SD02D CSET TSA Owner/Operator Checklist

Section I: Cybersecurity Implementation Plan (CIP) Evaluation

1. Does the Owner/Operator identify its Critical Cyber Systems as defined in Section VII of Security Directive SD02D?

2. Does the O/O 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?

3. As applied to Critical Cyber Systems, do these policies and controls include:

3.1. A list and description of Information and Operational Technology system interdependencies?

3.2. A list and description of all external connections to the Operational Technology system?

3.3. A list and description of zone boundaries:

3.3.1. Including a description of how Information and Operational Technology systems are defined?

3.3.2. A description of how information and Operational Technology systems are organized into logical zones based on criticality, consequence, and operational necessity?

3.4. An identification and description of measures for securing and defending zone boundaries, that includes security controls to prevent unauthorized communications between zones?

3.5. An identification and description of measures for securing and defending zone boundaries, that includes security controls to prohibit Operational Technology system services from traversing the Information Technology system? (Unless the content of the Operational Technology system is encrypted while in transit).

4. Does the Owner/Operator implement access control measures, including for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems that incorporate:

4.1.1. Identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems that include a schedule for memorized secret authenticator resets?

4.1.2. For Critical Cyber Systems that will not have passwords reset in accordance with the schedule required by the preceding subparagraph (111.C. l .a.), does the O/O have documented and defined mitigation measures for components of and a timeframe to complete these mitigations?

4.2. Do access control measures incorporate multi-factor authentication, or other logical and physical security controls that supplement password authentication to provide risk mitigation commensurate to multi-factor authentication?

- If an Owner/Operator does not apply multi-factor authentication for access to industrial control workstations in control rooms regulated under 49 CFR parts 192 or 195, does the Owner/Operator specify compensating controls used to manage access?

4.3. Do access control measures incorporate policies and procedures to manage access rights based on the principles of least privilege and separation of duties?

- Where not technically feasible to apply these principles, do the policies and procedures describe the compensating controls that the Owner/Operator will apply?

4.4. Do access control measures incorporate enforcement of standards that limit availability and use of shared accounts to those that are critical for operations, and then only if absolutely necessary?

4.4.1. When the Owner/Operator uses shared accounts for operational purposes, do the policies and procedures ensure access to shared accounts is limited through account management that uses principles of least privilege and separation of duties?

4.4.2. When the Owner/Operator uses shared accounts for operational purposes, do the policies and procedures ensure individuals who no longer need access do not have knowledge of the password necessary to access the shared account?

4.5. Do access control measures include:

4.5.1. A schedule for review of existing domain trust relationships to ensure their necessity?

4.5.2. Policies to manage domain trusts?

5. Does the O/O 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?

5.1. Do the continuous monitoring and detection measures include capabilities to:

5.1.1. Prevent malicious email, such as spam and phishing emails, from adversely impacting operations?

5.1.2. Prohibit ingress and egress communications with known or suspected malicious Internet Protocol addresses?

5.1.3. Control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites?

5.1.4. Block and prevent unauthorized code, including macro scripts, from executing?

5.1.5. Monitor and/or block connections from known or suspected malicious command and control servers (such as Tor exit nodes, and other anonymization services)?

5.2. Do the continuous monitoring and detection measures include procedures to:

5.2.1. Audit unauthorized access to internet domains and addresses?

5.2.2. Document and audit any communications between the Operational Technology system and an external system that deviates from the Owner/Operator's identified baseline of communications?

5.2.3. Identify and respond to execution of unauthorized code, including macro scripts?

5.2.4. Implement capabilities (such as Security, Orchestration, Automation, and Response) to define, prioritize, and drive standardized incident response activities?

5.3. Do the continuous monitoring and detection measures include logging policies that:

5.3.1. Require continuous collection and analyzing of data for potential intrusions and anomalous behavior?

5.3.2. Ensure data is maintained for sufficient periods to allow for effective investigation of cybersecurity incidents?

5.4. Do the continuous monitoring and detection measures include mitigation measures or manual controls to ensure industrial control systems can be isolated when a cybersecurity incident in the Information Technology system creates risk to the safety and reliability of the Operational Technology system?

6. Does the O/O reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems consistent with the O/O's risk-based methodology?

6.1 Do the O/O's patch management measures include:

6.1.1. A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current?

6.1.2. Does this strategy include:

6.1.2.1. The risk methodology for categorizing and determining criticality of patches and updates?

6.1.2.2. An implementation timeline based on categorization and criticality?

6.1.2.3. Prioritization of all security patches and updates on CISA's Known Exploited Vulnerabilities Catalog?

6.1.3. If the Owner/Operator cannot apply patches and updates on specific Operational Technology systems without causing a severe degradation of operational capability to meet necessary capacity, does the patch management strategy include a description and timeline of additional mitigations that address the risk created by not installing the patch or update?

Section II: Cybersecurity Incident Response Plan (CIRP) Evaluation

7. Has the O/O developed and maintained a Cybersecurity Incident Response Plan (CIRP)?

7.1 Does the CIRP include measures to reduce the risk of operational disruption, or the risk of other significant impacts on necessary capacity, should the pipeline or facility experience a cybersecurity incident?

7.2. Does the CIRP provide specific measures sufficient to ensure prompt containment of the infected server or device?

7.3. Does the CIRP provide specific measures sufficient to ensure segregation of the infected network (or devices) to ensure malicious code does not spread by, as necessary:

7.3.1. Segregating (removing from the network) the infected device(s)?

7.3.2. Segregating any other devices that shared a network with the infected device(s)?

7.3.3. Preserving volatile memory by collecting a forensic memory image of affected device(s) before powering off or moving?

7.3.4. Isolating and securing all infected and potentially infected devices, making sure to clearly label any equipment that has been affected by malicious code?

7.4 Does the CIRP provide:

7.4.1. Specific measures sufficient to ensure security and integrity of backed-up data, including measures to secure backups?

7.4.2. Specific measures sufficient to store backup data separate from the system?

7.4.3. Procedures to ensure that the backup data is free of known malicious code when the backup is made and when tested for restoral?

7.5. Does the CIRP establish capability and governance for isolating the Information and Operational Technology systems in the event of a cybersecurity incident that results or could result in operational disruption?

7.6 Does the CIRP establish:

7.6.1. Does the CIRP establish exercises to test the effectiveness of procedures, no less than annually?

7.6.2. Does the CIRP establish exercises to test the effectiveness of personnel responsible for implementing measures in this Cybersecurity Incident Response Plan?

7.6.3. Does the CIRP establish exercises that test **at least two** objectives from sections 7.2-7.5 (listed above) no less than annually?

7.7. Does the CIRP establish/identify who (by position) is responsible for implementing the specific measures in the Incident Response Plan and any necessary resources needed to implement the measures?

7.8. Do the exercises required in section 7.6 include the employees identified (by position) in section 7.7 as active participants in the exercises?

Section III: Cybersecurity Assessment Plan (CAP) Evaluation

8. Has the O/O developed a Cybersecurity Assessment **Plan** for proactively assessing and auditing cybersecurity measures?

8.1. Does the CAP proactively assess:

8.1.2. Does the CAP proactively assess the O/O's Critical Cyber Systems to ascertain the effectiveness of cybersecurity measures?

8.1.3. Does the CAP proactively assess the O/O's Critical Cyber Systems to identify and resolve device, network, and/or system vulnerabilities?

8.2 Does the CAP assess the effectiveness of the Owner/Operator's TSA-approved Cybersecurity Implementation Plan (CIP)?

8.3. Does the CAP include a **cybersecurity** architecture design review **at least once every two years** that includes:

8.3.1. Verification and validation of network traffic and system log review?

8.3.2. Analysis to identify cybersecurity vulnerabilities related to network design, configuration, and inter-connectivity to internal and external systems?

8.4. Does the CAP incorporate other assessment capabilities, such as:

8.4.1. Penetration testing of Information Technology systems?

8.4.2. The use of "red" and "purple" team (adversarial perspective) testing?

8.5. Does the CAP include a **schedule** for assessing and auditing specific cybersecurity measures and/or actions required by sections 8.2 through 8.4 above?

8.6. Does the schedule ensure at least 30 percent of the policies, procedures, measures, and capabilities in the TSA-approved Cybersecurity Implementation Plan are assessed each year, with 100 percent assessed over any three-year period?

8.7 Does the CAP ensure a “Cybersecurity Assessment Plan: Annual Report” containing the results of assessments conducted in accordance with the CAP is submitted to TSA as described in paragraph G.4. of this section?

8.8 Does the required CAP Annual Report include:

8.8.1. The assessment method(s) used to determine whether the policies, procedures, and capabilities described by the O/O in its Cybersecurity Implementation Plan are effective?

8.8.2. Results of the individual assessments conducted?

8.8.3. Assessments conducted only during the previous 12 month period?

8.9. Does the Owner/Operator review and update their Cybersecurity Assessment Plan on an annual basis?

8.10. Has the O/O submitted the CAP to TSA for approval **no later than 12 months** from the date of the previous Cybersecurity Assessment Plan submission or TSA's approval of the previous plan?