



OPERATIONAL TEST
AND EVALUATION

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

JUL 27 2016

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

SUBJECT: Cybersecurity Operational Test and Evaluation Priorities and Improvements

Reference: (U) DOT&E Memorandum, "Cybersecurity Testing of Industrial/Real-time Control Systems (ICS/RCS)," August 3, 2015 (S/NF)

The field of cybersecurity continues to evolve rapidly as both new threats and new defensive capabilities emerge and are fielded, but there are a number of key areas where our ability to test and evaluate these capabilities continues to lag. The purpose of this memorandum is to identify areas where the operational test and evaluation community should accelerate development of the tools and techniques necessary to conduct cybersecurity assessments which emulate the full range of potential threats in a consistent and rigorous way.

Non Internet Protocol Data Transmission

Aircraft using military standard (MilSTD) 1553 data buses or commercial equivalents (such as Aeronautical Radio INC (ARINC) 429 as well as 700 and 800 series high speed avionics data buses), and vehicles using both MilSTD 1553 and commercial Controller Area Network (CAN) bus protocols are potentially vulnerable to cyber attacks via code and data inserted across these communications protocols. At present, the ability to test against these threat vectors is rudimentary. Some Systems Commands and Test Agencies, notably Naval Air Systems Command and the 46th Test and Evaluation Squadron, are already examining this area, and all Operational Test Agencies should collaborate to develop methods to assess the cybersecurity of common non Internet Protocol data transmission systems.

Industrial Control Systems

Industrial Control Systems (ICS) are essential for the operation of both installations and deployable platforms such as ships and aircraft. Via the reference, DOT&E previously provided guidance on the necessity for caution in testing these components due to the risk of damage, and has invested in the development of safe test and evaluation techniques for control systems and programmable logic controllers. As these efforts evolve, test agencies must continue to use all available tools and resources to assess these systems, but the ubiquity of these systems across the



Department also warrants a concentrated effort to develop additional tools, techniques, and analytical capabilities to test and evaluate the risks and capabilities.

Multiple Spectrum Cyber Threats

The risk of adversaries introducing cybersecurity attacks via spectra and media other than the traditional computer-based networks and systems is growing. Across the Services mission-critical systems rely on radio frequency, acoustic and radar data feeds, and other non-Internet Protocol (IP) media. Operational Test Agencies must develop the means to conduct cyber attacks on systems using wireless, bluetooth, radar, and other radio frequency means as well as via sonar systems.

System-Customized Attacks

Adversaries are likely to develop custom exploits for the specialized or proprietary operating systems and software that control critical systems. The test and evaluation community should improve its cybersecurity toolset and test methodologies to include key efforts such as:

- Pre-test system reviews to identify key capabilities and attack avenues, such as the “Blue Book” effort currently being undertaken by the Air Force Research Laboratory.
- Pre-test system reconnaissance to identify potential vulnerability or credential disclosures in maintenance and other online/published sources.
- Embedding system/platform operators and designers with cyber test teams to provide the expertise necessary to exploit key system functions.

Test Preparation and Execution

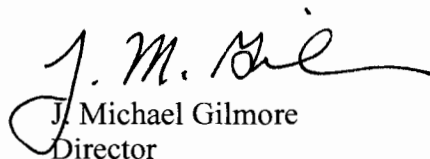
All cybersecurity operational tests require deliberate and careful planning. The following areas merit specific attention when preparing for a cybersecurity test.

- **System architecture.** A diagram or description of the physical or logical architecture of the system should be included in all test plans. The test team must be sufficiently familiar with the architecture before starting the test to assure DOT&E after the test that the entire system architecture was assessed adequately. The test team should have access to the system developers both prior to and during the test to clarify issues with system design or operations as they occur. Existing system discovery or vulnerability scans from local administrators can be an aid in outlining system architectural details and should be provided in advance of the test.
- **End-to-end testing.** All devices within the system / system-of-systems should be within the scope of the test and any device out of scope is a test limitation that must be assessed. Each test plan should include a comprehensive list of the tested systems devices including cross domain solutions, relevant IP addresses, hostnames, and operating system data and should include specific justification in terms of safety or operational risk for those devices that are not in scope. The testers should verify that all system components are present, powered-on, and

incorporated in testing; un-documented systems should be reported as a finding. Where necessary, the Operational Test Agency should make use of prior vulnerability scans or other objective evidence as available for out of scope components. The personnel operating the system, their training, behaviors, and passwords are always considered within scope of the test.

- **Test coordination and support.** Years of network and system cybersecurity testing has demonstrated that a dedicated adversary can gain access to networks and systems using compromised credentials, given enough time. Lack of network access or credentials at the start of a test can hinder test execution and reduce the effective test duration. Operational Test Agencies should account for this by obtaining appropriate credentials from system operators and administrators, or extending test schedules to allow for the red team to find and compromise the needed credentials. The number of personnel and test duration should allow for a comprehensive examination of the system under test.
- **Test execution.** While the Cooperative Vulnerability and Penetration Assessment should help determine the areas to be examined, the Adversarial Assessment should always be structured to allow for the discovery of additional threat vectors. During both phases, the ability for system defenders to detect cyber events should be assessed. Test teams should also develop capabilities that range from “difficult to detect” to “easy to detect,” and employ them in this order during Adversarial Assessments. This will allow us to collect additional data on defenders’ ability to protect and monitor systems and data, and effectively respond when faced with threats of varying sophistication.
- **Data delivery.** All test data must be provided to DOT&E no later than 60 days after test completion. It is not necessary to wait until all the documents are assembled – artifacts such as data sheets, surveys, scan outputs, and other immediately available data must be provided as soon as they are available. All validated vulnerabilities found during testing must be reported, including those that have been corrected during or between test phases.

The Secretary of Defense and all of the Services have articulated the need to improve the Department’s capability to develop cyber-hardened systems and ensure the survivability of our most critical systems. Ensuring that we can robustly test and identify weaknesses and vulnerabilities so they can be corrected is an essential part of this effort. I am dedicated to working with you in your efforts to continually expand and improve your test teams’ capabilities and reporting. I urge you to make these priorities a focus of the ongoing technical exchanges and collaboration amongst the Operational Test Agencies.


J. Michael Gilmore
Director