2021 FTA Joint SSO and RTA Virtual Workshop

CISA Cybersecurity Briefing

Benjamin Gilbert
Cybersecurity Advisor, Region III
Cybersecurity and Infrastructure Security Agency

October 2021
U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

DEFEND TODAY, SECURE TOMORROW
CISA Offers No-Cost Cybersecurity Services

• Preparedness Activities
  • Cybersecurity Assessments
  • Cybersecurity Training and Awareness
  • Cyber Exercises and “Playbooks”
  • Information / Threat Indicator Sharing
  • National Cyber Awareness System
  • Vulnerability Notes Database
  • Information Products and Recommended Practices

• Response Assistance
  • Remote / On-Site Response and Assistance
  • Incident Coordination
  • Threat intelligence and information sharing
  • Malware Analysis

• Cybersecurity Advisors
  • Incident response coordination
  • Cyber assessments
  • Workshops
  • Working group collaboration
  • Advisory assistance
  • Public Private Partnership Development

Contact CISA to report a cyber incident
Call 1-888-282-0870 | email Central@cisa.dhs.gov | visit https://www.cisa.gov
• Conducts cybersecurity outreach to critical infrastructure and other stakeholders
• Promotes the Framework, CISA cybersecurity resources and best practices

• February 2013, in collaboration with DHS NPPD, developed the Framework in concert with public and private sector stakeholders
• Released version 1.1 April 2018: [https://www.nist.gov/cyberframework](https://www.nist.gov/cyberframework)
The Cybersecurity Framework

- Establishes a common perspective and vernacular,
- Provides risk-based guidelines,
- Is collaboration-oriented, and
- Is internationally recognized
Cybersecurity Evaluation Tool

**Purpose:** Assesses control system and information technology network security practices against industry standards.

**Facilitated:** Self-Administered, undertaken independently

**Benefits:**
- Immediately available for download upon request
- Understanding of operational technology and information technology network security practices
- Ability to drill down on specific areas and issues
- Includes self-evaluations against NIST CSF v1.1
- Also includes self-evaluations with CMMC, RRA, and other maturity models

CSET®
CYBER SECURITY EVALUATION TOOL
Version: 10.3.0.0
Range of Cybersecurity Assessments

- Cyber Resilience Review (Strategic)
- External Dependencies Management (Strategic)
- Cyber Infrastructure Survey (Strategic)
- Cybersecurity Evaluations Tool (standards based)
- Validated Architecture Design Review (Tactical)
- Cyber Hygiene (Technical)
  - Phishing Campaign Assessment
  - Vulnerability Scanning
  - Web Application Scanning
  - Remote Penetration Test
  - Risk and Vulnerability Assessment (Technical)
BE CYBER SMART

#CyberMonth

CYBERSECURITY AWARENESS MONTH 2021
No-Cost CISA Cybersecurity Services

• Preparedness Activities
  • Cybersecurity Assessments
  • Cybersecurity Training and Awareness
  • Cyber Exercises and “Playbooks”
  • Information / Threat Indicator Sharing
  • National Cyber Awareness System
  • Vulnerability Notes Database
  • Information Products and Recommended Practices

• Response Assistance
  • 24/7 Response assistance and malware analysis
  • Incident Coordination
  • Threat intelligence and information sharing

• Cybersecurity Advisors – Regionally deployed advisors
  • Incident response coordination
  • Public Private Partnership Development
  • Advisory assistance and cybersecurity assessments

CISA Contact Information

| Benjamin Gilbert, CISSP, CRISC, CEH | Benjamin.gilbert@hq.dhs.gov  
| Integrated Operations Division – Regional Operations | iodregionaloperations@cisa.dhs.gov  

| CISA URL | https://www.cisa.gov  

| To Report a Cyber Incident to CISA | Call 1-888-282-0870  
| Email Central@cisa.dhs.gov  
| visit https://www.cisa.gov |
DHS THREAT INTELLIGENCE BRIEF - TRANSPORTATION SYSTEMS SECTOR

Anthony Militano
Branch Chief – CISA Intelligence, Analysis Branch
Cybersecurity and Infrastructure Security Agency
Agenda

Defining the Threat Environment

Threat Overview – Transportation Systems Sector

Cyber Threat Actor Capabilities and Attributes

Rail – Mass Transit
Defining the Threat Environment

Threat = Capability + Intent + Opportunity

Threat Mitigation = Threat - Opportunity
The Transportation Systems Sector faces a multitude of cyber threats at the hands of criminals, hackers, insiders, and nation-state actors.

Disruptive attacks, such as cyber physical manipulation, GPS spoofing and jamming, represent low-frequency—but potentially catastrophic threats—to the transportation industry.

Interdependencies between layers of air, rail, and maritime transportation systems provide actors with opportunities to perform operations leveraging a variety of attack surfaces.
Cyber Threat Actor Capabilities and Attributes

**APT and Nation State Programs**
- Offensive, espionage programs align w/ economic, security, natl. strategy
- Capable of destructive attacks against critical infrastructure
- May develop and deploy highly sophisticated, specialized tool kits
- Frequently exploit well-known tools, tactics, vulnerabilities
- Significant threat to intellectual property and supply chain

**Criminal Hacktivists**
- Target selection usually deliberate, coincides with high profile events
- Intended effect varies greatly; doxing, defacements, DoS attacks
- 'Hacking as a Service': credentials, bots, tools for a nominal price
- Secondary effect: damage to credibility and public trust

**Cyber Criminals**
- Ransomware: zero sum equation; lifeline sectors, critical services at risk
- Employ timely, high quality social engineering tools and tactics
- Use of modular malware, publicly known vulnerabilities and stealthy infrastructure (bots, exfil points, C2 nodes) increases probability of success
Rail cyber-reliance includes:

- Positive Train Control (PTC)
- Switch Positioning:
- Data and Voice Communication System
- Wayside Signal Systems
- Distributed Power
- End of Train Devices
- Highway Grade Crossing Systems
Cyber Espionage & Cyberattack Threats:

Chinese government cyber actors compromise New York MTA

The most frequent TTP known to compromise rail victim networks since January 2020 was ransomware.

Cybercriminals mostly targeted networks containing:
- Business data
- Personally Identified Information (PII)
- Credit card information from passenger ground service systems

Domestic or Canadian MTPR:
- 7 Ransomware attacks
- 3 Non-ransomware, malicious cyber activity (beaconing to foreign IP, DDoS, data breach, etc.

Foreign MTPR: 6 Ransomware attacks or other malicious cyber activity on entities

Most common Ransomware used: Nefilim, Netwalker, REvil, Ransom X

Cyberattack on Iranian Rail System
Please direct any questions or concerns regarding this brief to CISA Intelligence.

CISA.IOD.INTEL.ANALYSIS_Federal@cisa.dhs.gov
CYBER RISK SUMMARY:
TRANSPORTATION SYSTEMS SECTOR

OCTOBER 2020 – JULY 2021

Christopher Hild
Information Security Specialist, Vulnerability Management
Cybersecurity and Infrastructure Security Agency (CISA)
CISA recommends that all Transportation Systems (TS) entities review the following findings—derived from an analysis of 33 TS entities enrolled in CISA’s free Cyber Hygiene (CyHy) Vulnerability Scanning (VS) service and 11 TS entities that received CISA Assessment services from October to July 2021—and take appropriate action to reduce vulnerability, risk of compromise, and maintain resilient cybersecurity practices.

Existed Risky Services

54.5% of scanned TS entities exposed risky services on internet-accessible hosts that, absent compensating controls, can provide threat actors with initial access and avenues for command and control (C2) and data exfiltration.

Unsupported Operating Systems (OSs)

48.5% of scanned TS entities ran unsupported Windows operating systems (OSs) that no longer receive routine security updates on at least one internet-accessible host at the end of Jul 2021, increasing exposure to vulnerabilities that can enable compromise.

Spearphishing Weaknesses

54.5% of TS entities that participated in Remote Penetration Testing (RPT) had email filtering controls that were bypassed by spearphishing emails, suggesting threat actors may have similar success when launching phishing attacks.
Recommendations

Defend against ransomware
- Practice network segmentation and keep offline, encrypted backups of data.
- Maintain cyber incident response plans.
- Refrain from paying a ransom and report incidents to CISA and to your local FBI field office.

Improve phishing defenses
- Provide training to all levels of staff on how to identify and report phishing emails.
- Implement spam-filtering and border protections such as DMARC.
- Leverage outbound web-browsing protections to mitigate consequences if a phishing email defeats borderer protections and trained staff.

Improve patch management
- Prioritize remediation of vulnerabilities using a risk-based approach that considers likelihood of attack, ease of exploitation, and the magnitude of probable impact.
- Modify patch management strategies to prioritize patching vulnerabilities with known exploits.

Secure potentially risky service
- Evaluate the business need for exposing risky services on internet-accessible hosts.
- Disable or block all unnecessary services.
- If certain services are required, then operate the services with proper configurations and security features enabled, such as multifactor authentication (MFA).

CISA Insights
September 27, 2021
From Oct 2020 to Jul 2021, newly enrolled TS entities reduced active vulnerabilities by an average of 22.4% within the first three months of conducting vulnerability scanning.

CISA offers free cybersecurity services to TS entities:

- **Vulnerability Scanning**: Persistent scanning of internet-accessible systems for vulnerabilities, configuration errors, and suboptimal security practices.

- **Web Application Scanning**: Assesses the “health” of publicly accessible web applications by checking for known vulnerabilities and weak configurations.

- **CISA Assessments**: Agency cybersecurity assessments (e.g., RPT) provide actionable and risk-informed recommendations.

Email vulnerability_info@cisa.dhs.gov for more information and to sign up.
Cyber Risk Summary Questions and Feedback:
CSD_VM_Insights_Intake@cisa.dhs.gov

Cyber Hygiene Services:
https://www.cisa.gov/cyber-hygiene-services
vulnerability_info@cisa.dhs.gov
The Cybersecurity and Infrastructure Security Agency (CISA) Cyber Assessment team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA’s Cyber Hygiene Vulnerability Scanning (CyHy VS) is “internet scanning-as-a-service.” This service continuously assesses the “health” of your internet-accessible assets by checking for known vulnerabilities and weak configurations, and recommends ways to enhance security through modern web and email standards.

**OBJECTIVES**

- Maintain enterprise awareness of your internet-accessible systems
- Provide insight into how systems and infrastructure appear to potential attackers
- Drive proactive mitigation of vulnerabilities and reduce risk

**SCANNING PHASES AND STAGES**

**PHASES**

- Target Discovery: Identify all active internet-accessible assets (networks, systems, and hosts) to be scanned
- Vulnerability Scanning: Initiate non-intrusive checks to identify potential vulnerabilities and configuration weaknesses

**STAGES**

**Pre-Planning**

- Request Service
- Receive Cyber Hygiene brief
- Provide target list (scope)
- Sign and return documents

**Planning**

- Confirm scanning schedule
- Pre-scan notification

**Execution (Tailored*)**

- Initial scan of submitted scope
- Rescan scope based on detected vulnerability severity:
  - 12 hours for “critical”
  - 24 hours for “high”
  - 4 days for “medium”
  - 6 days for “low”
  - 7 days for “no vulnerabilities”

**Post-Execution**

- Ongoing weekly summary report
- Vulnerability mitigation recommendations
- Detailed findings in consumable format

---

CISA | DEFEND TODAY, SECURE TOMORROW
ABOUT

Our Team
This CISA team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the nation’s physical and cyber infrastructure.

Our Services
CISA Cyber Assessments services provide:

- A proactive, risk-based approach to analyzing stakeholder systems
- Expertise in identification of vulnerabilities, risk evaluation and prioritized mitigation guidance
- Comprehensive services that empower stakeholders to increase speed and effectiveness of their cyber response capabilities

Additional Information
CISA’s security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.

GET STARTED
Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at vulnerability_info@cisa.dhs.gov to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.

MISSION AND VISION
Mission: Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation’s cyber infrastructure.

Vision: To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats and fostering partnerships across the government landscape.

For more information or to seek additional help, contact us at vulnerability_info@cisa.dhs.gov.