



OPERATIONAL TEST  
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE  
1700 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1700

JAN 21 2015

MEMORANDUM FOR COMMANDER, ARMY TEST AND EVALUATION COMMAND  
COMMANDER, OPERATIONAL TEST AND EVALUATION  
FORCE  
DIRECTOR, MARINE CORPS OPERATIONAL TEST AND  
EVALUATION ACTIVITY  
COMMANDER, AIR FORCE OPERATIONAL TEST AND  
EVALUATION CENTER  
COMMANDER, JOINT INTEROPERABILITY TEST COMMAND

SUBJECT: Cyber Economic Vulnerability Assessments (CEVA)

I have previously provided guidance to Operational Test Agencies (OTAs) on conducting cybersecurity tests and evaluations (e.g., “Any data exchange, however brief, provides an opportunity for a determined and skilled cyber threat to ... damage information...”).<sup>1</sup>

Cyber threats present a risk of economic exploitation of information systems whose functions include financial management, payments, allotments, and fiscal transfers. Many of these systems connect to non-Department of Defense (DOD) networks and environments. An adversary may exploit such systems to disrupt mission-essential logistics or steal funds. Business-focused systems in the Department need to be secure and resilient in a potentially hostile information environment.

OTAs should modify their cybersecurity test and evaluation processes as appropriate for DOD systems whose functions include financial or fiscal/business activities or the management of funds, to include the following activities:

- Cyber Economic Threat Analysis – Development of a set of economic exploitation scenarios derived from threat analysis. The intelligence should come from a variety of sources (e.g., open source intelligence, intelligence agencies, commercial partners, etc.).<sup>2</sup> This analysis should consider the known or potential vulnerabilities of the system and its associated control processes in question, and establish test cases by which the financial security of the systems under test may be evaluated.

---

<sup>1</sup> DOT&E memorandum “Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs” dated August 1, 2014.

<sup>2</sup> The scenarios should be developed in coordination with financial auditing experts.

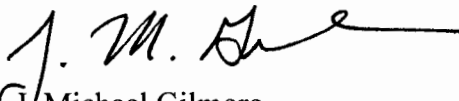


- Cyber Economic Scenario Testing – Tests threat vectors against the production system under realistic operating conditions, and with the participation of personnel who sufficiently understand the system and associated control processes and how they can be exploited. Testing should encompass scenarios ranging from small-scale fraud to attacks that might result in significant economic degradation to DOD or the U.S. government.
- Financial Transaction Analysis – Review a representative set of past and current financial transactions for evidence of fraudulent activity (e.g., fraud indicators that identify exceptions or transactions that fall outside normal activity).

To adequately assess cyber economic vulnerabilities, all cyber adversarial activities must be conducted with certified and accredited “red team” personnel and should include system and cyber economic subject matter experts to ensure the key operational capabilities and business processes are evaluated (roles, responsibilities, and business processes within the system, as well as dependencies between the host system and other enterprise systems.)

Attached to this memo is guidance for conducting a CEVA. Test reports from all operational test events with CEVA components should include recommendations, as appropriate, for improving the attached guidance. My office will update the CEVA guidance periodically based on your feedback. I expect this CEVA guidance to be implemented by the next operational test event of a business system on DOT&E oversight.

My point of contact for this action is Todd G. Fisher. He may be reached at [todd.g.fisher.civ@mail.mil](mailto:todd.g.fisher.civ@mail.mil) or (571) 372-3881.

  
J Michael Gilmore  
Director

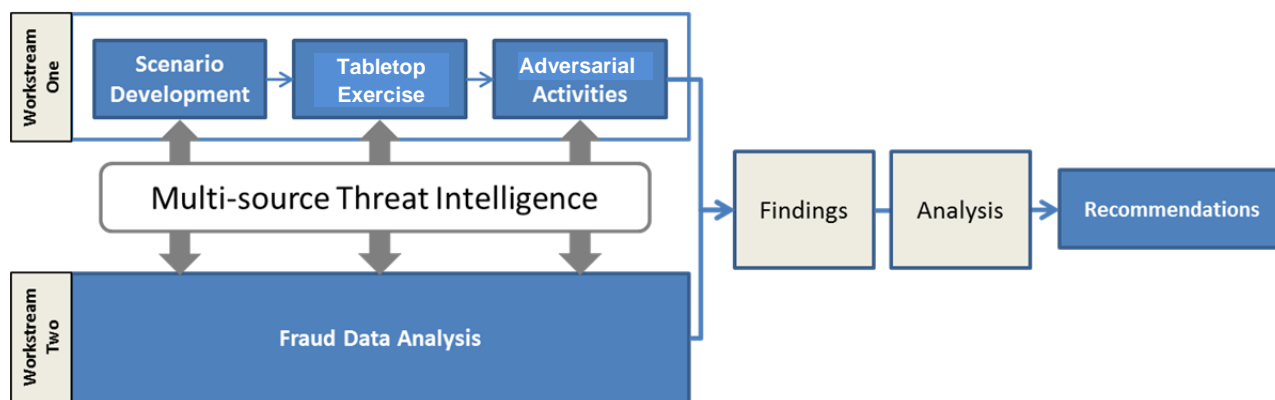
Attachment:  
CEVA Guidance

cc:  
Director, National Security Agency  
Director, Defense Information Systems Agency  
Department of Defense Chief Information Officer  
Director, Army Test Evaluation Office  
Director, Navy Test and Evaluation and Technology Requirements (N912)  
Director, Test and Evaluation, Headquarters, United States Air Force  
Commander, United States Cyber Command  
Director, Joint Chiefs of Staff

## Cyber Economic Vulnerability Assessment (CEVA) Guidance

### Process Overview

A Cyber Economic Vulnerability Assessment (CEVA) should be conducted in a series of phases across two workstreams. Workstream One is comprised of three separate activities: Scenario Development, Tabletop Exercise, and Adversarial Testing. The output of Workstream One is a set of findings on cyber economic threats with respect to the system under test (SUT). Workstream Two is the analysis of SUT data for fraudulent transactions. The output of this analysis is a set of initial findings and recommendations for further analysis.



**Figure 1. Assessment Process**

The CEVA should leverage, as available, threat intelligence from cyber intrusions into commercial industries to develop an initial set of cyber economic threat vectors (the Operational Test Agencies (OTAs) should use these types of reports which are produced by many commercial vendors; e.g., Mandiant, Verizon, Kaspersky). These threat vectors should be the foundation of stakeholder discussions to create cyber economic scenarios applicable to the functions of the SUT. The attack scenarios will serve as a basis for a Tabletop Exercise used to assess the probability of success for attackers and SUT defenders, and to refine scenarios. Upon conclusion of the Tabletop Exercise, the red team, acting as part of a Cyber Opposing Force (OPFOR), will execute a series of technical penetration tests and economic exploitation of the SUT. The Cyber OPFOR should be augmented with subject matter expertise (SME) from the SUT and Department of Defense (DOD) business processes.

Cyber economic threat vectors should be integrated into each step of test execution. The integration of current threat intelligence focuses the testing in order to achieve the most efficient and meaningful test process. The analysis of the outputs from both workstreams yields a set of programmatic recommendations to enhance the SUT (including associated control processes), as well as recommendations regarding the feasibility of further cyber economic analyses.

The following sections outline the planning, execution, and output of each phase within the above workstreams in more detail. Each section provides information regarding the planning, execution, and realized output from the phase.

## 1.0 Workstream One

Workstream One includes three separate phases. The first phase is Scenario Development. This phase initiates the development of cyber economic threat scenarios based on the role and function of the SUT. The second phase is the Tabletop Exercise. This phase develops a refined list of cyber economic scenarios based on the input from stakeholders attacking or defending the system. The third phase is the Adversarial Testing phase. This phase takes the refined set of scenarios and executes them on the system in order to determine whether or not attackers would be successful.

### 1.1 Scenario Development

#### 1.1.1 Planning

The intent of the scenario-based approach is to test threat vectors against realistic operating conditions. Scenarios should simulate likely threats to DOD financial management systems and should include new and emerging threats. Scenario developers should consider the inputs outlined in Table 1 below.

**Table 1. Example Inputs for Scenario Development Phase**

<b>Example Inputs for Scenario Development Phase</b>	
<b>Processes</b>	<ul style="list-style-type: none"> <li>• Cyber economic scenarios</li> <li>• Adversarial testing rules and requirements</li> <li>• Cyber economic testing ground rules (among all test stakeholders)</li> <li>• Results of most recent vulnerability assessment</li> <li>• Applicable cyber security or system certification documentation</li> <li>• User roles and responsibilities</li> </ul>
<b>Technology</b>	<ul style="list-style-type: none"> <li>• SUT architecture documentation</li> <li>• Domains applicable to System Under Test (SUT) (e.g., Air Force Network)</li> <li>• Defense Finance and Accounting Services architectures and interfaces</li> <li>• Account management architecture and interfaces</li> <li>• Intra-Service system interfaces</li> <li>• SUT segregation of duties rules</li> </ul>
<b>Skillsets</b>	<ul style="list-style-type: none"> <li>• Business acumen related to business operations, enterprise-wide system management, accounting, finance</li> <li>• Adversarial skills to include moderate to high levels of skill in underlying operating system(s), database(s), web application(s), or overall Commercial Off-the-Shelf (COTS) software supporting application(s)</li> <li>• Functional expertise from the system under assessment (knowledgeable on system functional processes)</li> <li>• Knowledge of system integration with other inter-dependent systems</li> <li>• All source intelligence analysis on current threats to underlying system components</li> </ul>

#### 1.1.2 Execution

Each scenario should be documented in an attack scenario summary sheet, providing a high-level overview of each stage of the attack (e.g., planning, reconnaissance, breach, establish control, and operational attack execution). The activities within these stages may be further divided (e.g., the primary attack, the diversionary attack to redirect blame, and the duress attack

to apply stress on key individuals responsible for the processes under attack). Scenarios should then undergo a consultative and iterative process of review with key stakeholders.<sup>1</sup>

### **1.1.3 Output**

The output from the scenario development process should be an agreed-upon set of scenarios to be used for the Tabletop Exercise and Adversarial Testing.

## **1.2 Tabletop Exercise**

### **1.2.1 Planning**

The intent of the Tabletop Exercise is to walk through scenarios and wargame the defender actions taken in response to threat actions. The attack scenarios identified as outputs from the scenario development phase are used as inputs to the Tabletop Exercise. The activities associated with each scenario should be used as the basis to facilitate the attack and defend actions from the Cyber OPFOR and network defenders during the Tabletop Exercise.

Prior to the Tabletop Exercise, all participating parties must agree on Adversarial Testing rules and requirements, Tabletop Exercise execution rules, and other scoping details requiring approval(s). The Tabletop Exercise planning relies on information from processes, technology, and a range of skillsets. Table 2 highlights inputs that could be used to plan and execute the Tabletop Exercise phase of the SUT assessment:

---

<sup>1</sup> An example scenario is provided in Annex B.

**Table 2. Example Inputs for Tabletop Exercise Phase**

<b>Example Inputs for Wargame Phase</b>	
<b>Processes</b>	<ul style="list-style-type: none"> <li>• Agreed upon cyber economic attack scenarios from Scenario Development Phase</li> <li>• Adversarial testing rules and requirements</li> <li>• Cyber economic testing ground rules (amongst all test stakeholders)</li> <li>• Tabletop Exercise execution rules</li> <li>• Tabletop Exercise data collection procedures</li> <li>• User roles and responsibilities</li> </ul>
<b>Technology</b>	<ul style="list-style-type: none"> <li>• System architecture documentation</li> <li>• Domains applicable to System Under Test (SUT) (e.g., Air Force Network)</li> <li>• Defense Finance and Accounting Services architectures and interfaces</li> <li>• Account Management architecture and interfaces</li> <li>• System interfaces</li> <li>• Intelligence reporting on current threat signatures</li> <li>• Most recent Vulnerability Assessment results</li> <li>• SUT segregation of duties rules</li> </ul>
<b>Skillsets</b>	<ul style="list-style-type: none"> <li>• Expertise for conduct of Tabletop Exercise</li> <li>• Business acumen related to business operations, enterprise-wide system management, accounting, finance</li> <li>• Certified and accredited red teams to include moderate to high levels of skill in underlying operating system(s), database(s), web application(s), or overall COTS software supporting application(s)</li> <li>• Functional expertise from system under assessment (knowledgeable on system functional processes)</li> <li>• Knowledge of system integration with other inter-dependent systems</li> <li>• System architecture and system engineering technical representatives</li> <li>• Security monitoring representative (if applicable)</li> <li>• All source intelligence analysis on current threats to underlying system components</li> </ul>

### 1.2.2 Output

The outputs of Tabletop Exercises are updated scenarios and community understanding of the CEVA.

## 1.3 Adversarial Testing

### 1.3.1 Planning

The intent of adversarial testing is to execute scenarios against the SUT application in a realistic operational environment. The Cyber OPFOR will employ various technical exploitation techniques against the SUT infrastructure in an attempt to gain access to the system as a normal user and conduct cyber economic scenarios. If the Cyber OPFOR is not able to gain unauthorized access, they will continue to execute the scenarios as an insider.

Cyber OPFOR planning integrates a range of processes, technology, and skillsets in order to ensure smooth execution. The following table outlines the details that may be used for each of these.

**Table 3. Example Inputs for Adversarial Testing Phase**

<b>Example Inputs for Adversarial Testing Phase</b>	
<b>Processes</b>	<ul style="list-style-type: none"> <li>• Guidance for Adversarial Testing on applicable domain</li> <li>• Escalation Points of Contact (POCs) from system functional management office for troubleshooting</li> <li>• In-brief / Out-brief schedule</li> <li>• Refined set of cyber economic attack scenarios defined in Tabletop Exercise Phase</li> <li>• Adversarial Testing rules and requirements</li> <li>• Cyber economic testing ground rules (amongst all test stakeholders)</li> <li>• Results from scans of pre-production or lab instance</li> <li>• Security monitoring alert procedures (if applicable)</li> <li>• User roles and responsibilities</li> </ul>
<b>Technology</b>	<ul style="list-style-type: none"> <li>• Access to System Under Test (SUT) pre-production instance, or lab instance of application</li> <li>• Access to SUT production instance</li> <li>• Appropriate penetration testing tools</li> <li>• SUT architecture documentation</li> <li>• Domains applicable to SUT (e.g., Air Force Network)</li> <li>• SUT segregation of duties rules</li> <li>• Defense Finance and Accounting Services architectures and interfaces</li> <li>• Account management architecture and interfaces</li> <li>• Intra-Service system interfaces</li> <li>• Intelligence reporting on current threat signatures</li> <li>• Most recent vulnerability assessment scanning results</li> </ul>
<b>Skillsets</b>	<ul style="list-style-type: none"> <li>• Adversarial skills to include moderate to high levels of skill in underlying operating system(s), database(s), web application(s), or overall commercial off the shelf software supporting application(s)</li> <li>• Business acumen related to business operations, enterprise-wide system management, accounting, finance</li> <li>• Functional expertise from system under assessment (knowledgeable on system functional processes)</li> <li>• Knowledge of system integration with other inter-dependent systems</li> <li>• System architecture and system engineering technical representatives</li> <li>• Security monitoring representative (if applicable)</li> <li>• All source intelligence analysis on current threats to underlying system components</li> </ul>

As individual skillsets can vary, multiple skillsets could therefore be combined into one role. The above list will need to be supplemented with additional roles. In addition to the processes, technology, and skillsets identified in the table above, the following roles should be considered for each Cyber OPFOR:

**Table 4. Example Roles and Responsibilities**

<b>Role Name</b>	<b>Responsibility</b>	<b>Notes</b>
Technical penetration testers	Conduct technical penetration testing of SUT; have requisite experience in exploitation of associated operating systems, applications, databases, etc.	If expertise is not available to the team, access to an individual with the required expertise should be provided.
System specific SME	Understand roles, responsibilities, and business processes within system as well as dependencies between host system and other enterprise system	This is a time saving measure, but it should be worth noting that attackers not familiar with the system would need time for reconnaissance in order to minimize potential for alerting security monitoring.
Lead Evaluator	Provides guidance to ensure proper test plan procedures are followed and that all required data are collected	N/A
Cybersecurity Manager	Provides guidance on standard cybersecurity posture of system components to technical penetration testers; captures relevant information on any vulnerability identified to ensure it is tracked and remediated	N/A
Cyber economic SME	Provides expertise on which economic information available within system is exploitable to achieve cyber economic effects	N/A
Data Collection	Accurately captures information on conduct of test	Guidance on potential classification of information associated with vulnerabilities should be considered here.

The Adversarial Testing planning process should allow adequate time for the technical penetration team to scan a pre-production instance of the system or have time to build a lab instance to scan. This approach mirrors typical adversarial pre-attack planning processes. Additionally, adequate time allows the Adversarial Testing to obtain proper approvals and signed documentation from approving authorities in order to traverse additional portions of the system footprint as required by the scenarios.

**System Specific and Cyber Economic Subject Matter Experts (SMEs).** To adequately execute the CEVA, the Cyber OPFOR should include system specific and cyber economic SMEs in addition to typical technically certified and accredited red team members. The system specific SME should understand the operational capabilities and key business process(es) used within the system to include roles and responsibilities, as well as inter-dependencies between host system and other enterprise system(s). The cyber economic SME should understand how to convert the technical penetration of the system to achieve economic effects as well as identify targets of economic exploitation during the testing process. A CEVA analyst team should have experience with the following:

- Quickly conducting research and analyzing large amounts of economic and financial data, threat intelligence data, and cyber-attack trends data and evidence



- Designing, building, and maintaining Enterprise Resource Planning systems and corresponding databases and interfaces
- Functional knowledge of the government Planning, Programming, Budgeting, and Execution, logistics, and other business processes
- Cyber red teams and exercises
- Cyber adversary Tactics, Techniques, and Procedures (TTPs) and translating those TTPs into Cyber OPFOR activities
- Collaborating with DOD acquisition programs
- DOD Acquisition process
- DOT&E test processes (e.g., Information Assurance operational testing)
- Comprehensive knowledge of Net-Centric and Business (Enterprise Resource Planning) systems operations for effectiveness, suitability, survivability, and military utility

### **1.3.2 Output**

The output of the Adversarial Testing phase will produce data regarding the adversary's ability to penetrate the SUT application and exploit system cyber economic data/information to achieve varying effects. In addition to the above, the Cyber OPFOR will execute cyber economic risk scenarios (e.g., Fraud and Denial of Service).

## **2.0 Workstream Two**

### **2.1 Data Analysis**

#### ***2.1.1 Planning***

The intent of the Data Analysis phase is to review a representative set of past and current transaction data for evidence of fraudulent activity. A set of automated business rules and fraud indicators identify exceptions or transactions that fall outside normal activity. A detailed analysis of the exceptions by fraud experts or individuals intimately familiar with the data and its structures will identify the true positives within the exceptions for further investigation and action. In order to prepare for the Data Analysis workstream, the following table provides considerations for Processes, Technology, and Skillsets:

**Table 5. Example Input for Data Analysis Phase**

<b>Example Inputs for Data Analysis Phase</b>	
<b>Processes</b>	<ul style="list-style-type: none"> <li>• Representative set of past and current transaction data</li> <li>• Data sorting logic for transaction exceptions</li> <li>• SUT segregation of duties rules</li> <li>• Refined set of cyber economic attack scenarios defined in Tabletop Exercise Phase</li> <li>• Cyber economic testing ground rules (amongst all test stakeholders)</li> <li>• Exception escalation procedures (to include POCs)</li> </ul>
<b>Technology</b>	<ul style="list-style-type: none"> <li>• Data sorting processing and sorting tool</li> <li>• SUT user access</li> <li>• External exception validation systems (e.g., Office of Foreign Asset Control (OFAC)) exception database)</li> <li>• Intra- and Inter-Service system interfaces</li> <li>• Intelligence reporting on current threat signatures</li> <li>• Most recent vulnerability assessment scanning results</li> </ul>
<b>Skillsets</b>	<ul style="list-style-type: none"> <li>• Business acumen related to business operations, enterprise-wide system management, accounting, finance</li> <li>• Knowledge of external exception validation systems</li> <li>• Knowledge of system integration with other dependent systems</li> <li>• System architecture and system engineering technical representatives</li> <li>• Security monitoring representative (if applicable)</li> <li>• All source intelligence analysis on current threats to underlying system components</li> </ul>

Using an automated tool set for the data analysis allows for bulk data processing, filter and logic customization, and the ability to sort and pivot data for further investigation. Pre-determined business rules and indicators within the automated system sort exceptions into logical findings categories. It is possible for a single transaction to show up in multiple sets of exceptions; therefore analysis should focus on the exception as a whole, not just the transaction. The automated tool sets on the market allow for configuration of additional business rules and indicators to help reduce false positives during analysis.

A detailed analysis of the exceptions by fraud experts or individuals intimately familiar with the data and its structures will identify the true positives within the exceptions for further investigation and action. The analysis should be clearly documented and provided to the program manager and other appropriate parties.

In addition to analyzing the data itself, access to the system as well as supporting research tools help reduce time to investigate the exceptions (e.g., review of the Department of Treasury Office of Foreign Assets Control (OFAC) exceptions requires access to the OFAC online database). Furthermore, the analyst(s) may require read-only access to the tested system to validate the exception findings against the system records.

### **2.1.3 Output**

The output of the Data Analysis process is an initial findings document outlining the exceptions identified during the analysis. Exceptions may be organized by the following finding types:

**Table 6. Example Exception Finding Types & Definitions**

<b>Finding</b>	<b>Definition</b>
Duplicate Vouchers	Invoices that have similar invoice numbers, similar invoice amounts, same or similar vendors, or a variation of invoice amount or naming that could be considered a transposition.
Voucher Outlier	Voucher amount is outside the average voucher amount for a specific vendor.
Purchase Order (PO) Outlier	PO has an amount outside the norm for the vendor or the buyer.
Invoice Line Predates Order	A voucher has been entered for an invoice, and invoice data and/or entry date predates the release of the PO.
Split PO	Multiple POs have been entered for a purchase that would normally exceed the chart of authority limit.
Office of Foreign Assets Control (OFAC) Exception	Same or similar spelling of entity name or related ownership to the spelling of known entities within the OFAC Specifically Designated Nationals (SDN) list.

This page intentionally left blank.

## Annex A – Example Timeline

The following table is an example timeline that could be used as the basis for planning a cyber economic vulnerability assessment.

<b>Cyber Economic Vulnerability Assessment Example Timeline</b>			
NOTE: Any of these activities could take longer or shorter than identified depending on the progress of the test.			
CEVA – Cyber Economic Vulnerability Assessment	FMO – Financial Management Office	OT – Operational Test	
DO – Due Outs	KP – Key Players	OTA – Operational Test Agency	
DOT&E – Director, Operational Test and Evaluation	O/S – Open Source	PMO – Program Management Office	
EC – Entrance Criteria	OCI – Organization Conflict of Interest	ROM – Rough Order of Magnitude	
ERB – Emerging Results Brief	OPFOR – Opposing Force	WG – Working Group	
Phase	Timing	Title	Description
<b>Planning</b>	ASAP	Threat Intel	Gather threat intelligence from which the entire test will be built upon. The threat intelligence is the requirement that should be tested to and will drive scenario development.
	T-180	Kickoff	KP: DOT&E, OTA, PMO, FMO, CEVA Analyst, Cyber OPFOR DO: ROM, schedule, scope, key players Initial meeting between the system owners and the test community. Discussion will include an overview of the testing process, system overview, cyber security status, test objectives. The team will scope the test activities, data sources for analysis, identify key player(s), develop a high-level schedule, and discuss level of effort to create a ROM.
	T-170	OSINT	Responsibility: Cyber OPFOR Cyber OPFOR will begin researching the system
	T-160	Scenario WG #1	KP: OTA, CEVA Analyst DO: High-level scenarios (actors, goals, storyline) The OTA and CEVA Analyst will meet to draft initial scenario framework based on threat intelligence (OSINT and closed source). The objectives should be to identify the threat actor(s) being represented, the goals of these actors (focused on affecting mission not just stealing data, committing fraud, or causing issues with the system. Continue asking why would an adversary want to do something), and an overarching story.
	T-125	Scenario WG #2	KP: OTA, CEVA Analyst, Cyber OPFOR, PMO/FMO DO: Scenarios with actionable objectives for the Cyber OPFOR Taking the scenarios developed during the first WG, the OTA should now include the Cyber OPFOR and the PMO/FMO to develop the actual steps that will be taken to achieve the adversarial goals. The OTA should also confirm the data sources or sets with the PMO/FMO that should be run for fraud indicators and anomalies.

T-120	DRAFT OCI Document	<p>Responsibility: CEVA support contractor</p> <p>As required. In place to prevent any potential overlap between audit services and CEVA services if supported by the same organization. This needs to be in place as soon as possible.</p>
T-120	DRAFT Test Plan	<p>Responsibility: OTA</p> <p>Should include, at a minimum: Scenarios, test description, scope, schedule, key players, test locations, and environmental requirements (e.g., accounts/access to pre-production environments). The DRAFT should be provided to all personnel who will participate in the tabletop exercise and should be provided in sufficient time for all participants to provide initial feedback.</p>
T-120	DRAFT Ground Rules	<p>Responsibility: OTA, Cyber OPFOR</p> <p>This outlines what portions of the system will be “fair game” during the CEVA. The ground rules will identify all key defensive players in the assessment. The ground rules should be drafted in sufficient time to allow coordination of defensive players’ attendance at the tabletop exercise. Additionally, the ground rules should address how data will be analyzed (e.g., transferred to 3<sup>rd</sup> party, completed in house) as part of the financial fraud analysis.</p>
T-110	Test Plan WG #1	<p>Responsibility: OTA</p> <p>Meet with key players to explain and discuss contents of the test plan.</p>
T-90	Signed OCI Document (if needed)	<p>Responsibility: Government will review CEVA support contractor OCI mitigation plan and accept if adequate.</p> <p>Goal is to have it done before the tabletop exercise so that there are no perceptions of lacking independence.</p>
T-90	Submit Financial Data	<p>Responsibility: PMO/FMO</p> <p>EC: Signed OCI Document</p> <p>The PMO/FMO should provide the OTA with a representative set of past and current transaction data to investigate for evidence of fraudulent activity. Analysis of the data will continue into the reporting period of the CEVA.</p>
T-90	Tabletop Exercise	<p>KP: OTA, CEVA Analyst, Cyber OPFOR, PMO/FMO, Network Defenders, DOT&amp;E</p> <p>EC: DRAFT Scenarios, DRAFT Test Plan</p> <p>Walk through scenarios and Wargame (tabletop) the defender actions taken in response to threat actions and determine the ability to execute the scenarios during adversarial testing.</p> <p>DO: Refined scenarios, community buy-in and understanding</p>
T-80	Begin Recon	<p>Responsibility: Cyber OPFOR, PMO/FMO</p> <p>Cyber OPFOR will familiarize themselves with the system by using test environment accounts provided by PMO/FMO.</p>
T-80	Test Plan WG #2	<p>Responsibility: OTA</p> <p>OTA will work with key players to adjudicate comments.</p>

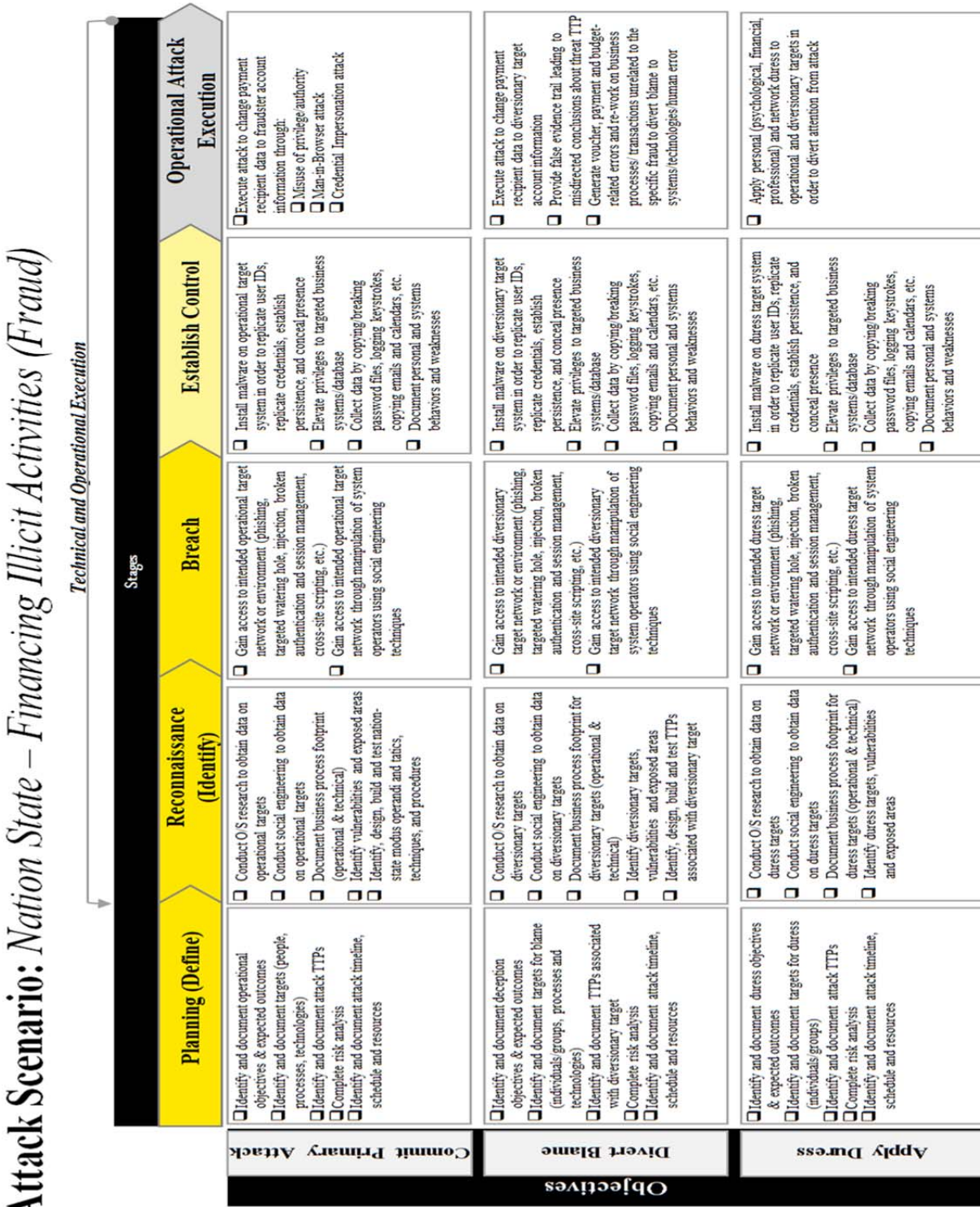
	T-60	Staffing Test Plan	Responsibility: OTA
	T-60	Staffing Ground Rules	Responsibility: OTA
	T-45	Test Plan Approval	Responsibility: OTA, DOT&E (as appropriate)
	T-30	Ground Rules Signed	Responsibility: Cyber OPFOR, Network Defenders
	T-30	Data Analysis	Responsibility: OTA Initiate data analysis for financial fraud indicators and anomalies.
	T-15	Test Readiness Review	Responsibility: OTA EC: Signed Ground Rules, Signed Test Plan OTA will lead a review to determine if key players are ready for test.
<b>Execution</b>	T-30	Active Recon	Responsibility: Cyber OPFOR, Network Defenders EC: Signed Ground Rules The Cyber OPFOR will perform active scans and determine their path to the system. The defenders should perform their normal daily activities.
	T-14	Intel Prep of the Battlefield	Responsibility: Cyber OPFOR, Network Defenders The Cyber OPFOR will begin positioning themselves on the network in preparation to attack the system. The defenders should perform their normal daily activities.
	T	Technical Exploitation	Responsibility: Cyber OPFOR, Network Defenders, OTA, CEVA Analyst The Cyber OPFOR will attempt to gain unauthorized system access and defenders should perform normal daily activities.
	T+7	Scenario Execution	Responsibility: Cyber OPFOR, Network Defenders, OTA, CEVA Analyst, PMO/FMO The Cyber OPFOR will execute the test plan's approved scenarios. Depending on the ground rules, the Cyber OPFOR may only be authorized to execute the scenarios to the point of causing system effects. The PMO/FMO may require the Cyber OPFOR to move to a non-production environment to cause effects.
	T+14	Effects Demonstration	Responsibility: Cyber OPFOR, OTA, CEVA Analyst, PMO/FMO If required, the Cyber OPFOR will demonstrate scenario effects in a non-production environment.
	Daily	Stand up / Hotwash	Responsibility: OTA The OTA should hold a daily stand-up and hotwash to lay out what is expected for the day and to review the day's activities.

<b>Reporting</b>	E+14	Quick Look	Responsibility: OTA The OTA will provide initial findings to the PMO/FMO
	E+30	ERB	Responsibility: OTA The OTA will brief leadership on the test results
	E+60	Report	Responsibility: OTA



## Annex B – Example Scenario

The following is an example of a cyber economic vulnerability assessment scenario. This scenario is not meant to limit test planning or attack vectors. Testers may use whatever mechanism that best allows adequate testing of the system.



This page intentionally left blank.

## Annex C – Example Lessons Learned

**Intent:** The lessons learned are broken into the four major phases of the conduct of this assessment program. The recommendations are intended to enhance the efficiency and effectiveness of testing operations, as well as overall test output.

### 1. Program Development:

- What worked well
  - Executive-level support at all phases worked very well
  - Executive agent that commissioned the project is, by charter, an objective and independent testing organization and has authority to direct the review of DOD systems

### 2. Scenario Development:

- What worked well?
  - In-person meeting provided opportunity to quickly arrive at consensus about which scenarios to utilize going forward
  - Inclusion of system functional Subject Matter Expert(s) (SMEs) from beginning of scenario development
  - Leveraging a wide range of cyber economic risk scenarios based on known activities from nation state and insider threats to refine the likely attack scenarios against a DOD system.
- Points to consider for future testing
  - Prior to initiation of scenario development, a draft version of the test and evaluation (T&E) plan should be prepared for all participants to review and provide comments
  - Collect known cyber intrusion information targeting DOD systems from Joint and Service-level cyber commands to identify potential attack scenarios
  - Involve functional and technical SMEs from system(s) under consideration for their perspective on potential attack scenarios
  - Once scenarios have been defined, the next step is to review the system architecture, network architecture as well as geographic footprint. With that information, the ground rules can be effectively documented so that executive-level input and planning can start as early as possible

### 3. Tabletop Exercise Development:

- What worked well?
  - Commitment from all stakeholders to provide resources and participate in Tabletop Exercise
  - Output of Tabletop Exercise provided consensus on the approach and scenarios
  - Output of Tabletop Exercise clearly identified what stakeholders wanted out of the Adversarial Testing
- Points to consider for future testing
  - Tabletop Exercise mission and expectations should be provided as early as possible to stakeholders before convening in order to ensure proper participation
  - Ground rules for execution of the overall project need to be clear and properly communicated prior to Tabletop Exercise execution so that restricted Cyber Opposing

Force (OPFOR) movements are not considered during Tabletop Exercise (e.g., approved and unapproved domains, system components)

- Ensure that data on time to remediation are captured during Tabletop Exercise
- Ensure data are captured on sequence of team moves, including remediation steps / next actions until scenario is completed

#### **4. Adversarial Development:**

- What worked well?
  - Coordination and support across participating organization and agencies helped to ensure resources were made available and on time
  - Presence of application SME provided ability to adapt scenarios as needed based on capabilities within system
  - Daily calls in morning and afternoon provided near real-time information to stakeholders and helped ensure resources were made available as needed
  - Consistency of resources among Cyber OPFOR members helped provide continuity of operations
  - Acknowledgement and acceptance of test results along the way helped move testing further along and faster
- Points to consider for future testing
  - Cyber OPFOR has proper tools to execute tactics, techniques and procedures (TTPs) and that the identification and acquisition of these tools starts as early as possible
  - Assuming test of entire system without limitation, Cyber OPFOR should be afforded approximately 120 days prior to execution in order to:
    - Coordinate across all stakeholders
    - Understand and submit pre execution planning documentation
    - Have enough time to scan lab instance of system in order to be more efficient during the Adversarial Testing phase
  - Cyber OPFOR staffing should consist of approximately 4-6 operators with access to:
    - Application SME / system architect
    - Operating system SME (as needed)
    - Database/application SME that can provide response or access to back end of application to see effects of injection attacks
  - The following documentation should be provided approximately 30 days prior to execution:
    - Previous Blue Team testing with results
    - Current versions of operating systems
    - Latest patch levels for associated operating system, as well as application-level patches
    - Architectural diagrams, including interfaces with other systems
    - List of custom-built objects provided by system owners

#### **5. Data Assessment:**

- What worked well?
  - Data were provided to analysis team in short order
  - An automated tool was used to sort the data, which made analysis more efficient
  - Having a system SME who understands financial and system data helped eliminate

- false positives quickly and provided context to exceptions that might otherwise take more time to resolve
- Points to consider for future testing
    - Inclusion of Personally Identifiable Information (e.g., bank account, social security number, etc.) would provide ability to have whole data records available to analytic team and therefore identify anomalies sooner
    - Thresholds and business rules for sorting data should be defined prior to analysis
    - Initial analysis should cover a data set spanning two years (current business year and one prior). Agreement from stakeholders should be obtained ahead of time so that additional data can be gathered should initial analysis require more years to be assessed
    - Data set should be run once with automated tool and then reviewed for sufficiency of sorting logic. If refinement needs to take place, document changes, change sorting logic and then run data again
    - If exceptions are found during data analysis, access to live system data needs to be available to analysts in order to be more efficient with time and remove any false positives