U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

Surface Operations
Cybersecurity On-Site Inspection
Process Guide

Security Directive Pipeline – 2021-02C

Issued

Version

Applicability of Security Directive
Owners and operators of a hazardous liquid and natural gas pipeline or a liquefied natural gas facility notified by TSA that their pipeline system or facility is critical.

Background:

TSA issued a Memorandum dated July 21, 2022 that directed all covered pipeline owner/operators (O/O) to meet the requirements of Security Directive Pipeline-2021-02C (SD02C). The memorandum specifically directed that each O/O: 1) Establish and implement a TSA-approved Cybersecurity Implementation Plan; 2) Develop and maintain a Cybersecurity Incident Response Plan to reduce the risk of operational disruption; and 3) Establish a Cybersecurity Assessment Program and submit an annual plan that describes how the O/O will assess the effectiveness of cybersecurity measures.

The Cybersecurity Implementation Plan (CIP) must provide the information required by Sections III.A. through III.E. of SD02C and describe in detail the O/O's defense-in-depth plan, including physical and logical security controls, for meeting each of the requirements in Sections III.A. through III.E.

This CIP was required to be submitted by each O/O within 90 days of the effective date of SD02C which was July 27, 2022. The plan required review and approval by TSA and once approved, the O/O must implement and maintain all measures contained in the CIP.

Purpose:

This guide has been developed to enable consistency and apply a structured process that will support TSA regional inspection teams with the application of a methodology for inspecting each covered O/O for compliance with the TSA-approved CIP. This document is not intended to supersede any inspection requirements as defined in TSA's approved inspection manuals. The inspection will rely on a thorough review of the CIP; associated documentation such as policies, controls and procedures identified in the CIP; and evidence requested by the inspection team prior to, and at the time of inspection. The inspection will validate the O/O's assertions made in the TSA-approved CIP. The CIP for each O/O is unique to that entity's operating environment and will require the inspection teams to supplement and tailor each inspection utilizing this guide as a baseline.

Inspection Methodology:

The inspections will be conducted in three primary phases: Planning, On-site Inspection, and Post Inspection. The inspection team will use the SD02C Inspection workbook to execute the on-site inspection.

Phase 1 – Planning

Planning and Coordination for the On-Site Inspection

During this phase the designated inspection teams will schedule the on-site inspection dates, make the necessary logistical arrangements such as identify the site location, visitor access requirements, conference room scheduling, and internet access for the inspection team computers. Some elements may be conducted virtually depending on circumstances. The inspection will be planned for a period of 1-5 days depending upon the scope which is defined in SD02C Section III.A., and the O/O's CIP. Once the date of the on-site inspection is determined the appropriate travel arrangements should be made.

Preparation for CIP Reviews during the Inspection

The TSA inspection team will need to perform a thorough review of the O/O's TSA-approved CIP and all associated documentation identified in the CIP prior to the formal on-site inspection. The inspection

team will request any additional documentation identified in the CIP which the O/O has not already provided prior to the start of the inspection. The inspection team should request the O/O provide a list of tools deployed that support the assertions of the CIP. The documentation and tools request must be made at a minimum of 30 days prior, with a recommended timeframe of 45-60 days prior to the on-site inspection. The document request should state that the documents be submitted within the next 14 calendar days. Should the O/O decline to provide the requested documents this will increase the time required on-site to allow for document review prior to inspection close out.

Planning for Verification and Validation Inspection Process

In order to verify and validate the controls and procedures are operating and capable of satisfying the measures as required by the O/O's CIP, the inspection team should leverage the tools already present on the O/O's system whenever possible. The O/O's CIP may identify some of these tools and the inspection team should attempt to familiarize themselves with these tools. The inspection team should discuss with the O/O the availability and use of these tools. If the O/O does not have applicable tools or the tools are unavailable for review by the inspection team, the inspection team should discuss with O/O the use of basic commands and scripts in Appendix B. If neither of these options can be utilized or the inspection team believes they would not be capable to establish compliance of the measures the O/O's CIP, then a network Packet Capture (PCAP) should be captured.

Should the inspection team determine that a PCAP is required to validate network traffic control assertions contained in the CIP, the inspection team will work with the O/O and the Surface Cyber Assurance Division to determine network span locations and length of time required for the PCAP. This PCAP will consist of header information only often referred to as a 5-tuple Packet Capture; this would include a set of five different values that comprise a connection. The five values are: a source IP address and port number, destination IP address and port number and the protocol in use.

Before requesting a PCAP from the O/O the inspection team must verify that there are enough resources to review a PCAP. The PCAP will need to be received a minimum of 2 weeks prior to the on-site inspection. This is to allow enough time for the current limited resources to process and analyze the PCAP. Future inspections should include as a standard practice a PCAP of 24 hours, once this capability is fully developed.

Phase 2 – On-site Inspection

Understanding the Inspection Methodology

The on-site inspection will provide opportunities for the inspection team to interview key operational and security personnel and collect evidence. TSA's inspection methodology consists of four types of inspection methods: surveillance, interview, document review, and testing (SIDoT). However, testing has not been approved for these inspections at this time. Documents and measures that could be reviewed and observed include but are not limited to:

- Log files;
- Device configuration settings;
- Visual confirmation of physical security protections; and
- Observance of operational tasks.

The inspection team may request any additional documentation they feel is necessary to validate compliance with the CIP. The on-site inspection may take up to 5 days to complete depending upon the size and complexity of the O/O's in scope systems.

Handling Compliance Determinations

When the inspection team and the O/O disagree in regard to the compliance, or non-compliance, of a section or sub-section in the CIP, the inspection team lead will consult with the O/O's primary point of contact (POC), and the TSA cyber assurance team to attempt to resolve the disagreement. The inspection team will identify:

- The CIP section or sub-section in question,
- The required outcome,
- Steps that need to be addressed or information that needs to be provided to determine compliance, and
- Any additional clarification of the inspection team observation for the O/O.

It is important that the inspection team not delay completing the inspection of the CIP while waiting for any clarifications from the O/O or HQ Cyber. The inspection team should endeavor to inspect and evaluate as much of the CIP as possible while awaiting any necessary feedback from either the O/O or HQ Cyber.

An outline for this process has been provided an Appendix A.

Phase 3 – Post Inspection

The inspection team will evaluate all information and determine if any of the inspected items result in non-compliance findings. During this phase, the inspection team will also evaluate if the CIP requires any adjustments to meet the intent of SD02C. All findings on CIPs must be communicated to the Regional Security Directors (RSD) assigned to the O/O.

When making PARIS system entries, the inspection team will only use data needed to support the PARIS system requirements. All supporting data such as the workbook, and evidence collected will be stored in the Microsoft Teams site for that O/O: TSA-SurfOps-RegionX-Inspections\SD2C Pipeline\O/O name\Onsite Inspection\Documents and Analysis) A hyperlink to this site will need to be included in the PARIS entry for reference.

Process/Procedures:

PHASE 1 - Planning

1. TSA will contact the O/O to determine a date for the onsite inspection. After establishing the inspection dates the inspection team should schedule a meeting to discuss the following:
    - Locations of on-site inspection.
    - Visitor access requirements.
    - On-site location for interviews.
    - On-site location for the inspection team's operational use that has internet access.

- IT support logistics (i.e., presentation of slide decks, internet access for inspection team, print/copy capability)
- On-Site physical security inspection safety and Personal Protective Equipment (PPE) requirements.
- On-Site walk through, a tour of control rooms, data centers, compressor and pump stations.
- Request any additional documentation that has not been previously provided. This should include any policies or procedures referenced in the CIP, as well as the documents identified in the Section IV Records of SD02C. If the O/O does not wish to provide documentation in advance TSA should advise them that this may prolong the on-site inspection process. TSA has the authority to copy and retain documentation required for further analysis. Upon further review this may result in the need to conduct an additional on-site inspection.
- Additional documents the inspection team may need to request include but are not limited to:
    a. Specific list of Critical Cyber systems (CCS). This should include hardware, software and data types. This includes asset inventories with Internet Protocol (IP) addresses, Classless Inter-Domain Routing (CIDR) and Virtual Local Area Network (VLAN) IDs.
    b. Network diagrams for both Operational Technology/Information Technology (OT/IT) that contain CCS. These diagrams need to clearly define the zones and boundaries that exist. The OT diagram needs to identify any external connections.
    c. Network Architectural design documents that describe how the IT and OT systems are defined and organized as depicted in the network diagrams by criticality, consequence, and operational necessity. Where OT data traverses the IT network, the encryption method should be described. This should describe the method used to segment and segregate the zones to control east-west and north-south network traffic.
    d. Virtual Private Network (VPN) community strings within the VPN configuration. Can be used to validate what is traversing the VPN tunnel. The hit counts on the VPN setup can be used to validate that traffic is flowing through the VPN tunnel.
    e. Data flow diagrams for both OT/IT systems. This diagram needs to identify any interdependencies.
    f. Switch configuration files, including IP space tables, VLAN segmentation and Access Control Lists (ACLs) implemented.
    g. Router configuration files, ACL statements on interfaces, routing tables, and types of dynamic routing in use. Tunnel information such as Generic Routing Encapsulation (GRE) tunnels and any VPN configurations in use on routers (if applicable).
    h. Policies and procedures used to manage firewalls.
    i. Comprehensive list of tools the O/O uses to implement the measures identified in the CIP. This list should identify if the tool is in-house developed or provided by a third-party vendor. If the tool is a third-party vendor it should be identified by product name and version. The configuration, management, procedure or SOP documentation should be provided for each tool in use. Tools may include:
        I. In house developed applications that are used to manage areas covered within the CIP such as account management.
        II. End point management tools such as anti-virus/end point detection and response (EDR).

III. Network monitoring tools.
IV. Configuration management tools.
V. Network and Host based Intrusion Detection/Intrusion Prevention tools.
VI. Email and Web filtering tools.
VII. Log forwarding and aggregation tools to include Security Information and Event Monitoring (SIEM) tools.

j. Account and Access Management policies, controls and procedures that describe how accounts/access are provisioned/terminated and managed for the lifecycle of the account.
k. Policies and procedures that govern how multi-factor authentication (MFA) is implemented to include what method of MFA is used, e.g., Smartcards, RSA tokens, other third-party tools.
l. Continuous monitoring policies and procedures.
m. Patch management policies and procedures.
n. Configuration management policies and procedures.
o. Contingency/disaster recovery plans.
p. Data backup/recovery policies and procedures.
q. Auditing and logging policies/procedures.
r. Cybersecurity Incident Response Plan, if not already on file.

2. Inspection team will determine travel requirements and submit travel request.
3. Inspection team will review the CIP and associated documentation and tailor the inspection topics to ensure validation of compliance with the CIP.
4. In addition to the list of documents identified above, the inspection team should develop a list of evidentiary documents required to support the assertions of controls identified in the CIP. This will vary depending upon the types of tools employed as well as logging and retention requirements of the O/O. This can include items such as: Operating System (OS) log files, Web filter logs, spam filter logs, phishing logs, firewall logs and running configurations, router and switch running configurations, vulnerability scanning reports, hardware and software asset lists with current versions and patching level including firmware.
5. Inspection team will develop a schedule to conduct a physical security/facilities inspection of those measures identified in the CIP as compensating controls used to mitigate risk, and for interviews with key personnel identified. These interviews should validate the assertions of processes and procedures identified in the CIP and documentation provided. If operational procedures require observation they should be identified and scheduled.

PHASE 2 – On-Site

1. Arrive on-site and conduct introduction presentation and review agenda/schedule.
2. Where applicable, conduct inspection of any physical security measures that were identified in the CIP as compensating controls to mitigate risk to critical cyber systems.
3. Conduct interviews with operational and security staff. Collect any evidence required to support assertions of technical security controls identified in the CIP.
4. Analyze all collected information and determine if any findings or recommended CIP improvements have been identified.
5. Conduct informal out-brief/next steps with operator.

PHASE 3 - Post Inspection

a. Complete inspection After Action Report (AAR) with analysis of the observations, tools utilized, and evidence collected during the on-site inspection.
b. Generate final inspection report detailing any potential findings, PARIS entry.
c. Evaluate if the CIP requires any adjustments to meet the intent of SD02C.
d. All findings on CIPs must be communicated to the RSD assigned to the O/O.

Appendix A

The following information provides an outline to follow in conducting the CIP inspection. The information described in each section applies to all phases of the inspection process.

SD02C Section III A.

Does the CIP adequately identify all cyber critical systems within the O/O's environment? The O/O should be able to provide a detailed list of all systems/devices, software and data that are subject to the requirements of the CIP. The inspection team should validate a sampling of items identified by visual inspection of hardware devices and associated software/firmware on those devices. Data flow diagrams should be evaluated and described by the O/O for CCS data flows and validate that no CCS data traverses or resides on devices not designated CCS.

SDO2C Section III B.1 -Implement network segmentation policies and controls designed to prevent operational disruption to the Operational Technology system if the Information Technology system is compromised or vice versa. As applied to Critical Cyber Systems, these policies and controls must include:

1. A list and description of –

    a. A list of IT/OT interdependencies should be validated with a detailed operational data flow analysis, and identification corresponds with the definition of section VII of SD02C; "*Critical Cyber System* means any Information or Operational Technology system or data that, if compromised or exploited, could result in operational disruption. Critical Cyber Systems include business services that, if compromised or exploited, could result in operational disruption.". *Operational disruption,* for purposes of the SD, means a deviation from or interruption of necessary capacity that results from a compromise or loss of data, system availability, system reliability, or control of a TSA-designated critical pipeline system or facility.
    Necessary capacity means Owner/Operator's determination of a capacity to support its business-critical functions required for pipeline operations and market expectations. This can be done by reviewing network diagrams/data flow diagrams and interviewing operational personnel. When connections and data are exchanged between the IT and OT systems and establishes an interdependency, the inspection team will need to determine through interviews if the connections are severed what is the impact on the operation of the pipeline if any. If interdependencies are critical, are there redundant systems in place to ensure continued operations? What, if any, contingency plans are in place to ensure the O/O can maintain operations? This area of evaluation is where the inspection team would determine if a PCAP should be collected. If the network diagrams/data flow diagrams do not clearly reflect what is asserted in the CIP or the O/O cannot adequately explain and describe any IT/OT connections and whether or not severing these connections would disrupt operations, then a PCAP should be done to evaluate actual traffic.
    b. External connections should be validated with a detailed network diagram showing the connections/lack of connections. If connections exist, how are the connections managed? Are they managed using firewalls, router ACLs, Virtual Private Networks (VPN), Multiprotocol Label

Switching (MPLS) VPN/Point-To-Point (PTP) circuits, LTE, satellite, etc.? The inspection team should validate the operational impact due to a loss of any external connections and what the O/O's contingency plan is to maintain operations. If the external connection is critical to continued operation is there built in redundancy?

c. Zone boundaries should be validated with a detailed network diagram and an architectural design document that describes the criticality, consequences and necessity. If the zones are created using VLANs this should be validated with switch/router configuration files as well as any associated documentation, they have that defines each VLAN/Zone and what resides in each zone. This may also be defined and controlled with firewalls which could also manage network traffic as described in the next section.

SD02C Section III B.2 - An identification and description of measures for securing and defending zone boundaries, that includes security controls –

a. The network traffic control measures should be evaluated to ensure that the only required traffic is permitted between the zones identified above. This should be validated by examining firewall rules/logs, switch and router ACLs and logs. The inspector should observe an attempt to communicate between zones to confirm. Are tools employed to inspect traffic such as, Network Intrusion Detection/Prevention (NIDS/NIPS) and Host based (HIDS/HIPS) sensors.
b. All traffic from the OT Services traffic traversing the IT network must be encrypted appropriately. The inspector should ascertain what traffic requires encryption using network diagrams/data flow diagrams. The O/O will need to provide the inspector with what method of encryption is being used, e.g., symmetrical or asymmetrical, and what encryption algorithm they are using. Observe an attempt to send unencrypted traffic between OT/IT.

Section III.C.

Implement access control measures, including for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures must incorporate the following policies, procedures, and controls:

1. Verify with the O/O what policies and procedures prevent the unauthorized access to CSS.
    a. Verify the O/O complies with their defined schedule for memorized secret authenticators. This can be accomplished by reviewing Identity Provider (IDP) logs or requesting a password age report. If change is only required due to a known/suspected compromise, determine if this has occurred and if so review last password change date.
    b. Verify the mitigation measures in place for those accounts that do not comply with III.C.1.a. These may include physical security measures, increased monitoring of these accounts and should be clearly defined in the CIP.
2. Review the O/O's implementation of Multi-Factor Authentication (MFA) e.g., smartcards, RSA tokens, or other known MFA solutions. Observe or walk-through the process for issuing authenticators. Particular attention should be paid to identity proofing processes to ensure the tokens are possessed by the authorized user. Validate the use of MFA by observing MFA logon to the devices and systems asserted in the CIP. Observe an attempt to authenticate to an MFA required device/account with username/password to validate access in not granted. Verify controls asserted in CIP that mitigate lack of MFA are implemented and are commensurate with MFA. These should

include things such as physical security, increased monitoring and logging, and analytical anomalous behavior tools.

3. Validate with the O/O the least privileged concept as it applies to account management and access controls. Determine how the O/O defines privileged versus non-privileged accounts or normal user accounts. Observe or walk-through how this is applied to account provisioning. Verify the compensating controls asserted in the CIP to mitigate the risk when least privilege cannot be applied. Verify accounts with administrative or privileged access are separate from standard user type accounts. Are highly privileged accounts like Microsoft Active Directory domain admins restricted from interactive logons to only the domain controllers? Are other OS highly privileged accounts restricted in the same fashion. Does the O/O have monitoring in place for highly privileged accounts? Are log files protected from unauthorized manipulation/deletion? How are privileged functions on OT devices controlled?
4. Review the process the O/O uses to determine the need for shared accounts that are critical to operations and verify this is following the measures outlined in their CIP. Request the number of shared accounts that exist.
    a. Observe or walk-through how these accounts are provisioned and how users are granted access to these accounts to include the application of least privileged concepts.
    b. Verify that the O/O's process for removing knowledge of the password complies with the CIP. Review IDP logs to validate last password change date on a shared account that was required to have a password change.
5. Validate trust relationships asserted in the CIP. If separate domains are implemented verify domain trusts by observation and using IDP admin tools.

Section III D.

Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and anomalies affecting Critical Cyber Systems. These measures must include:

1. Capabilities to:
    a. What tools are in place to prevent malicious email? Verify the tools in place are capable to evaluate incoming email for possible spam, phishing, malicious code and other malware. The O/O should describe in detail the capabilities of the tool used. What automated capabilities are in place when spam/malicious emails are detected? Validation may be done by reviewing filtering/blocking rules and logs. Is there a reporting tool/method for end users?
    b. What tools are in place to prevent ingress/egress from known or suspected malicious IP addresses? Validation may be done by reviewing router ACLs and firewall rules. Observe an attempt to access a known or suspected malicious IP and verify it is blocked and logged.
    c. What tools are in place to control the impact of known or suspected malicious web domains or applications? Review the method the tools use to accomplish this. Observe an attempt to navigate to a blocked domain or execute a blocked application.
    d. What tools or method is used by the O/O to block unauthorized code, including macro scripts? Observe an attempt to execute an unauthorized application or macro.
    e. How does the O/O block connections from known or suspected command and control servers? Observe an attempt to connect to a TOR exit node or an anonymization service.
2. Procedures to:

a. How does the O/O monitor the tools described above? Is there a Security Operations Center (SOC) that is 24/7 operation or do the tools send alerts to operators/security personnel? If a SOC exists, observe and interview SOC operations, interview staff to validate how alerts are processed.
b. What is the auditing frequency for unauthorized access to internet domains and addresses? Is there real-time alerting?
c. How does the O/O document and audit external communications that deviate from their baseline? Review any documentation that exists to support assertions in policy or procedure documents.
d. What Security, Orchestration, Automation and Response (SOAR) capabilities does the O/O have in place that standardize incident response?

3. Logging Policies:
    a. Does the O/O's logging policies and tools provide for continuous logging and analysis for intrusions and anomalous behavior? How are events and logs correlated to detect an intrusion or anomalous behavior?
    b. Observe a sampling of logs collected and confirm they adhere to the retention policy defined by the O/O's CIP.
4. Have the O/O walk-through the procedures to isolate the OT system from the IT system in the event that a cybersecurity event jeopardizes the safety and reliability of the OT system.

Section III E.

1. Verify that the O/O's patching policies/procedures ensure that systems are patched to the most current version possible for the environment. Determine what method or tools the O/O utilizes to ensure patches are current and up to date. Conduct a sampling of systems for verification of current patches to include OS, applications and firmware.
2. Walk through the process the O/O uses to prioritize application of patches to include the CISA Known Exploitable Vulnerabilities catalog.
3. Verify the mitigation strategies in place for systems that cannot be patched or updated to include a timeline to apply those patches.

Appendix B

Commands, Scripts and Tools

Windows Commands

secedit.exe is a command line tool that can update security policies on machines that are not part of an Active Directory domain. *Security templates* are in plain text

System log is where device driver issues would be recorded.

Fundamental grammar: C:\> wmic (alias) (where clause) (verb clause)

- WMIC.EXE; Manages Windows machines – setting variables
- Alias: process, share, service, nicconfig, startup, useraccount, qfe (quick fix eng-patches)
- Verb: list, get, call, delete
- SHARE – lists shared drives

Registry grammar: C:\> reg | add,export,import,query

Netsh (network shell): C:\> netsh | Can configure; firewall, DNS, DHCP, local area connections

Netstat: C:\> netstat -nao (Shows all TCP and UDP port usage and process ID)

- Local user manager: C:\> lusrmgr.msc
- Service control panel: C:\> services.msc
- Task Manager: C:\> taskmgr.msc
- Sec policy manager: C:\> secpol.msc
- Event viewer: C:\> eventvwr.msc
- Control Panel: C:\> control

Linux Commands

- **grep** command (Globally search a regular expression and print) used to search for a string or pattern of text within a file. None of the other answers will search the entire file.
- **head** command shows only a specific number of lines at the beginning of a file
- **tail** command shows only a specific number of lines at the end of a file
- **cat** command (concatenate) is used to display the entire contents of a file but wouldn't narrow the search for specific text strings found in a brute force attack.

iptables: IP packet filter of the kernel firewall

- IPv4 rules: sudo iptables -S.
- IPv6 rules: sudo ip6tables -S.
- tables rules: sudo iptables -L -v -n | more
- INPUT tables: sudo iptables -L INPUT -v -n.

Linux Directories

/ - “root”

- /bin - Essential command binaries
- /boot – boot loader files (kernel/initrd)
- /dev - Device files
- /etc - Host-specific system-wide configuration files
- /lib - Libraries essential for the binaries in /bin
- /mnt – temp mounted file systems
- /usr - for read-only user data; contains the majority of (multi-)user utilities and applications.
- /usr/local - third-party apps

Tools

Intrusion Detection System (IDS)

- Passive monitoring for attacks
- Monitoring and responding to alerts
- Potential for false positives

Intrusion Prevention System (IPS)

- Active blocking of attacks
- Potential for false positives

Scanning tools:

- Nessus – remote vulnerability scanner
- Nmap - network discovery and security auditing
- Saint – Security Administrators Network Tool
- SATAN – Security Administrators tool for Analyzing Networks

Packet Capture Methods

Command Switch	Description	Example
-D	Prints a list of all your network interfaces by number so that you can figure out which one to specify in a capture command	C:\Program Files\ Wireshark>**tshark -D**
-i	Specifies the capture interface that you will use	C:\Program Files\ Wireshark>**tshark -i eth0**
-b (filesize:{number})	TShark will stop writing to the cmTent capture file and switch to the next one if filesize is reached.	C:\Program Files\ Wireshark>**tshark -i eth0 -b filesize:300000** Note: 300000 sets the capture to wrap at 300MB
-s (snaplen)	Sets the default snapshot length to us during live data captures. Note: only the first 120 bytes of the data packet are necessary, so the command would be "-s 120"	C:\Program Files\ Wireshark>**tshark -i eth0 -b filesize:300000 –s 120**
-w (filename)	Writes the capture to the file identified	C:\Program Files\ Wireshark>**tshark -i eth0 -b filesize:300000 –s 120 –w packetcapture.pcap**