

## Cybersecurity – Appendix E Tactical Aircraft 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 Tactical Air Vehicle System (TAVS) in accordance with 1 Aug 2014 DOT&E guidance. Prior to these tests, TAVS will have a signed Authority to Operate.

**E.1. System Description** A unit equipped with TAVS performs armed reconnaissance missions and provides operators with multiple sensors and weapons to observe and engage various enemies. In-flight digital communications are performed using multiple external data links, which are detailed below. Units equipped with the TAVS perform cyber defense functions interoperating with the 24<sup>th</sup> Air Force.

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

### **E.3. TAVS Architecture and Test Boundary**

TAVS comprises the air vehicle with its integrated sensors, weapons, propulsion systems, computers, various displays, controls, external data links (RF, SATCOM), and other networked devices hosted on-board the air vehicle (see Figure E-1). Systems that connect with the TAVS include mission planning and maintenance systems. Communications include IP and 1553 data bus traffic and some components have connectivity through both. External data sources including NIPRNet provide data used by the maintenance and mission planning components of TAVS.

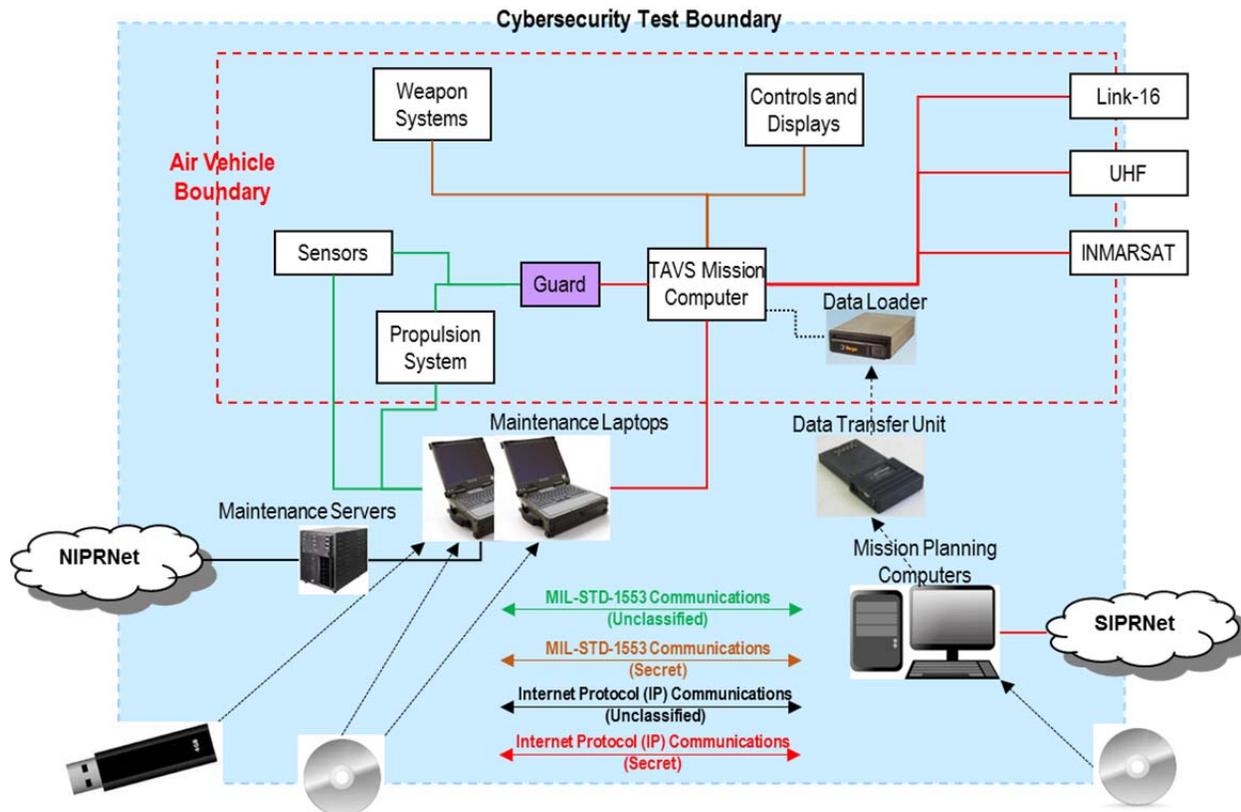
The architecture, proposed test boundary for the CVPA and AA, and external interfaces of the TAVS are shown in Figure E-1.

In typical operations, cyber defense for the TAVS is provided locally (Tier 3) by the system operators, maintainers, and system administrators, including a contingent of sustainment support from the development contractor. The 24<sup>th</sup> Air Force in San Antonio, Texas is the Tier 2 Computer Network Defense Service Provider (CNDSP)<sup>1</sup> for TAVS.

---

<sup>1</sup> Sometimes called Cybersecurity Defense Service Provider (CDSP)

## TAVS Test Architecture



**Figure E-1: TAVS Test Architecture**

**E.4. Cooperative Vulnerability and Penetration Assessment (CVPA).** The OTA will employ the 92<sup>d</sup> Information Operations Squadron (92 IOS) cyber team to perform the Cooperative Vulnerability and Penetration Assessment (CVPA) during the OA. The 92 IOS will perform the CVPA on an operationally representative TAVS, including local cybersecurity defenders such as system operators, maintainers, and system administrators to support data collection (e.g., through interviews), while the aircraft is on the flight line with all systems present and powered. The 92 IOS will execute vulnerability and penetration testing using their accredited tools and processes, which include automated scans and manual inspection. The TAVS will have all external interfaces active, and the 92 IOS will conduct assessment activities from the insider, outsider, and nearsider postures; the proposed test boundary is shown in Figure E-1. The 92 IOS will collect and report, at a minimum, the data in Attachments A and B of DOT&E guidance. 90 IOS will provide a full report and all data to DOT&E within 45 days of the assessment. Resources required for this test can be found in Table E-1. The OTA will submit the CVPA test plan to DOT&E 90 days prior to execution.

**E.5. Adversarial Assessment (AA).** The OTA will conduct an Adversarial Assessment (AA) during the IOT&E using a 177<sup>th</sup> Information Aggressor Squadron (177 IAS) to portray the cyber threat. The 177 IAS is an NSA-certified, USCYBERCOM-accredited cyber threat team. The

## Cybersecurity – Appendix E Tactical Aircraft Example

177 IAS will execute the AA using their accredited tools and processes to portray a cyber threat (insider, nearsider, and outsider) in accordance with the TAVS STAR and the DIA Computer Network Operations Capstone Threat Assessment. The OTA will conduct the assessment in the context of TAVS 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, maintainer, and administrator defense functions, and will measure the detect and react abilities of a unit equipped with the TAVS and interoperating with the Tier 2 CNDSP, 24<sup>th</sup> Air Force.

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. Where allowed by equipment damage concerns, the OTA will directly measure mission effects; otherwise, 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.

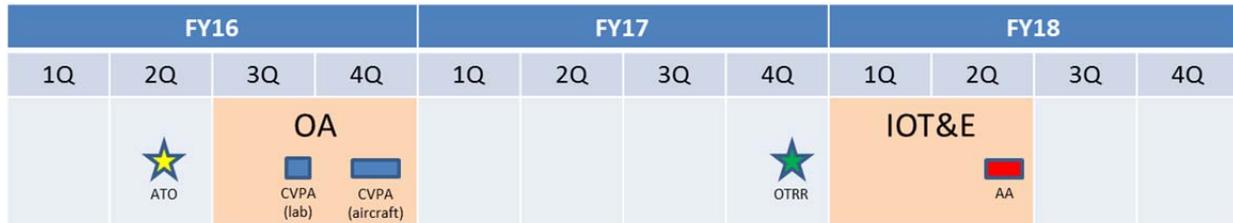
### **E.6 Test Limitations**

Both the CVPA and AA will be conducted with the aircraft on the ground to ensure physical safety. Flight safety concerns related to later flight ops will not limit testing as the platform will be reimaged and recertified after both the CVPA and the AA (this process will support data collection for the Restore evaluation). System operators will be executing mission threads using simulated data to support data collection on mission effects during the AA.

If equipment damage concerns preclude the evaluation of any systems on the aircraft (e.g., avionics), independent laboratory testing of these systems will be performed. This data will be included in the CVPA report and cyber exploitations based on the findings will be white-carded in the AA.

## Cybersecurity – Appendix E Tactical Aircraft Example

**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. TAVS Cybersecurity Test Schedule**

**E.8 Resources** Resources required for TAVS cybersecurity testing are found in Table E-1. The figures for the 92 IOS CVPA Team and the Air Force Research Lab include funds for developing advanced cyber exploits against the system, e.g. for the subsystems on the 1553 bus.

**Table E-1. TAVS Cybersecurity Test Resources**

SUPPORTING UNITS	FY16	FY17	FY18
92 IOS CVPA Team	\$x1		
177 IAS AA Team			\$x2
OTA AA PDRR Data Collection			\$x3
OTA Cybersecurity Testing Support	\$x4		\$x5
Simulation & Instrumentation			\$x6
Air Force Research Lab Testing Support	\$x7		\$x8

**E.9 Evaluation Structure.** The OTA will use the results of TAVS 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-2: TAVS Cybersecurity Critical Operational Issue Evaluation Criteria**

Criterion	Standard	Minimum Data Required
<b>CyberX.1: Ability to Protect Information and Information Systems</b>	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
<b>CyberX.2: Ability to Detect Cyber Threat Activity and Malfunctions</b>	Are the accuracy of detections by the TAVS-equipped unit and their defenders during cybersecurity testing sufficient to identify cyber threat activity	DOT&E 2014 Attachments A and C

## Cybersecurity – Appendix E Tactical Aircraft Example

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