Cybersecurity – TEMP Body Example

1.3. System Description

(...) A unit equipped with TGVS performs armed reconnaissance missions and provides operators with sensors and weapons to observe and engage enemies. TGVS uses the Single Channel Ground and Airborne Radio System (SINCGARS) and Force XXI Battle Command Brigade and Below (FBCB2) systems to communicate digitally with other TGVSs and tactical vehicles on the battlefield.

The TGVS comprises the ground vehicle with its integrated sensors, weapons, computers, displays, controls, external data links, and other networked devices hosted on board the vehicle. Systems that connect with the TGVS vehicle include the maintenance support device and the remote computer display unit. Communications include IP and Controller Area Network (CAN) data bus traffic. External data sources including NIPRNet provide data used by the maintenance components of TGVS. Units equipped with the TGVS perform cyber defense functions interoperating with the U.S. Army Cyber Command (ARCYBER) Regional Cyber Centers (RCCs).

1.3.4. System Threats (...) A full range of cyber adversaries with nascent, limited, moderate, and advanced capabilities will target the Tactical Ground Vehicle System (TGVS). 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 TGVS is provided in the TGVS 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. (…)

3.5. Operational Evaluation Approach

(...) The OTA will use the results of TGVS cybersecurity testing, in part, to determine its operational effectiveness, suitability, and survivability. These evaluations should take into account the results of any bench testing.

3.5.1. Cybersecurity Operational Test Events and Objectives. The Operational Test Agency (OTA) will perform cybersecurity testing as part of OT&E for the Tactical Ground Vehicle System (TGVS) in accordance with 1 Aug 2014 DOT&E guidance. Prior to these tests, TGVS will have a signed Authority to Operate. The overall schedule of cybersecurity testing events is shown in Figure 3-1. *<If the CVPA and AA scheduling is not already denoted in the integrated test schedule in the body of the TEMP >*

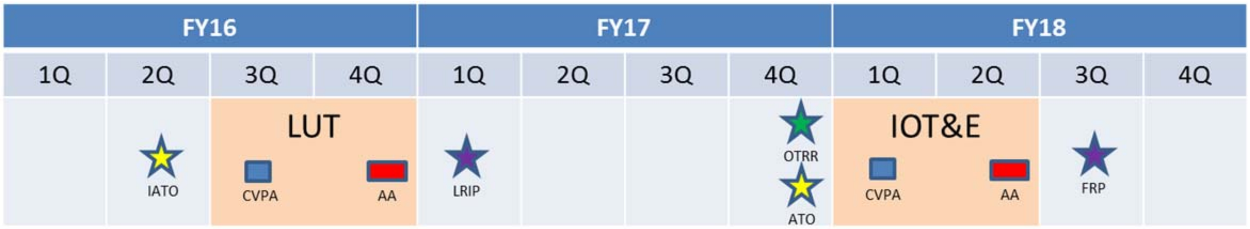

Figure 3-1. TGVS Cybersecurity Test Schedule

3.5.1.1. Cooperative Vulnerability and Penetration Assessment (CVPA). The OTA will employ the Army Research Laboratory Survivability/Lethality Analysis Directorate (ARL/SLAD) to perform Cooperative Vulnerability and Penetration Assessments (CVPAs) during both the LUT and the IOT&E prior to Adversarial Assessments. ARL/SLAD will perform the CVPAs on an operationally representative TGVS, including the use of local cybersecurity defenders such as system operators, maintainers, and system administrators to support data collection (e.g., through interviews), while the TGVS is in the motor pool with all systems present and powered. ARL/SLAD will execute vulnerability and penetration testing using their accredited tools and processes, which include automated scans and manual inspection. The TGVS will have all external interfaces active, and ARL/SLAD will conduct assessment activities from the insider, outsider, and nearsider postures; the proposed test boundary is shown in Figure 3-2. ARL/SLAD will collect and report, at a minimum, the data in Attachments A and B of DOT&E guidance. ARL/SLAD 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 4-1. The OTA will submit the CVPA test plan to DOT&E for approval 90 days prior to execution.

3.5.1.2. Adversarial Assessment (AA). The OTA will conduct Adversarial Assessments (AAs) during both the LUT and 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 AAs using their accredited tools and processes to portray a representative cyber threat (insider, nearsider, and outsider) in accordance with the TGVS STAR, the DIA Computer Network Operations Capstone Threat Assessment, and the TGVS Computer Network Operations (CNO) Annex to the Threat Test Support Package. The OTA will conduct the assessment in the context of TGVS mission operations, with representative data sources, network traffic, and external interface connectivity; the proposed test boundary is shown in Figure 3-2. The assessment will include operationally representative network defense, including local operator, maintainer and administrator defense functions and will measure the detect and react abilities of a unit equipped with the TGVS and interoperating with the Tier 2 CNDSP, the ARCYBER 2nd RCC.

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 crew safety or 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 of the end of the assessment.

3.5.1.3. Cybersecurity Test Architecture. The architecture, proposed test boundary for the CVPA and AA, and external interfaces of the TGVS are shown in Figure 3-2.

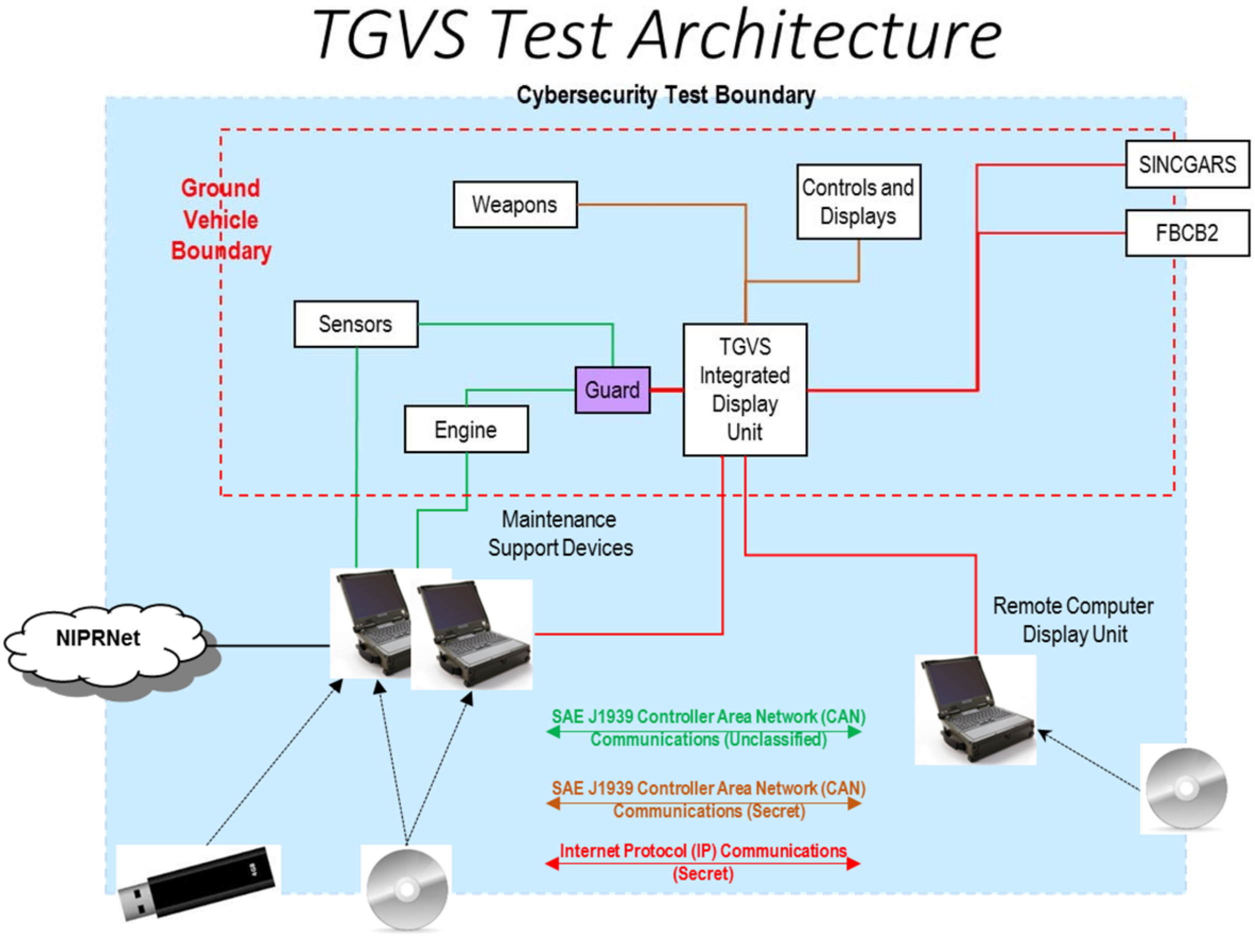
TGVS Test Architecture
Cybersecurity Test Boundary
Ground Vehicle Boundary
Weapons
Controls and Displays
SINCGARS
FBCB2
Sensors
Guard
TGVS Integrated Display Unit
Engine
Maintenance Support Devices
NIPRNet
Remote Computer Display Unit
SAE J1939 Controller Area Network (CAN) Communications (Unclassified)
SAE J1939 Controller Area Network (CAN) Communications (Secret)
Internet Protocol (IP) Communications (Secret)

Figure 3-2. TGVS Test Architecture

In typical operations, cyber defense for the TGVS is provided locally (Tier 3) by the system operators, maintainers, 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 TGVS is the U. S. Army Cyber Command (ARCYBER) Regional Cyber Center (RCC). (…)

3.5.2.1. Cybersecurity Critical Operational Issue. The OTA will assess cybersecurity under Critical Operational Issue X using the following evaluation criteria:

Table 3-1: TGVS 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
CyberX.2: Ability to Detect Cyber Threat Activity and Malfunctions	Are the accuracy of detections by the TGVS-equipped unit and their defenders during cybersecurity testing sufficient to identify cyber threat activity or malfunctions that put the unit's ability conduct missions at risk?	DOT&E 2014 Attachments A and C
CyberX.3: Ability to React to Cyber Threat Activity and Malfunctions	Are the mitigation actions provided by the TGVS-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
CyberX.4: Ability to Restore System after Cyber Threat Activity or Malfunction	Has the TGVS-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
CyberX.5: Ability to Conduct Missions	Can a TGVS-equipped unit conduct their missions in the presence of malicious cyber threat activity or when encountering malfunctions?	DOT&E 2014 Attachment C
CyberX.6: Ability to Perform Reliably and Be	Can the TGVS-equipped unit perform its mission reliably and perform	DOT&E 2014 Attachments A, B,

[1] Sometimes called Cybersecurity Defense Service Provider (CDSP)

Maintained while also being Secure from Cyber Threat Activity	maintenance in the operational context with a degraded cyberspace environment?	and C
CyberX.6: Ability to Preserve System Physical Integrity and the Safety of Operators from Cyber Threat Activity and Malfunctions	In the presence of malicious cyber activity or following a malfunction, is the TGVS able to preserve its own physical integrity and the physical safety of its operators?	DOT&E 2014 Attachments B and C

3.5.4. Test Limitations. (…) Because the unit equipped with the system normally operates in a team with other identically-equipped units that are not resourced for the AA, the scope of mission threads the operators will execute for supporting mission effects data collection may be reduced. Also, TSMO will not knowingly launch cyber attacks that could affect control of the vehicle while it is in motion.

If equipment damage concerns preclude the evaluation of any systems connected to the CAN bus, 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. (…)

4.2.5. Threat Representation. (…) Resources required for TGVS cybersecurity testing are found in Table 4-1. The figures for the Army Research Lab include funds for developing advanced cyber exploits against the system, e.g. for the subsystems on the CAN bus. (…)

Table 4-1. TGVS 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
Instrumentation			$x6
Army Research Lab Testing Support	$x7		$x8