

Cybersecurity – Appendix E Command and Control System Example

<The following information is provided in Appendix E only if not already included in the body of the TEMP. The cybersecurity information need not be duplicated in both places.>

The Operational Test Agency (OTA) will perform cybersecurity testing as part of OT&E for the Warfighter Command and Control System (WC2S) in accordance with 1 Aug 2014 DOT&E guidance. Prior to these tests, WC2S system will have a signed Authority to Operate.

E.1. System Description A unit equipped with WC2S is able to communicate between the Joint Warfighting Command and deployed Joint Warfighting Units. WC2S allows commanders at the Joint Warfighting Command to receive and synthesize intelligence from unclassified and classified sources, and to issue orders in those domains. WC2S also hosts database services at all classification levels. Units equipped with WC2S perform cyber defense functions interoperating with the Defense Information Systems Agency (DISA) Global Support Center – North America (GNSC-NA) for unclassified and secret networks and the Defense Intelligence Agency (DIA) Regional Support Center (RSC) for the JWICS network.

E.2. System Threats A full range of cyber adversaries with nascent, limited, moderate, and advanced capabilities will target WC2S. Adversaries will attempt to compromise the system; exfiltrate, infiltrate, or corrupt data; disrupt system operations; and, if possible, physically destroy equipment. Additional cyber threat information for the WC2S is provided in the System Threat Assessment Report (STAR) and the Computer Network Operations Capstone Threat Assessment (IO Capstone, Volume 10) (CORRECTED), 2nd Edition, May 2013, DIA-08-1209-908.A.

E.3. WC2S Architecture and Test Boundary

WC2S comprises servers hosted at the Joint Warfighting Command Headquarters with unclassified, secret, and TS/SCI enclaves (see Figure E-1). In all three enclaves, there are database servers, and infrastructure and customer-facing services. On the unclassified enclave, WC2S receives and delivers data via NIPRNet, including web applications, and physical media devices. The unclassified enclave transfers information to the secret enclave via an approved cross-domain solution and connects via Ethernet (RJ-45) to the legacy system that WC2S is replacing.

In addition to the unclassified data that arrives via the cross-domain solution, the WC2S secret enclave receives data via the SIPRNet and physical media devices. WCS2 has a web-based interface for SIPRNet users, similar to the NIPRNet version, to allow those users to query the secret database. The TS/SCI database consists of the data transferred from the secret and unclassified enclaves via the attached cross-domain solution and JWICS data. JWICS users can use a virtual private network (VPN) to connect and query the WC2S database.

Cybersecurity – Appendix E Command and Control System Example

Finally, commanders can push appropriately-tagged intelligence products and tactical messages from the TS/SCI and secret enclaves down to the lower-classification enclaves via the cross-domain solutions.

The architecture, proposed test boundary for the CVPA and AA, and external interfaces of the WC2S are shown in Figure E-1.

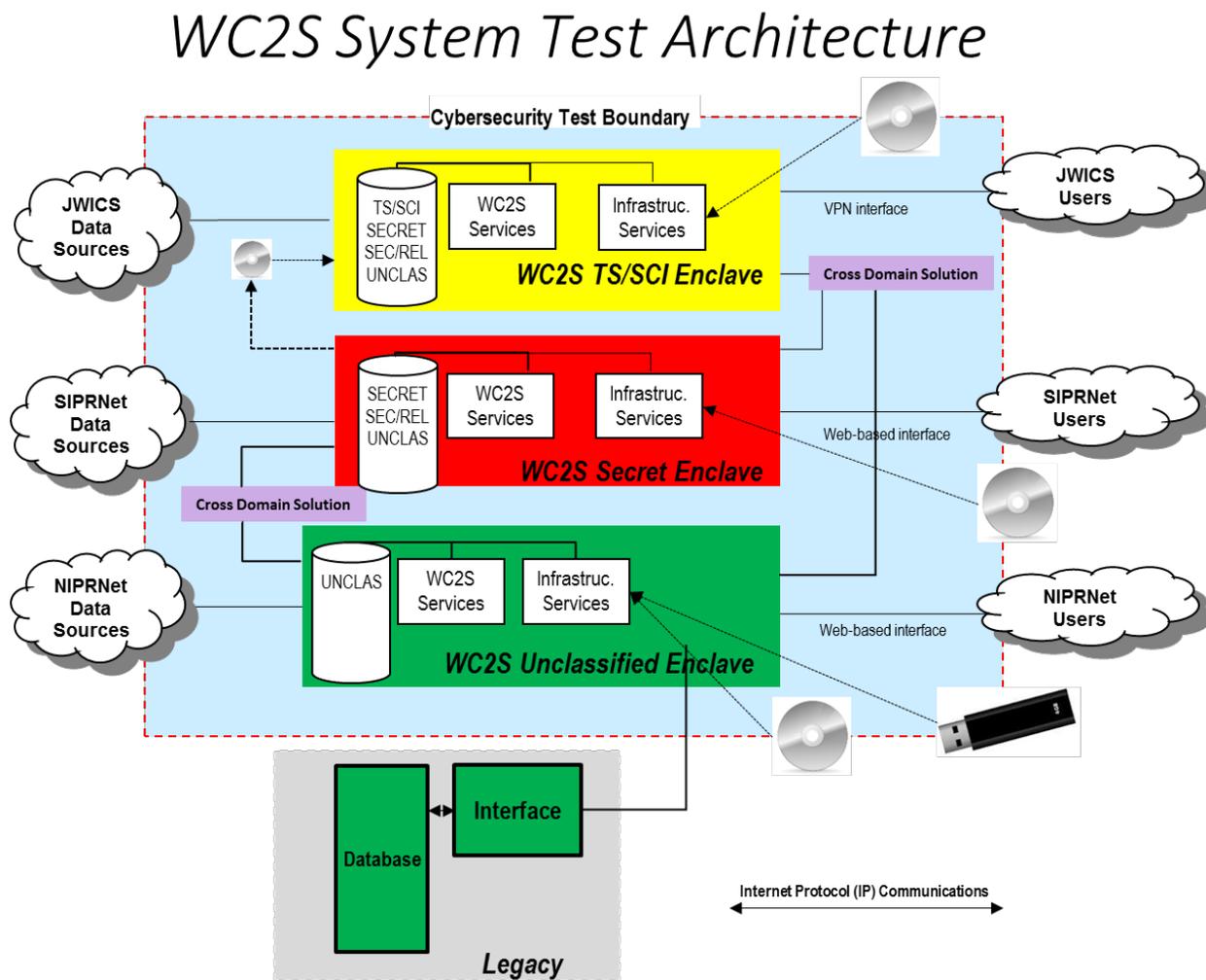


Figure E-1. WC2S System Test Architecture

In typical operations, cyber defense for the WC2S is provided locally (Tier 3) by the system operators and system administrators, including a contingent of sustainment support from the development contractor. The Tier 2 Computer Network Defense Service Provider (CNDSP)¹ for the unclassified and secret portions is the Defense Information Systems Agency (DISA) Global Support Center – North America (GNSC-NA) in Columbus, Ohio. The JWICS Tier 2 CNDSP is the Defense Intelligence Agency (DIA) Regional Support Center (RSC). See Table E-1 for each organizations cyber defense and test responsibilities.

¹ Sometimes called Cybersecurity Defense Service Provider (CDSP)

Cybersecurity – Appendix E Command and Control System Example

Table E-1. WC2S Cyber Defenders’ Roles and Responsibilities

| Cyber Tier | Role | Cyber Defense Responsibility | Test Responsibility |
|--|---|---|---|
| Local Subscribers and Defenders (Tier 3) | Commander WC2S Operations Center (Network AO/Owner) | Ensure that the network is maintained and available to support operations. | The Network AO/Owner is responsible for identifying personnel for testing support under their control (example, Network or System Administrators) and ensuring the personnel availability for supporting the test efforts. The roles can be combined if the Network AO/Owner is the same as the Facility Owner/Ops or System Program Manager/Owner. |
| | Commander WC2S Operations Center Facility Owner/Ops | Establishes physical security for networks operating within the facility. | The Facility Owner/Ops is responsible for identifying personnel for testing support under their control (example, Network or System Administrators) and ensuring the personnel availability for supporting the test efforts. The roles can be combined if the Facility Owner/Ops is the same as the Network AO/Owner or System Program Manager/Owner. |
| | WC2S Program Office (System Program Manager/Owner) | Designs and implements the system with cyber security as a priority. Creates patches to identified vulnerabilities in a timely manner. Identifies and publishes mitigation techniques to known vulnerabilities until patches are implemented. | The System Program Manager/Owner is responsible for identifying personnel for testing support under their control (example, Network or System Administrators) and ensuring the personnel availability for supporting the test efforts. The roles can be combined if the System Program Manager/Owner is the same as the Facility Owner/Ops or Network AO/Owner. |
| | Vandenberg Base Network Administrator (Network Administrator) | Ensures that the Network is patched and only accessed by authorized users. Implements actions to mitigate known vulnerabilities. Configures Host Based Security Systems. Monitors the system for unauthorized and malicious activity. Reports anomalies to the Information Assurance Manager. | Responsible for providing network assistance and troubleshooting to the Red team for access needed to execute the events. This will include assisting with placement of remote access devices or virtual machines employed on the network infrastructure. |
| | WC2S Local System Administrator | Ensures that the system is patched and only accessed by authorized users. Implements | Responsible for providing system level assistance and troubleshooting to the Red |

Cybersecurity – Appendix E Command and Control System Example

| Cyber Tier | Role | Cyber Defense Responsibility | Test Responsibility |
|-------------------------------|--|--|--|
| | (System Administrator) | actions to mitigate known vulnerabilities. Monitors the system for unauthorized and malicious activity. Reports anomalies to the Network Administrator or the Information Assurance Manager. | team for access needed to execute the events. This will include assisting with troubleshooting issues with the system, passwords, or access management. |
| | Vandenberg Air Force Base IAM (Information Assurance Manager) | Ensures that information systems are compliant with the Information Assurance Vulnerability Management Program and all applicable Security Technical Implementation Guides. Ensure security incidents are reported and corrective action taken. The IAM operates the Tier 3 Help Desk. | Trusted Agent responsible for assisting with deconfliction of events if needed and assist in ensuring that the test is executed in a secure posture. Assist in data collection and providing information needed for the report from this Tier Level and participating in any post-test events as needed. |
| Unclassified & SIPRNET Tier 2 | DISA Global Support Center (Cyber Network Defense Service Provider) | Certified and accredited by US Cyber Command. Provides component attack detection, malware protection, situational awareness, and incident response and analyses. The CNDSP coordinates the reporting flow between Tier 1 and Tier 3 and operates Tier 2 Help Desk. | Trusted Agent responsible for assisting with deconfliction of events if needed and assist in data collection or providing information needed for the report. |
| JWICS Tier 2 | DIA RSC (Cyber Network Defense Service Provider) | As directly above. | As directly above. |
| Tier 1 | Joint Force Headquarters – Department of Defense Information Network Joint Operations Center | Centrally coordinates and directs cyber network defense that affect more than on DoD Component. Coordinates with law enforcement and counter-intelligence operations. | Trusted Agent responsible for assisting with deconfliction of events if needed and assist in ensuring that the test is executed in a secure posture. Assist in data collection and providing information needed for the report from this Tier Level and participating in any post-test events as needed. |

E.4. Cooperative Vulnerability and Penetration Assessment (CVPA) The OTA will employ the Army Research Laboratory Survivability Lethality Analysis Directorate (ARL/SLAD) to perform the Cooperative Vulnerability and Penetration Assessment (CVPA) during the OA. ARL/SLAD will perform the CVPA on the operationally representative WC2S, including the use

Cybersecurity – Appendix E Command and Control System Example

of local cybersecurity defenders such as system operators and system administrators to support data collection (e.g., through interviews). ARL/SLAD will use accredited tools and processes, which include automated scans and manual inspection and will execute their activities from the insider, nearsider, and outsider postures. All external interfaces to the WC2S will be active and accessible; the proposed test boundary is shown in Figure E-1. ARL/SLAD will collect, at a minimum, the data in Attachments A and B of DOT&E guidance. ARL/SLAD will provide a full report and all data will be provided to DOT&E within 45 days of the assessment. Resources required for this test can be found in Table E-2. The OTA will submit the CVPA test plan to DOT&E for approval 90 days prior to execution.

E.5. Adversarial Assessment (AA) The OTA will conduct an Adversarial Assessment (AA) during the IOT&E using the Army Threat Systems Management Office (TSMO) to portray the cyber threat. TSMO is an NSA-certified, USCYBERCOM-accredited cyber threat team. TSMO will execute the AA using their accredited tools and processes and portray a representative cyber threat (insider, nearsider, and outsider) in accordance with the WC2S STAR, the DIA Computer Network Operations Capstone Threat Assessment, and the W2CS Computer Network Operations (CNO) Annex to the Threat Test Support Package. TSMO will obtain any and all special authorizations from DIA needed to operate on JWICS. The OTA will conduct the assessment in the context of WC2S mission operations, with representative data sources, network traffic, and external interface connectivity; the proposed test boundary is shown in Figure E-1. The assessment will include operationally representative network defense, including local user and administrator functions and will measure the detect and react abilities of a unit equipped with the WC2S and interoperating with the Tier 2 CNDSPs, the DISA GNCS-NA and DIA RSC. Because of the complexity of the system and the extent of the cyber defense capabilities to be exercised, an extended assessment period is planned (see schedule below.)

During the Adversarial Assessment, the OTA will collect and report, at a minimum, the data in Attachment C of the DOT&E guidance, which requires cyber-trained protect, detect, react, and restore (PDRR) data collectors located in both the local and Tier 2 network defense locations. Direct measurement of mission effects will be made; however, if such a demonstration would interfere with real world operations, the OTA will evaluate mission effects using independent subject matter experts and the details of the attacks performed during the Adversarial Assessment. These subject matter experts will consider the effect of the attacks and any demonstrated cyber defender responses on the execution of mission threads and associated system performance parameters.

In the event that the network defenders do not detect malicious network activity, the OTA will inject one or more detection scenarios (white cards) in order to evaluate the reaction and response chain of events.

The OTA will submit the Adversarial Assessment plan for DOT&E approval 90 days prior to execution, and provide a report from the cyber test team along with the data collected in accordance with Attachment C of DOT&E Guidance within 45 days after the assessment.

Cybersecurity – Appendix E Command and Control System Example

E.6 Test Limitations

To avoid interfering with real-world operations, system operators will execute mission threads using simulation data sources to support mission effects data collection during the AA.

E.7 Schedule <If the CVPA and AA schedules are not already denoted in the integrated test schedule in the body of the TEMP, they should be included in the Appendix. Multiple CVPA and AA events may be required to support milestone/production decisions.>

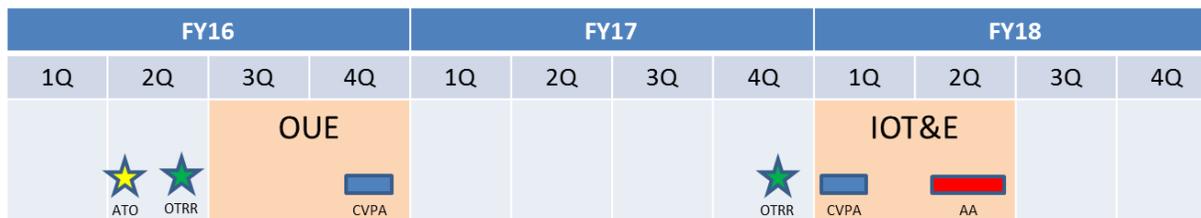


Figure E-2. WC2S Cybersecurity Test Schedule

E.8 Resources Resources required for WC2S cybersecurity testing are found in Table E-2. The figures for ARL include funds for developing advanced cyber exploits against the system; e.g., for bridging air-gaps.

Table E-2. WC2S Cybersecurity Test Resources

| SUPPORTING UNITS | FY16 | FY17 | FY18 |
|-----------------------------------|------|------|------|
| ARL/SLAD CVPA Team | \$x1 | | |
| TSMO AA Team | | | \$x2 |
| ARL/SLAD AA PDRR Data Collection | | | \$x3 |
| OTA Cybersecurity Testing Support | \$x4 | | \$x5 |
| Simulation & Instrumentation | | | \$x6 |
| Army Research Lab Testing Support | \$x7 | | \$x8 |

E.9 Evaluation Structure The OTA will use the results of WC2S cybersecurity testing, in part, to determine its operational effectiveness, suitability, and survivability. These evaluations should take into account the results of any bench testing. The OTA will assess cybersecurity under Critical Operational Issue X using the following evaluation criteria:

Table E-3: WC2S Cybersecurity Critical Operational Issue Evaluation Criteria

| Criterion | Standard | Minimum Data Required |
|---|--|--------------------------------|
| CyberX.1: Ability to Protect Information and Information Systems | Do the Vulnerabilities and Exploitations discovered during cybersecurity testing of the system put the unit’s ability to conduct missions at risk? | DOT&E 2014 Attachments A, B, C |

Cybersecurity – Appendix E Command and Control System Example

| | | |
|---|--|---|
| <p>CyberX.2: Ability to Detect Cyber Threat Activity and Malfunctions</p> | <p>Are the accuracy of detections by the WC2S-equipped unit and their defenders during cybersecurity testing sufficient to identify cyber threat activity or malfunctions that put the unit’s ability to conduct missions at risk?</p> | <p>DOT&E 2014 Attachments A and C</p> |
| <p>CyberX.3: Ability to React to Cyber Threat Activity and Malfunctions</p> | <p>Are the mitigation actions provided by the WC2S-equipped unit and their defenders during cybersecurity testing sufficient to ensure the unit’s ability to conduct missions following cyber threat activity or malfunctions?</p> | <p>DOT&E 2014 Attachment C</p> |
| <p>CyberX.4: Ability to Restore System after Cyber Threat Activity or Malfunction</p> | <p>Has the WC2S-equipped unit and their defenders demonstrated the ability to restore normal system operation and conduct missions following cyber threat activity or malfunctions?</p> | <p>DOT&E 2014 Attachments A and C</p> |
| <p>CyberX.5: Ability to Conduct Missions</p> | <p>Can a WC2S-equipped unit conduct their missions in the presence of malicious cyber threat activity or when encountering malfunctions?</p> | <p>DOT&E 2014 Attachment C</p> |
| <p>CyberX.6: Ability to Perform Reliably and Be Maintained while also being Secure from Cyber Threat Activity</p> | <p>Can the WC2S-equipped unit perform its mission reliably and perform maintenance in the operational context with a degraded cyberspace environment?</p> | <p>DOT&E 2014 Attachments A, B, and C</p> |
| <p>CyberX.7: Ability to Preserve System Physical Integrity and the Safety of Operators from Cyber Threat Activity and Malfunctions</p> | <p>In the presence of malicious cyber activity or following a malfunction, is the WC2S able to preserve its own physical integrity and the physical safety of its operators?</p> | <p>DOT&E 2014 Attachments B and C</p> |