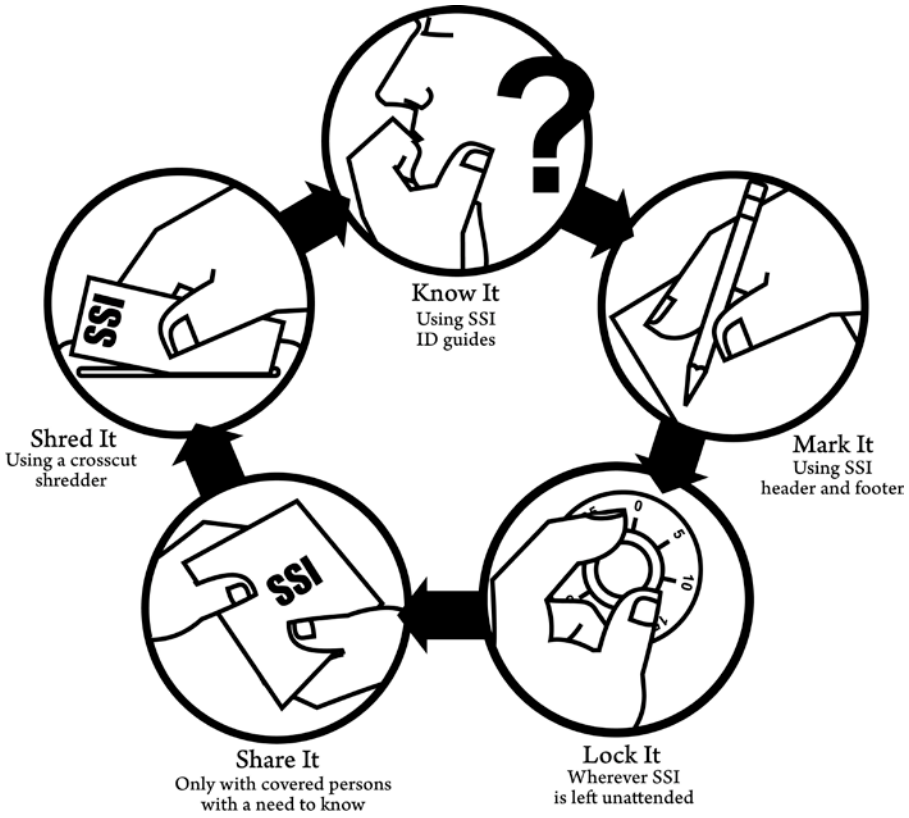
DEPARTMENT OF HOMELAND SECURITY

# SENSITIVE SECURITY INFORMATION

## Cover Sheet




**For more information on handling SSI, contact SSI@dhs.gov.**

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

DHS Form 11054 (8/10) Reference: 49 CFR § 1520.13, Marking SSI

OMB Control Number 1652-0074

# Sensitive Security Information

**This record contains Sensitive Security Information when completed**

Transportation Security Administration

U.S. Department of Homeland Security

Version 1.0

**Instructions:** Select the appropriate response for each question below. The Additional Information column **must** include the following information based on response:
1) If answering "Yes", either list the security plan, policy, document name, etc. with chapter/section; or if implemented but not documented, provide a brief explanation.
2) If answering "No", identify the gap, intended mitigation(s) measures, and the mitigation timeline.
For any questions concerning the completion of this assessment please email SurfOpsRail-SD@tsa.dhs.gov

## TSA Surface (Rail and Public Transportation) Cybersecurity Vulnerability Assessment

| | | | |
|---|---|---|---|
| Owner/Operator Name: | | Assessment Completed Date: | |
| Submitter (First/Last): | | Submitter Title: | |
| Submitter Email: | | Submitter Contact Number: | |
| Cybersecurity Coordinator (First/Last): | | Cybersecurity Coordinator Title: | |
| Cybersecurity Coordinator Email: | | Cybersecurity Coordinator Contact Number: | |
| 24 Hour Operations Center phone number, if applicable: | | | |

| Question # | Question | Answer (Yes/No) | Additional Information |
|---|---|---|---|
| **Cyber Asset Security Measures** | | | |
| 1.00 | Do your cybersecurity plans incorporate any of the following approaches? | | |
| 1.00A | National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity | Select | |
| 1.00B | U.S. Department of Homeland Security, Transportation Systems Sector Cybersecurity Framework Implementation Guidance | Select | |
| 1.00C | Industry-specific methodologies | Select | |
| 1.00D | Other (if checked, elaborate) | Select | |

# Sensitive Security Information

**This record contains Sensitive Security Information when completed**

| Asset Management | | | |
|---|---|---|---|
| 2.00 | Has your company established and documented policies and procedures for the following? | | |
| 2.00A | Assessing and maintaining configuration information. | Select | |
| 2.00B | Tracking changes made to surface transportation cyber assets. | Select | |
| 2.00C | Patching/upgrading operating systems and applications. | Select | |
| 2.00D | Ensuring that the changes do not adversely impact existing cybersecurity controls. | Select | |
| 2.00E | Other (if checked, elaborate) | Select | |
| 2.01 | Does your company evaluate and classify surface transportation cyber assets using the following criteria? | | |
| 2.01A | Cyber assets that are operational technologies (OT/ICS/SCADA systems) that can control surface operations. | Select | |
| 2.01B | Cyber assets that are OT systems that monitor surface operations. | Select | |
| 2.02 | Has your company developed and maintained a comprehensive set of network/system architecture diagrams or other documentation, including nodes, interfaces, remote and third-party connections, and information flows? | Select | |
| 2.03 | For cyber assets that can control surface operations, does the OT environment have a detailed software and hardware inventory of cyber asset endpoints? | Select | |
| 2.04 | For cyber assets that can control surface operations, has an inventory of the components of the operating system been developed, documented, and maintained that accurately reflects the current OT/ICS/SCADA system? | Select | |

# Sensitive Security Information

**This record contains Sensitive Security Information when completed.**

| | | | |
|---|---|---|---|
| 2.05 | Does your company periodically review network connections, including remote access and third-party connections for cyber assets that can control surface operations? | Select | |
| 2.06 | For cyber assets that can control surface operations, has your company implemented the following measures? | | |
| 2.06A | Restrict user physical access to control systems and control networks by using appropriate controls. | Select | |
| 2.06B | Employ more stringent identity and access management practices (e.g., authenticators, password-construct, access control). | Select | |
| 2.07 | For cyber assets that can control surface operations, does your company review, assess, and update as necessary all cybersecurity policies plans, processes, and supporting procedures at least every 12 months, or when there is a significant organizational change? | Select | |
| 2.08 | Does your company review and assess surface transportation cyber asset functions controlling or monitoring OT systems at least every 12 months? | Select | |
| **Business Environment** | | | |
| 3.00 | Does your company have a designated individual solely responsible for cyber/ IT/ OT / SCADA security? | Select | |
| 3.01 | Does your company document new transportation cyber assets, when changes or upgrades are made to control operations resulting in the system being recognized as such? | Select | |
| **Governance** | | | |
| 4.00 | Has your company established and distributed cybersecurity policies, plans, processes, and supporting procedures commensurate with the current regulatory, risk, legal, and operational environment? | Select | |

# Sensitive Security Information

**This record contains Sensitive Security Information when completed**

| | | | |
|---|---|---|---|
| 4.02 | Does your company review, assess, and update as necessary all cybersecurity policy plans, processes, and supporting procedures at least every 36 months, or when there is a significant organizational or technological change? | Select | |
| **Risk Management Strategy** | | | |
| 5.00 | Has your company developed an operational framework to ensure coordination, communication,and accountability for information security on and between the control systems and enterprise networks? | Select | |
| **Risk Assessment** | | | |
| 6.00 | For cyber assets that can control surface operations, does your company use independent assessors to conduct surface transportation cybersecurity assessments? | Select | |
| 6.01 | Has your company established a process to identify and evaluate vulnerabilities and compensating security controls? | Select | |
| 6.02 | Does the process address unmitigated/accepted vulnerabilities in the IT and OT environment? | Select | |
| **Access Control** | | | |
| 7.00 | Has your company implemented the following measures? | | |
| 7.00A | Establish and enforce unique accounts for each Individual user and ensure each administrator has an Individual account and an administrator account. | Select | |
| 7.00B | Establish security requirements for certain types of Privileged accounts. | Select | |
| 7.00C | Prohibit the sharing of these accounts. | Select | |
| 7.01 | Does your company employ strong credential management or Active Directory monitoring throughout the company's cyber access control environment and is it documented in overarching corporate IT/OT security plans? | Select | |

# Sensitive Security Information

**This record contains Sensitive Security Information when completed**

| | | | |
|---|---|---|---|
| 7.02 | Where systems do not support unique user accounts, are appropriate compensating security controls (e.g., physical controls) implemented? | Select | |
| 7.03 | Does your company ensure user accounts are modified, deleted, or de-activated expeditiously for personnel who no longer require access or are no longer employed by the company? | Select | |
| 7.04 | Has your company implemented the following measures? | | |
| 7.04A | Establish and enforce access control policies for local and remote users. | Select | |
| 7.04B | Have procedures and controls in place for approving and enforcing remote and third-party connections. | Select | |
| 7.05 | Are access control levels of permission and privileges defined in the IT/ OT security plan? | Select | |
| 7.06 | Does your company ensure appropriate segregation of duties is in place and where this is not feasible, apply appropriate compensating security controls? | Select | |
| 7.07 | Does your company change all default passwords for new software, hardware, etc., upon installation and, where this is not feasible (e.g., a control system with a hard-wired password), implement appropriate compensating security controls (e.g., administrative controls)? | Select | |
| 7.08 | Do email and communications systems have features that automatically download attachments turned off? | Select | |
| 7.09 | Do systems only allow the execution of programs known and permitted by security policy (i.e., allow lists?) | Select | |
| **Awareness & Training** | | | |
| 8.00 | Do all persons requiring access to the company's surface transportation cyber assets receive cybersecurity awareness training? | Select | |

# Sensitive Security Information

**This record contains Sensitive Security Information when completed**

| | | | |
|---|---|---|---|
| 8.01 | For cyber assets that can control surface operations, does your company provide role-based security training on recognizing and reporting potential indicators of system compromise prior to granting access to those cyber assets? | Select | |
| 8.02 | Is there a cyber-threat awareness program for employees that includes practical exercises/testing? | Select | |
| **Data Security & Information Protection** | | | |
| 9.00 | Has your company established and implemented policies and procedures to ensure data protection measures are in place, including the following? | | |
| 9.00A | Identifying critical data and establishing classification of different types of data. | Select | |
| 9.00B | Establishing specific data handling procedures. | Select | |
| 9.00C | Establishing specific data disposal procedures. | Select | |
| **Protective Technology** | | | |
| 10.00 | Are surface transportation cyber assets segregated and protected from enterprise networks and the internet by use of physical separation, firewalls, and other protections? | Select | |
| 10.01 | Do IT/ OT systems monitor and manage communications at appropriate IT/ OT network boundaries? | Select | |
| 10.02 | Does your company employ mechanisms (e.g., active directory) to support the management of accounts for cyber assets that can control surface operations? | Select | |
| 10.03 | Does your company regularly validate that technical controls comply with the company's cybersecurity policies, plans, and procedures, and report results to senior management? | Select | |
| 10.04 | Has your company implemented technical or procedural controls to restrict the use of surface transportation cyber assets to only approved activities? | Select | |

# Sensitive Security Information

**This record contains Sensitive Security Information when completed**

| | | | |
|---|---|---|---|
| **Anomalies & Events** | | | |
| 11.00 | Has your company implemented processes to respond to anomalous activity through the following? | | |
| 11.00A | Generating alerts and responding to them in a timely manner. | Select | |
| 11.00B | Logging cybersecurity events and reviewing these logs. | Select | |
| **Security Continuous Monitoring** | | | |
| 12.00 | Does your company monitor for unauthorized access or the introduction of malicious code or communications? | Select | |
| 12.01 | Does your company monitor physical and remote user access to cyber assets that can control surface operations? | Select | |
| 12.02 | For cyber assets that can control surface operations, does your company employ mechanisms to detect components that should not be on the network? | Select | |
| 12.03 | Does your company conduct cyber vulnerability assessments as described in your risk assessment process? | Select | |
| **Detection Processes** | | | |
| 13.00 | Has your company established technical or procedural controls for cyber intrusion monitoring and detection? | Select | |
| 13.01 | Does your company perform regular testing of intrusion and malware detection processes and procedures (e.g., penetration testing)? | Select | |
| **Response Planning** | | | |
| 14.00 | Has your company established policies and procedures for cybersecurity incident handling, analysis, and reporting, including assignments of specific roles/tasks to individuals and teams? | Select | |
| 14.01 | For cyber assets that can control surface operations, are cybersecurity incident response exercises conducted periodically? | Select | |
| 14.02 | For cyber assets that can control surface operations, has your company established and maintained a process that supports 24/7 cyber-incident response? | Select | |

# Sensitive Security Information

**This record contains Sensitive Security Information when completed**

| | | | |
|---|---|---|---|
| 14.03 | Has your company established and maintained a cyber-incident response capability? | Select | |
| **Communications** | | | |
| 15.00 | Does the company have procedures in place for reporting to CISA Central, actual or suspected cyber attacks that may impact surface transportation surface industrial control systems (SCADA, PCS, DCS), measurement and telemetry systems, or enterprise-associated IT systems (IAW Security Directive 1580-21-01)? | Select | |
| **Mitigation** | | | |
| 16.00 | Do your company's response plans and procedures include mitigation measures to help prevent further impacts? | Select | |
| **Recovery Planning** | | | |
| 17.00 | Has your company established a plan for the recovery and reconstitution of surface transportation cyber assets within a time frame to align with the company's safety and business continuity objectives? | Select | |
| 17.01 | Does the company have documented procedures in place to coordinate restoration efforts with internal and external stakeholders (coordination centers, Internet Service Providers, victims, vendors, etc.)? | Select | |
| **Continuous Improvement** | | | |
| 18.00 | Does your company review its cyber incident response plan annually and update it as necessary? | Select | |