VFC Cyber Program
Cybersecurity 5x5

Date Published: OCT 15, 2026

(U) Transportation Services Cybersecurity 5x5

(U//FOUO) Introduction: The VFC's Cybersecurity 5x5 is a concise summary that highlights five key insights alongside five opportunities for mitigation in a specific critical infrastructure sector. This product is intended to give leaders a quick snapshot of a sector's cybersecurity posture to provide awareness and inform decision-making.

(U) 5 Key Cyber Insights on Transportation Services

1. (U) Artificial Intelligence is reshaping both operations and attack methods. While transportation systems are using AI for routing, predictive maintenance, and autonomous operations, adversaries are exploiting AI to automate reconnaissance, craft spear-phishing campaigns, and identify vulnerabilities faster.
2. (U) Transportation agencies increasingly rely on connected OT systems such as signaling, traffic management, fleet telematics, and automated fare collection. These systems present attractive targets for disruption as many were not originally designed with cybersecurity in mind.
3. (U) The Transportation sector relies on large networks of vendors for software, hardware, maintenance, and analytics. Compromises in third-party systems, including ticketing vendors or maintenance contractors, can create entry points into core operations.
4. (U) Ransomware continues to be the most significant threat vector for the Transportation sector. Transit agencies, ports, airports, and freight operators remain prime targets for ransomware as service disruptions have immediate economic and public impacts.
5. (U) Funding for cybersecurity is complicated as gas tax revenues are declining, adding additional financial burden and strain on the industry and difficulties in funding all necessary improvements and security measures.

(U) 5 Opportunities for Mitigation

1. Develop and regularly exercise transportation-focused incident response plans, covering signal fallback operations, disrupted transit management, emergency coordination, and safe OT system recovery.
2. Harden National Transportation Communications for Intelligent Transportation System Protocol (NTCIP) devices with secure configurations, unique credentials, disabled defaults, and up-to-date firmware aligned with current NTCIP standards.
3. Fully assess the capabilities and gaps associated with Intelligent Transportation Systems (ITS) procurement projects; use guidance from National Cooperative Highway Research Program (NCHRP) Project 3-77 or NCHRP Report 560 to follow best-practice contracting methods.
4. Ensure RSU firmware, certificates, and message security comply with IEEE 1609.2 so safety-critical messages remain authenticated, private, and resistant to spoofing or replay.
5. Use the Federal Transit Administration's Cybersecurity Assessment Tool for Transit (CATT) to evaluate cybersecurity posture and plan targeted network hardening improvements.

This is UNCLASSIFIED//FOR OFFICIAL USE ONLY information protected by Virginia Code Section 52-48, unless otherwise noted. ***Further dissemination of this information outside of your organization is prohibited unless written approval is obtained from the VFC prior to dissemination****. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Pursuant to Virginia Code Section 52-48(D), anyone violating distribution restrictions may be prosecuted and may be prohibited from receiving future reports. Please contact the Virginia Fusion Center at (804) 674-2196 if you have any questions or need additional information.*