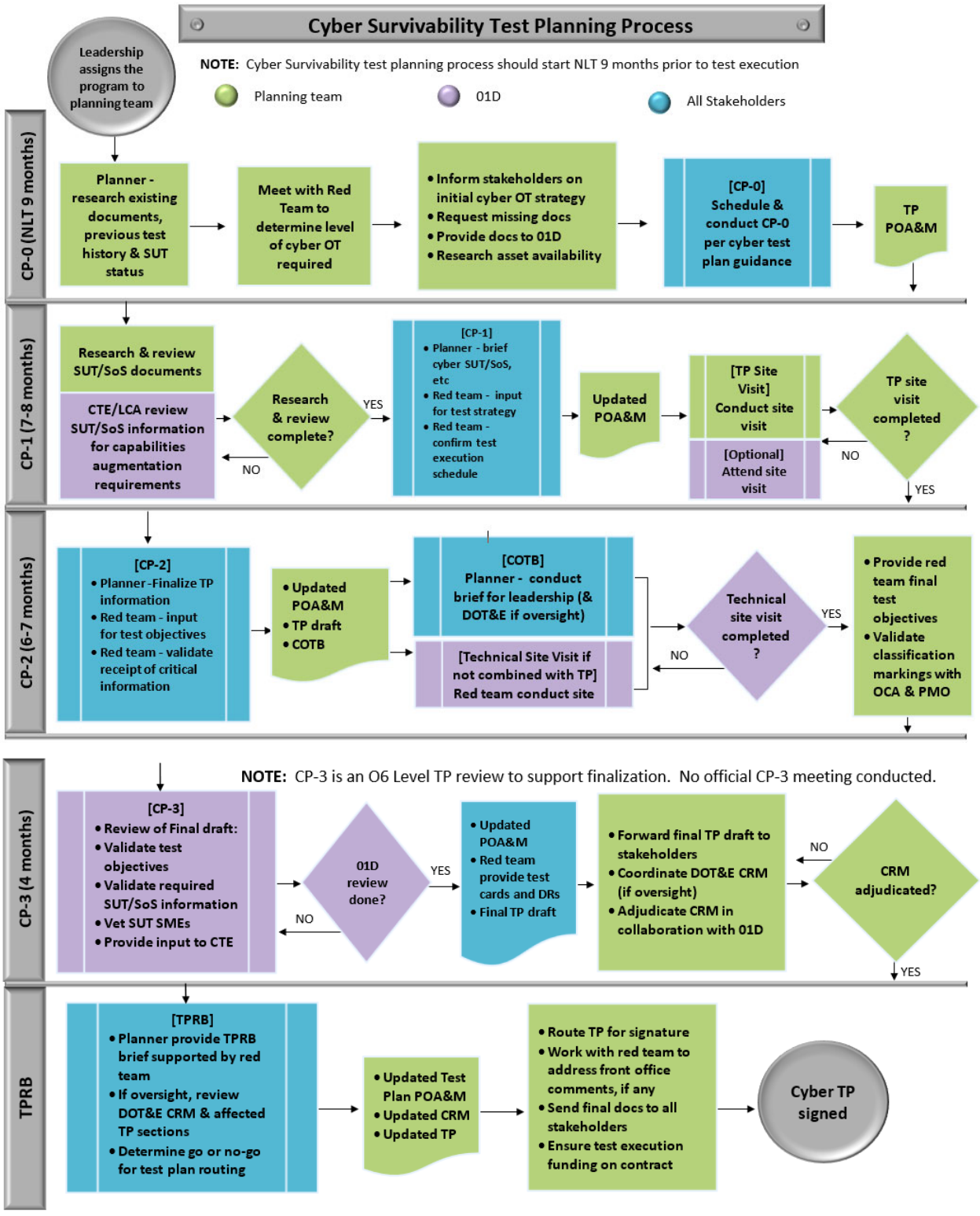
Each cyber T&E test planning milestone is called a Checkpoint (CP) and it represents the maturity level of the planning process up to a point in time. Some CPs culminate in a stakeholder brief/review while others culminate when all necessary stakeholders concur that the necessary exit criteria have been 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 OPTEVFOR Red Team 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 CTE'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 and classified sharedrive Y:\OT&E Production Library\Test Plan and DCP\Cyber Survivability Test Plan folder. 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 OPTEVFOR Red Team 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 are provided in table 5-1 below.

Table 5-1 Roles and Responsibilities Overview

01D	Warfare Division
• Provide process, templates & tools for test planning • Lead Change Control Board to incorporate lessons learned • Provide guidance for overall test planning & checkpoint (CP) processes • Participate as a subject matter expert and a stakeholder • Collaborate and support 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 support for test execution • Provide OPTEVFOR Red Team review and input for attack surface, vectors, test objectives, data requirements and test cards • Provide resource requirements for test execution • Provide technical support for system/component off-limits discussions • Conduct technical site visit and provide input for Test Plan (TP) • Support DOT&E Comment Resolution Matrix (CRM) adjudication • Coordination with external entities with respect to red team resources and capabilities	• Lead test plan generation following the cyber survivability test planning process • Use OPTEVFOR published cyber templates and products • Warfare Division (WD) Cyber Test Engineer (CTE) lead/complete CPs, generate Plan of Action and Milestones (POA&M), and write TP • CTE collaborate with 01D to determine cyber OT strategy • CTE communicate & inform Operational Test Coordinator (OTC) / Operational Test Director (OTD) and WD leadership on schedule and status • (If applicable) Collaborate with augmenting organization during test planning process • CTE coordinate/incorporate 01D input for TP • CTE conduct TP site visit • CTE leads system/component off-limits discussion and finalization • OTC/D lead Concept of Test Brief (COTB) • Route final TP for signature. • Lead DOT&E CRM adjudication • Version control of test products post COI Evaluation Working Group (CEWG) and getting concurrence from 01D regarding technical changes to the same

5.3 - OFF-LIMITS, OUT OF SCOPE 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 authorities 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 their responsibility to execute the testing. 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.** 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 will need to be referenced with specific detail in the TEMP/MTS. There are four main justifications supporting an off-limits declaration:

- Effects to real world operations (data spillage, interruption of services, etc.)
- Loss of life or personnel injury
- Irrecoverable effects to system or component (kinetic and non-kinetic)
- Damage or destruction of surrounding environment

The proper authority shall provide the CTE 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 or items that are "one of" or obsolete should not be the sole reason for an off-limits designation. For efficiency, a digitally signed e-mail from a government authority is sufficient to count as a formal declaration. During test planning, the CTE is responsible to coordinate 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.

Out of scope means that the system or component is not targeted for exploitation during the test and no data is required to be collected off of stated system/component. However, it may still be involved during the conduct of the testing as it may facilitate access, persistence, and/or lateral movement during test. Designating a system/component out of scope does not require a test limitation as it is not foreseen to cause an impact to making the cyber survivability determination. Common reasons a system is designated out of scope are:

- The system has been previously tested and not changed
- It is a SoS component
- It is not evaluated as a critical aspect of the system's mission relevant cyber terrain

A test limitation is necessary if data collection requirements are unable to be met for a particular part of the test in order 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 - 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 in order 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 CTE 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, CTE, 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.

5.4.1 - NLT 9 Months Prior To Test

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 CTE(s) or an Accelerator team (AT), however the OTD/OTC retains overall responsibility. The cyber AT is available for use in situations where a WD does not have CTE support available during MBTD for initial system research and analysis or in cases where test planning needs to begin and CTE support is unavailable. For test planning support, the cyber AT is limited to providing support up to a Check Point 0 (CP-0) milestone. Any support requirements beyond CP-0 would need to be coordinated through 01D. The OTD shall:

- Notify 01D Operations Officer of upcoming testing requirements to provide the following information so 01D support personnel can be designated:
  - System name and Test and Evaluation Identification Number (TEIN), if known
  - Dates for planned testing, if known. Coordinate with 01D for level of effort determination and test duration
  - Type of support requested such as, but not limited to, IOT&E, OA,

    and DT Assists
  - Amplifying info or additional support being requested
- Review latest OPTEVFOR published cyber templates available in the Y:\OT&E Production Library\Test Plan and DCP\Cyber Survivability Test Plan folders on OPTEVFOR's unclassified and classified network share drives
- Identify asset availability with program management office
- Begin gathering the information needed for test planning, including compiling a list of contact information program stakeholders
- In collaboration with 01D, identify if there is a need for augmentation of OPTEVFOR Red Team
- Check availability of the OPTEVFOR Red Team to support the projected test schedule (schedule will be confirmed by 01D)

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

5.4.2 - 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-checkpoint engagements, the CTE 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 CTE may have additional requirements for information. When it is not possible to get all the information in the below list, the CTE and 01D should work together to determine if the level of documentation is sufficient to proceed with testing. This determination will be made at CP-0 and updated at CP-1. CTE will document the missing information on the respective checkpoint templates and meeting minutes.

- Detailed network architecture documentation (Note: This also pertains to all sub-systems within the SUT):
  - Data flows
  - Physical and logical connections
  - External Interfaces
  - Virtual LAN configurations
  - Intrusion Detection Systems (IDS)
  - Intrusion Prevention Systems (IPS)
  - Network demilitarized zones
  - Proxies
- Technical manuals or interactive electronic technical manual
- 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
- Cyber table top 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 Tactics Techniques and Procedures (TTP)
- Classification requirements for cyber survivability test planning, data collection, analysis, and reporting including SoS and subsystems
- Interface Control Documentation (ICD) / Software Interface Descriptions / Software Design Descriptions
- Cross Domain Interface list
- Developmental Test Plans and Results
- Previous OT Test Plans and Results
- System Subject Matter Expert (SME) Point of Contact (POC) Information

When these documents are requested, the CTE should 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, system engineering plan, etc.) should 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 CTE will update the POA&M 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.

5.5 - CHECKPOINT 0 (CP-0)

5.5.1 - CP-0 Preparation

Approximately two to three months prior to the expected date of Checkpoint 0, the WD Section Head assigns a CTE or coordinates with 01D to get cyber AT support to begin documentation collection and analysis. If not completed in the pre-test planning phase, the CTE 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 5.4.2. If the documentation does not exist or is not available, the CTE should note this as an area of concern.

The CTE will also meet with the 01D LCA prior to the CP-0 review to determine the level of testing required for the system to inform all internal and external stakeholders and that a consistent approach to cyber T&E is maintained. During the meeting, the CTE will be expected to present a technical overview of the system including SUT and SoS descriptions, system architecture and

interfaces. At the conclusion of this meeting, copies of all available documentation should be provided to 01D for inclusion in the OPTEVFOR Red Team's documentation.

The CTE will have to research test asset availability for both the site visit and the projected test dates. If specific dates are not known, the CTE should estimate the dates as closely as possible to ensure that the OPTEVFOR Red Team has sufficient availability on their execution calendar.

5.5.2 - 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 CTE and OTD as a venue to discuss the focus areas of the subsequent planning effort in order to solicit inputs on test scope resourcing requirements early. The CTE will schedule the CP-0 review. The entrance criteria for CP-0 are below:

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

Insufficient system documentation may not enable an accurate estimate of the final scope of testing and associated OPTEVFOR Red Team level of effort at the CP-0 milestone. In this case, an estimate based on historical data 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 OPTEVFOR Red Team support over what is finally determined later on 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 any need for outside augmentation needed from outside test teams and to continue to work with them and include them in meetings for the entirety of the test planning process if it is determined they are required. Table 5-2 lists the necessary CP-0 attendees.

Table 5-2 CP-0 Attendees

Warfare Division	Director or Deputy Director, OTD or OTC, CTE
01D	Director or Deputy Director, Operations Officer, LCA, 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

- CTE provides an overview of previous cyber test (DT/OT), if any
- CTE reviews documentation requirements and identifies missing documents/information
- CTE provides details on declaring items off-limits in accordance with section 5.3
- CTE provides a documentation delivery timeline required to complete test planning
- Stakeholders review and confirm asset schedule
- 01D Operations Officer discusses the funding requirement for test execution and tentative schedule
- Stakeholders determine if the test plan will be a standalone document or an enclosure
- CTE inquiries about PMO operational risk management and post-test system recertification concerns (if applicable)
- CTE begins discussions with PMO regarding off-limits systems and out of scope components with justifications
- CTE briefs areas of concerns and entrance criteria to CP-1

CP-0 exit criteria are listed as follows:

- CTE finalizes POA&M for rest of test planning milestones
- CTE has pulled current test plan template and begins to tailor content for SUT
- CTE has identified need for augmentation from outside test teams with 01D support

Upon conclusion of CP-0, the 01D LCA 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, bi-directionally, between 01D the WD and any other stakeholder involved. Once comments are resolved, they remain on the CRM for historical purposes. Critical comments left unresolved after 90 days may 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 on in the process. Once CRM has been created, it is the responsibility of the CTE to maintain the CRM. In order for a comment to be considered resolved, all parties involved with the original comment must agree with how the comment was addressed.

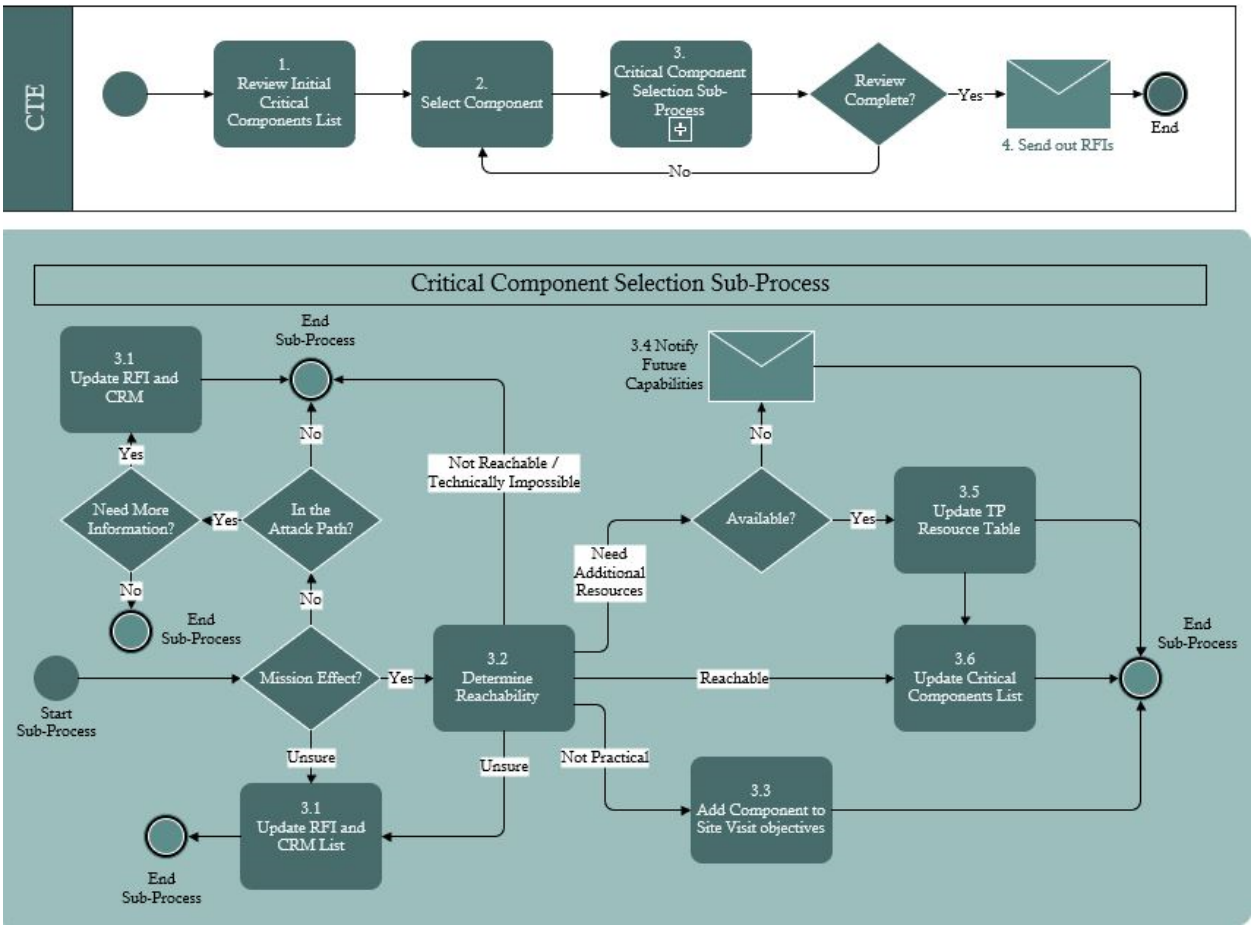
Once approved by the 01D Director or Deputy Director, 01D will provide an initial IGCE for test execution, typically prior to CP-2. The IGCE cannot be provided until a level of test determination has been made. This requires that sufficient information is available to understand the location(s) of the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

5.6 - CHECKPOINT 1 (CP-1)

5.6.1 - CP-1 Preparation

CP-1 is a series of technical interchanges that begin immediately after CP-0, the CTE will begin an in-depth analysis of the SUT using the documentation collected, and begin the critical component identification process laid out in Figure 5-2 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 the CP-0 and CP-1.

Figure 5-2 Mission Critical Component Decision Flow Process



5.6.1.1 - Review Mission Areas

The CTE 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 CTE 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 CTE 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 CTE to enable this critical exchange of knowledge. The CTE 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 Critical Components Breakdown (CCB) spreadsheet provided by the 01D LCA.

5.6.1.2 - 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 CTE 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?

5.6.1.3 - Determine Environmental Cyber Threats

The CTE should 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.

5.6.1.4 - Evaluate the System Architecture

When evaluating the system architecture, the CTE uses 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
- Embedded operating systems
- Ingress and egress routes
- Locations for Critical Program Information (CPI)

The CTE 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.

5.6.1.5 - 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 CTE will develop a list of initial critical components. This list is preliminary because it must be verified at the site visit or through conversation with system subject matter experts. Experience has shown it is invaluable to sit with the subject matter experts 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 LCA. The CTE should work closely with the LCA 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 site visit. Refer to Figure 5-2 above for method of determining critical components.

5.6.1.6 - Determine Interfaces

The CTE should look at interfaces to determine how an attacker could get a foothold on the system to begin working toward reaching the critical components determined 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 CTE must be creative.

Special attention should 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.

5.6.1.7 - Determine Initial Attack Surface and Vectors

Now that the CTE understands the interfaces and the critical components, they can use this information to map the attack path through the system. The attack surface are different places where an adversary can gain an initial foothold. The attack vectors are paths or means by which an adversary can gain access to the critical components.

The CTE 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. The elements on the path that the attack vector traverses, as well as the critical components themselves will be analyzed to determine potential vulnerabilities in the next step.

5.6.1.8 - Determine Countermeasures

In order to adequately assess the mitigate capabilities of the system, the CTE must research and document the inherent countermeasures within the system. 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:

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

5.6.1.9 - Determine Test Planning Site Visit Objectives

Once the mission and environment are understood, the CTE may have additional information requirements. These should be documented as site visit objectives and provided to the site or program office for them to address, with the appropriate personnel, during the test planning site

visit. The site visit should not be ad hoc, it should be a well-organized event that facilitates a technical exchange between representatives from the Fleet, program management office, engineering support, and OPTEVFOR.

Regardless of the additional information required, the CTE must be able to accomplish the following objectives during the 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 solicits inputs from proper authorities
- Discuss pre-test risk reduction events and/or post-test system re-baselining requirements

5.6.1.10 - Test Objectives

Test objectives are a critical piece of the cyber OT&E process and should 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 TTPs. 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 they execute test objectives based on their TTPs, capabilities and their vulnerability discovery. Test objectives are operationally focused and linked to the effectiveness COIs for the associated SUT.

The CTE, with technical support from the LCA and supporting red team members, develops the test objectives based on the technical analysis and exchanges leading up to a Checkpoint 1. 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 a sufficient amount to capture a holistic evaluation based on relevant cyber threats to the system.

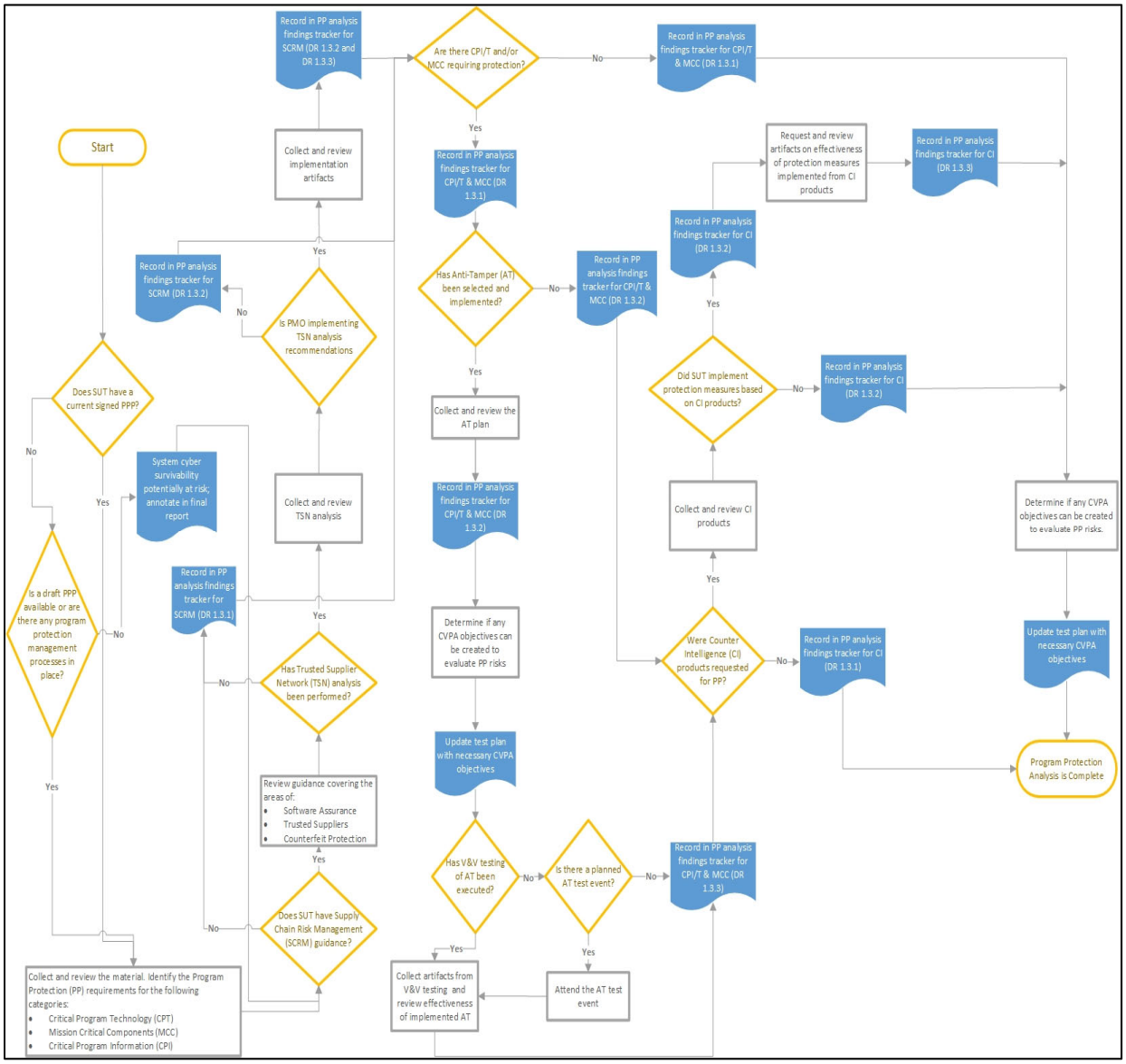
5.6.1.11 - Initial Program Protection Plan (PPP) Analysis

As soon as the CTE receives the PPP, they should begin its analysis. 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 includes implementation guidance for selected countermeasures, and addresses processes and procedures for ensuring countermeasures are implemented and their effectiveness assessed and monitored. 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 Program Protection Analysis (PPA) can be found in Figure 5-3 below. The result of the initial analysis should be documented in the Program Protection Analysis Findings Tracker spreadsheet 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 CTE is responsible for conducting this analysis and providing the data to the OPTEVFOR Red Team test team 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 in order to afford time to address residual risks prior to test execution.

Figure 5-3 Program Protection Analysis Flowchart



5.6.2 - 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 OPS Officer. The entrance criteria for CP-1 are as follows:

- CTE 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)
- CTE begins program protection analysis

CP-1 is an iterative research and analysis process for the CTE to request documentation and review it to determine if it meets the information requirement(s) for test planning. The CTE will lead the discussion for the technical working group session(s) and only schedule these sessions with the 01D LCA and Test Execution team (OPTEVFOR Red Team or augmented) once the research and analysis is complete and the CTE 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 CTE provides the overview of the system architecture, nominated critical components, and the attack surface with an end goal to derive at test objectives and resource requirements for the test team. The CTE 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 CTE 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 CTE needs to be able to "bridge-the-gap" with basic technical competency in order to engage with the selected test teams.
- The CTE needs to be able to understand test team capabilities/requirements and collaborate to develop test objectives that are relevant to critical components from operational perspective and aligned to test duration available to the test team

The CTE 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.

Critical components are essentially recommended "targets" for the test team to try and affect mission; the more critical components selected the more test time required (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 CTE research contained in the Critical Components Breakdown document.

- CP-1 should 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 identifiable initial:
- System attack surface
- Attack vectors
- Off-limits component list
- Test objectives with OPTEVFOR Red Team input
- CTE developed test planning site visit objectives
- CTE updated test planning POA&M as necessary
- CTE coordinates test plan site visit & SME support
- CTE has completed Critical Components Breakdown Spreadsheet

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

5.7 - CHECKPOINT 2 (CP-2)

5.7.1 - CP-2 Preparation

Beginning about 6 months prior to test the CTE will begin final test planning. During this stage, the CTE will have completed the test planning site visit and will have all the information needed to complete the test plan. 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 warfare division 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.

5.7.2 - CP-2 Execution and Closeout

CP-2 occurs after the site visit. The focus of this CP is for the CTE to present the results of the site visit and the new information gained. The CTE will schedule the CP-2 review. The three approved methods to deliver CP-2 briefs to meet the program's needs are:

- Electronically via email
- Formal brief in person or virtual
- In conjunction with TP-B or COTB

The entrance criteria for CP-2 is as follows:

- CTE completed TP site visit and collects remaining system information

- CTE engages with test team(s) to update scope of test based on the site visit and additional information received
    - Prioritized critical components
    - Finalized test objectives
    - Final off-limits components w/ PMO SME inputs
    - Finalized test limitations
- CTE has satisfactorily completed their PPA

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

Table 5-3 CP-2 Attendees

Warfare Division	Director or Deputy Director, OTD or OTC, CTE
01D	Director or Deputy Director, LCA, 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:

- CTE provided program/vendor SME(s) POC information
- 01D OPS confirmed receipt of pertinent SUT/SoS information (examples: off limits list, IP addresses, Virtual Local Area Networks (VLAN)s, etc.)
- 01D OPS 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 OPS schedules technical site survey and/or risk reduction event (if applicable)
- CTE continues to work on completing the TP with information from previous CPs

- CTE support OTC/D to create COTB

5.7.3 - Refine test plan

The CTE 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 CTE will:

- Finalize attack surfaces, vectors, critical components, off-limits components and test objectives
- 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.

5.8 - CONCEPT OF TEST BRIEF

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. Be sure the SUT COTB depicts how the cyber survivability evaluation contributes to the overall SUT evaluation plan (spanning operational effectiveness, operational suitability and cyber survivability).

The CTE will support the WD development of the COTB using the standard OPTEVFOR template provided in **Y:\OT&E Production Library\Test Plan and DCP\Concept of Test Brief** in order to capture the following minimum information regarding the system's cyber survivability test:

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

The CTE shall use the warfare division's guidance to develop, schedule, and conduct the COTB. The CTE shall coordinate the required technical support and COTB participation with 01D including any necessary travel requirements and/or 01D contractor support.

5.9 - TECHNICAL SITE VISIT

The technical site visit must take place on the test asset. It should be scheduled to coincide with the test planning site visit whenever possible. However, if the test planning site visit is conducted

at a location other than the test asset, then this site visit is mandatory. In general, the OPTEVFOR Red Team will be looking for 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
- Final logistics

5.9.1 - Final Test objectives

The CTE will work with 01D to refine the initial test objectives created during CP-1 if required by findings on Technical Site Visit. It is important to ensure that the final test objectives allow for the gathering of all the data requirements listed in the test plan. It is entirely possible that the CTE will determine that additional data requirements need to be collected. Conversely, if any data requirements need to be removed, the CTE must coordinate with 01D and receive concurrence to ensure it does not impact test adequacy. DOT&E approval of test objectives may be required for oversight programs. The data collection framework was designed to meet DOT&E requirements. Any changes to data collection requirements **MUST** be communicated and agreed to between the CTE and the OPTEVFOR Red Team. Otherwise, a risk of collecting incorrect or insufficient data is possible.

5.9.2 - Classification Verification

The OTD is responsible for ensuring the test plan and posttest documents is classified to the appropriate level according to applicable Security Classification Guides (SCGs) with concurrence from the Original Classification Authority (OCA). The test plan being developed for a SUT captures aspects of the system that, potentially, are of high value to an adversary since it outlines how the OPTEVFOR Red Team will attempt to degrade or deny a system using cyber capabilities. As derivative classifier, the CTE shall follow the appropriate security classification guide while drafting the test plan. Prior to specifying potential attack vectors and associated vulnerabilities in the test plan, the CTE shall request formal guidance from the OCA for the system in order to confirm the classification level of the test plan. Historically, security classification guides contain vague derivative classification guidance regarding the existence of potential cyber vulnerabilities and related mission impacts. In order to ensure OPTEVFOR Red Team uses the appropriate classification determinations and handling for data collection, any on test analysis, and for posttest products, the CTE will provide a classification list of all systems contained within the SUT that denote the classification of raw data, cyber vulnerability data, and any posttest data analysis or aggregation. 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.

5.10 - CHECKPOINT 3 (CP-3)

5.10.1 - CP-3 Preparation

At this point in the test planning process (approximately 4 months prior to test) the CTE 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 CTE should plan for at least 30 days to conduct the remaining actions, test plan review board, and document routing for signature. Additionally, for oversight programs, DOT&E requires the final test plan 60 days prior to commencement of test.

5.10.2 - Test Cards and Data Requirements

Prior to completing CP-3, 01D will provide test cards and the final data requirements to the CTE as input to the test plan. The CTE will need to work closely with the OPTEVFOR Red Team (and augmentees if applicable) to ensure the input delivery timeline is confirmed in order to meet the CP-3 milestone.

5.10.3 - CP-3 Execution and Closeout

CP-3 is the final review of the test plan where the 01D OPS & LCA representatives will review the test plan and provide final input for the 01D Director or Deputy. The CTE should provide a test plan that is ready for 01D Director level review at this time, and allow five working days for test plan review. This CP is not a meeting but is used as a milestone to track document finalization progress.

The entrance criteria for CP-3 are as follows:

- CTE finalizes test plan with the exception of Detailed Method of Test (DMOT) section
- OPTEVFOR Red Team and/or augmenting team review TP comprehensively and provide content for DMOT back to CTE
- OPTEV-RT and/or augmenting team comments adjudicated and/or documented in the CRM
- CTE receives Program OCA concurrence on TP classification marking

Participants: CTE and 01D (AOs meet as necessary)

- 01D ensures test team inputs are captured correctly and that objectives are executable
- 01D ensures that test team comments are satisfactorily adjudicated and documents outstanding items in the CRM
- 01D provides test cards and final data collection requirements as input to TP

The exit criteria for CP-3 are as follows:

- 01D Director or Deputy reviews the document and CTE is provided updated running CRM as necessary
- CTE updates POA&M as necessary
- CTE finalizes TP

- CTE provides TP to external stakeholders for review

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

5.10.4 - Test Plan Comment Adjudication

Once the test card and data collection requirement inputs are provided from 01D to the CTE and the document is in a signature ready state, the CTE should distribute the test plan to the OTD, OTC, Section Head, the 01D LCA rep, and DOT&E AO (oversight programs only) for input. The CTE should provide all stakeholders a desired date to receive comments in order to maintain the test planning POA&M. The CTE is responsible for adjudicating all comments with 01D support. The CTE should communicate any updates that change the level of effort, test scope or the Test Execution section of the test plan with the warfare division leadership and 01D. The 01D review of the changes are necessary to ensure test execution is not impacted.

5.11 - 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.

5.12 - 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).

5.12.1 - Quick Reaction Assessment (QRA)

QRA's 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 in order to keep the scope of the QRA streamlined, concise and cost effective.

5.12.2 - 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. Due to the fact that 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.

5.12.3 - 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 conduct. From the Test Planning Handbook: "The purpose of a VCD is to confirm correction of deficiencies identified during IOT&E or Final Operational Test and Evaluation (FOT&E). This evaluation applies to only those deficiencies the Program Manager 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. In order 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 conduct 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 division 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 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, Program Management Office, and the assigned 01D LCA discuss VCD efforts prior to establishing a formal VCD request.

5.12.4 - Cyber LTD

01B is the authority on conducting LTDs, and the LTD process is discussed 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 similar to those of MBTD, and the following information must be considered:

- New or enhanced SUT capabilities
    - Example: If 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 *OPTEVFOR Red Team Memo*, 28 March 2019. This includes coordination with DoD Red Teams, test teams, and external organizations for augmentation support. Augmentation may be required to deconflict OPTEVFOR Red Team's schedule or to partner with an external organization to conduct non-traditional test such as Radio Frequency (RF), hull, mechanical & electrical systems, and Cross Domain Solution (CDS). The OPTEVFOR Red Team is authorized by the Navy Authorizing Official (NAO) to operate on Navy operational environment up to TS GENSER. However, the OPTEVFOR Red Team is limited to local, onsite 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 environment. For Top Secret (TS)/Sensitive Compartmented Information networks/systems, augmenting red teams must have NAVINTEL Designated Authorizing Official (DAO) authorization. The OPTEVFOR Red Team has authorization from the NAVINTEL DAO.

6.1 - FUNDING REQUIREMENTS

Cyber test execution and reporting is funded by the SUT program management office according to the TEMP and detailed in the test execution IGCE. OPTEVFOR Red Team is composed of primarily contracted workforce (prime contractor with multiple sub-contractors). In order 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 - SCHEDULING

The OPTEVFOR Red Team is a mission funded capability and a shared resource to support cyber OT&E execution requirements. In order 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 (located under the document section of 01D's OPTEVFOR portal page). This document details specific scheduling characteristics, processes and responsibilities to ensure the scheduling process supports the overall OPTEVFOR cyber T&E mission. Below is the general outline of the process, refer to the business rules for more detailed information:

1. Prior to seeking execution support, OTD checks OPTEVFOR Red Team availability for desired dates via the OPTEVFOR portal (look for "Cyber Execution Schedule" link on the homeport)
2. If availability is indicated on the execution calendar, OTD requests execution support via the OPEVFOR Red Team Test Execution Questionnaire provided by the OPTEV-RT scheduler

3. 01D evaluates requested dates, level of support and any associated technical details
4. 01D provides a written recommendation detailing estimated level of effort, expected execution test duration and dates available for support
5. OTD provides written acknowledgement and acceptance of the test dates
6. 01D updates cyber execution schedule

An OTD may request execution support without confirmed test asset availability. However, if a test asset is not yet confirmed at the time of scheduling, 01D may provide a "no later than" date for the OTD to get confirmation by. If the test asset is unable to be confirmed by the established date, the scheduled test window may be given to another program that is ready to execute in place of the OTD's program.

01D test execution calendar modifications occur on a first come, first serve basis for initial scheduling requests, or by OTD request to cancel a test, or by direction of the OPTEVFOR Director. In the event where schedule conflicts arise between multiple programs, the respective warfare divisions are responsible to coordinate and determine scheduling priority. If unable to be resolved, the priority determination will be made by the OPTEVFOR Director with consultation by 01D leadership.

In rare cases where conflicts between program requirements and the OPTEVFOR Red Team availability cannot be resolved, it may be necessary to "outsource" cyber OT execution to an external organization. An outsourced test is where the OPTEVFOR Red Team is not involved in the execution and subsequent reporting; making the OTD responsible to coordinate directly with the supporting organization for planning, execution, and reporting. If outsourcing is required, 01D is responsible for identifying the organization to provide the outsourced support along with the initial scheduling and resourcing requirements. Once that is provided to the OTD, 01D will step into a technical advisor role for the OTD. A determination to use outsourcing must be made at the warfare division and 01D leadership levels and may require Director approval prior to beginning planning.

6.3 - COOPERATIVE VULNERABILITY PENETRATION ASSESSMENT (CVPA)

The CVPA is a cooperative evaluation of the system's vulnerabilities in an operational context and provide 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 OPTEVFOR Red Team or another qualified organization designated by 01D attempts to discover system vulnerabilities that impact its mission capabilities and the results support development of AA attacker storyboards. The CVPA is fully informed and supported by system owners and operators and system engineering experts. The CVPA data supports the evaluation of the system's "prevent" capabilities within the PMR construct.

The CVPA must be conducted in 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 Sites (LBTS) or labs. Such concessions are subject to the M&S accreditation policies conveyed by OPTEVFORINST 5000.1C and Section two 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 warfare division and 01D collaborate to determine the requirement for use of LBTS or labs during test strategy discussions. Once determined, the effort is coordinated with 01B and 01D as described in section two 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 an insider, nearsider, and outsider perspectives as applicable. In addition to the system's prevent capabilities, mitigate and recover capabilities from both the system and operator perspective will be observed within the PMR construct during an AA.

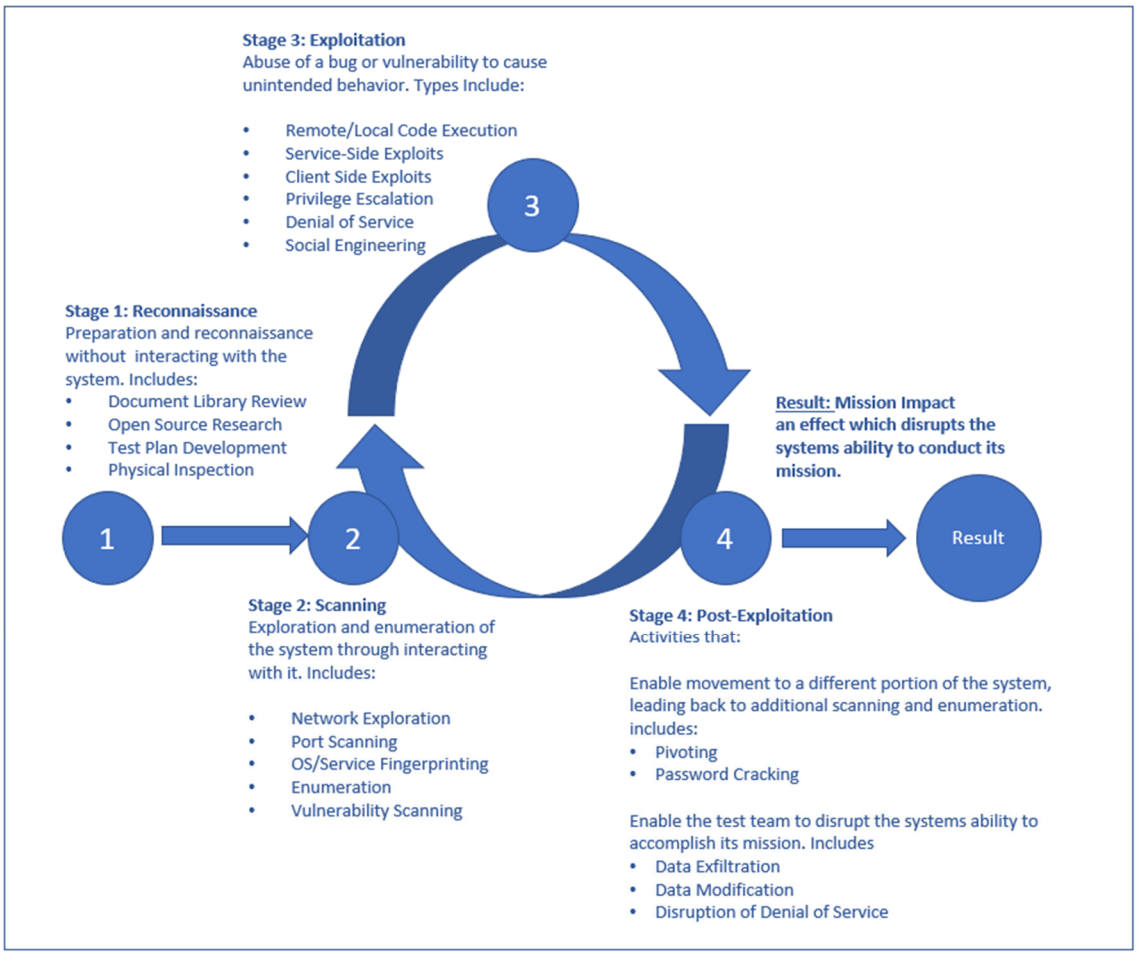
6.5 - EXECUTION METHODOLOGY

The OPTEVFOR Red Team conducts cybersecurity test 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 reconnaissance stage of the execution cycle for the OPTEVFOR Red Team.

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



6.5.1 - Stage 1: Reconnaissance

Reconnaissance involves gathering available information about the SUT without connecting any digital cybersecurity tools to it. Test planning efforts significantly contribute to this stage as well as the OPTEVFOR Red Team's open source research.

6.5.2 - Stage 2: Scanning

Stages 2-4 are cyclical and continue until the completion of execution. During scanning, the OPTEVFOR Red Team uses automated tools to explore and discover potential vulnerabilities on the SUT and SoS.

6.5.3 - Stage 3: Exploitation

During exploitation, the OPTEVFOR Red Team attempts to exploit discovered vulnerabilities to gain additional access or information.

6.5.4 - Stage 4: Post Exploitation

During post exploitation, the OPTEVFOR Red Team will attempt to gain access to other components and laterally move throughout the SUT and SoS. The OPTEVFOR Red Team will also attempt to degrade or deny the system's ability conduct mission(s).

6.5.5 - Result: Mission Impact

The objective of the execution methodology is to create a mission impact. The observed mission impact(s) will be documented and supported by the data collected. During the AA portion of the test, the team will collect Prevent, Mitigate, and Recover data.

SECTION 7 - POST-TEST PROCESS

The Warfare division will coordinate and lead the Post-Test Iterative Process (PTIP) per OPTEVFOR INST 3980.2(series), the OT&E Manual and supporting handbook. The OTD is responsible for ensuring that the post-test documents are classified to the appropriate level according to applicable SCGs with concurrence from the OCA(s). In the event where test execution was "outsourced" to an external organization, the OTD is fully responsible to produce all required PTIP products and content. 01D can serve as a technical advisor in these instances but, without first-hand knowledge of the executed test and associated data collection, the OTD will have to coordinate directly with the external organization for the test analysis and reporting.

Upon completion of OPTEVFOR-RT testing and once the test data has been uploaded, the PTIP can be initiated by the OTD in coordination with the test team lead(s). The OTD and 01D Test Team Lead will coordinate and manage the PTIP POA&M; ensuring enough time for test data shipping and upload, internal 01D reviews, and the routine PTIP milestones.

The OTD can expect three products from the OPTEVFOR Red Team in preparation for the COI Evaluation Working Group (CEWG) and follow-on PTIP milestones from 01D. These products are the data analysis summary, draft system deficiency sheets, and cyber survivability evaluation results write-up. Cyber deficiency sheets provide narrative analysis and graphical illustrations of exploited cyber-attack kill chains that affected the SUT mission capabilities. These deficiency sheets are intended to be used by the Program Management Office to remediate or mitigate the discovered cyber-attack kill chain. The OTD is responsible for the product integration into the program's final report along with generating the content for the Director's letter. 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 T&E reports. In accordance with section 6.2 the OTD is responsible for product generation normally provided by 01D for tests that are outsourced to other organization's red teams.

7.1 - 01D REVIEW BOARD

01D review board is an internal meeting between the test team and 01D Director/Deputy to vet the draft report products at the highest level for technical accuracy in between the data scoring board and the CEWG, and is not part of the standard PTIP process. This step is necessary in order to streamline the review process and avoid unnecessary churn post-CEWG. Depending on the data and subsequent post-test analysis, there may be some unresolved items out of the 01D review board that require further discussion with 01D and WD leadership. Should this be necessary, 01D will schedule a meeting with the WD leadership to present the items and obtain consensus for how to address them for the remainder of the test reporting process.

Due to the technical scrutiny established during the 01D Review Board, this review could result in significant changes to the draft report products. Therefore, it is strongly recommended that draft report products do not get 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 a review board to ensure products meet quality standards.

7.2 - CYBER DEFICIENCY SEVERITY DETERMINATION

01D uses the basis for deficiency severities from the OPTEVFOR Test Reporting Handbook when recommending severity levels for cyber deficiencies when moving into a CEWG. The additional considerations for cyber deficiency severity are (but are not limited to):

- 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?
- Exploit Difficulty – Would this attack require extensive monetary and technical resources or advanced capabilities to accomplish, or could it be performed by an adversary with relatively little experience, limited to no physical access, and common system knowledge?
- Indicators of Compromise – Are there any indicators that an attack is taking place in real time, and can the SUT subsequently recover from and eliminate the threat?
- 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.

APPENDIX A - ACRONYMS AND ABBREVIATIONS

AA	Adversarial Assessment
APM	Assistant Program Manager
AT	Accelerator Team
CCB	Critical Components Breakdown
CDS	Cross Domain Solution
CEWG	Critical Operational Issue Evaluation Working Group
COI	Critical Operational Issues
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
CTE	Cyber Test Engineer
CTT	Cyber Table Top
CVPA	Cooperative Vulnerability and Penetration Assessment
DAO	Designated Authorizing Official
DMOT	Detailed Method of Test
DoD	Department of Defense
DoDI	DoD Instruction

DoN	Department of the Navy
DOT&E	Director, Operational Test & Evaluation
DT	Developmental Testing
EOA	Early Operational Assessment
FOT&E	Final Operational Test and Evaluation
IDS	Intrusion Detection Systems
IEF	Integrated Evaluation Framework
IGCE	Independent Government Cost Estimate
IOT&E	Initial Operational Test & Evaluation
IPS	Intrusion Prevention Systems
ISP	Information Support Plan
JCIDS	Joint Capabilities Integration and Development System
KPP	Key Performance Parameter
LBTS	Land Based Test Sites
LCA	Lead Cyber Analysist
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
PMR	Prevent, Mitigate, and Recover
PMT	Platform Mission Task
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPA	Program Protection Analysis
PPP	Program Protection Plan
PPP	Program Protection Plan
PTIP	Post-Test Iterative Process
QRA	Quick Reaction Assessment
RF	Radio Frequency
SME	Subject Matter Expert
SoS	System of Systems
SS	System Survivability
SUT	System Under Test

T&E	Test & Evaluation
TEMP	Test and Evaluation Master Plan
TP	Test Plan
TS	Top Secret
TTP	Tactics Techniques and Procedures
USB	Universal Serial Bus
V&V	Verification & Validation
VCD	Verification of Correction of Deficiencies
VOLT	Validated Online Lifecycle Threat
WD	Warfare Division