TSA Cybersecurity Requirements for Oil and Natural Gas Owner/Operators

Assistant Administrator Sonya T. Proctor

September 11, 2023

Security Directives SD2C and SD2D

Section II.A.3. – Scope

Pipeline SD2C

Scope: The requirements of this SD apply to the covered Owner/Operators' (O/O) Critical Cyber Systems (CCS).

Pipeline SD2D

Scope: The requirements of this SD apply to the covered Owner/Operators' (O/O) Critical Cyber Systems (CCS).

Note: If an O/O determines they have no CCS, as defined in Section VII.,

The following must occur:

- **O/O notify TSA in writing within 60 days of the effective date of this Security Directive**
- **TSA will notify the O/O if the agency disagrees with the O/O's determination**
- **TSA may require the O/O to provide additional information regarding the methodologies or rationale used to identify CCS**
- **If O/O, who initially declared no CCS, changes the method of operations, the O/O must reevaluate for CCS,**
- **If CCS is determined the O/O shall notify TSA within 60 days of the change in operations to determine the schedule for complying with the requirements of SD 2021-2D**

Security Directives SD2C and SD2D

- Section II.B.3. – CIP

Pipeline SD2C	Pipeline SD2D
3. Once approved by TSA, the O/O must implement and maintain all measures in the TSA-approved CIP within the schedule as stipulated in the plan. 4. Unless and until TSA approves the O/O's CIP, the O/O must implement the requirements in the Attachment to this SD, as amended by any TSA-approved alternative measures and/or action plan requirements. Any approved alternative measures or action plan requirements remain in force and effect until completed or rescinded by TSA.	2. Once approved by TSA, the O/O must implement and maintain all measures in the TSA-approved CIP and meet any schedule stipulated in the plan. **3.O/O must follow procedures in Section VI to amend TSA approved CIP based on newly implemented SD2D**

Security Directives SD2C and SD2D

Section III.A. – Critical Cyber Systems

Pipeline SD2C	Pipeline SD2D
The Owner/Operator must: A. Identify the O/O's CCS as defined in Section VII. of this SD	The Owner/Operator must: A. Identify the O/O's CCS as defined in Section VII. of this SD**2D** **TSA will notify the O/O if the agency disagrees with the O/O's determination and reserves the right to require the O/O to provide additional information regarding the methodologies or rationale used to identify CCS** **After consultation with O/O's, TSA reserves the right to mandate the O/O to include additional CCS's identified by TSA not previously identified by the O/O in their CIP**

Security Directives SD2C and SD2D

Section III.F.1.e. – Incident Response Plan

Pipeline SD2C	Pipeline SD2D
F. Develop and Maintain a CIRP. e. Exercises to test the effectiveness of procedures, and personnel responsible for implementing measures in the Incident Response Plan, no less than annually.	F. Develop and Maintain a CIRP. e. Exercises to test the effectiveness of procedures, and personnel responsible for implementing measures in this CIRP, no less than annually. **These exercises must –** **i. Test at least two objectives of the O/O's CIRP required by subparagraphs F.1.a. through F.1.d. of this section, no less than annually; and** **ii. Include the employees identified (by position) in paragraph F.2 of this section as active participants in the exercises.**

Security Directives SD2C and SD2D

Section III.G. – Cybersecurity Assessment Plan

Pipeline SD2C

2. The Cybersecurity Assessment Program required by Section III.G.1. must –

a. Assess the effectiveness of the O/O's TSA-approved CIP;

b. Include an architectural design review at least once every two years that includes verification and validation of network traffic and system log review and analysis to identify cybersecurity vulnerabilities related to network design, configuration, and inter-connectivity to internal and external systems; and

c. Incorporate other assessment capabilities, such as penetration testing of Information Technology systems and the use of "red" and "purple" team (adversarial perspective) testing.

Pipeline SD2D

2. The Cybersecurity Assessment **Plan** required by Section III.G.1. must –

d. Include a schedule for assessing and auditing specific cybersecurity measures and/or actions required by Sections G.2.a. through G.2.c. The schedule must ensure at least 30 percent of the policies, procedures, measures, and capabilities in the TSA-approved CIP are assessed annually so that 100 percent will be assessed every three years; and

e. Ensure a CAP annual report encompasses results of assessments conducted in accordance with the CAP are submitted to TSA. The required report must indicate—

i. Which assessment method(s) were used to determine if the policies, procedures, and capabilities described by the O/O in its CIP are effective; and

ii. Results of the individual assessments conducted.

Security Directives SD2C and SD2D

Section III.G. – Cybersecurity Assessment Plan

Pipeline SD2C	Pipeline SD2D
3. No later than 60 days after TSA's approval of the O/O's CIP, the OO must submit the annual plan for their CAP to SurfOps-SD@tsa.dhs.gov. This plan must describe the CAP required by Section III.G.1., including the schedule for specific actions. The O/O must update this plan on an annual basis and submit it no later than one year from the date of the previous plan's submission.	**3. The O/O shall review and update the CAP annually and submit to TSA for approval no later than 12 months from the date of the previous CAP submission or TSA's approval of the previous plan.** **4. The CAP report required by Section G.2.e. shall be submitted to TSA annually no later than 12 months from the date of the previous CAP submission or TSA's approval of the previous plan. The annual report covers assessments conducted in the previous 12 months.**

Security Directives SD2C and SD2D

Section IV.A. – Records

Pipeline SD2C

IV. RECORDS

A. Use of previous plans, assessments, tests, and evaluations. As applicable, O/O may use previously developed plans, assessments, tests, and evaluations to meet the requirements of this SD. If the O/O relies on these materials, they must include an index of the records and their location organized in the same sequence as the requirements in this SD.

Pipeline SD2D

IV. RECORDS

A. Use of previous plans, assessments, tests, and evaluations. As applicable, O/O may use previously developed plans, assessments, tests, and evaluations to meet the requirements of this SD. If the O/O relies on these materials, they must include an index of the records and their location organized in the same sequence as the requirements in this SD.

In addition, these materials must be explicitly incorporated by reference into the CIP and made available to TSA upon request.

Security Directives SD2C and SD2D

Section V.C. – Submission of Documents

Pipeline SD2C	Pipeline SD2D
B. Comments. O/Os' may comment on this SD by submitting data, views, or arguments in writing to TSA via e-mail at TSA-Surface@tsa.dhs.gov. Any comments referring to specific measures in this SD must be protected in accordance with the requirements in 49 CFR part 1520. TSA may amend the SD based on comments received. Submission of a comment does not delay the effective date of the SD or requirement to comply with the provisions of the SD	B. Comments. O/Os' may comment on this SD by submitting data, views, or arguments in writing to TSA via e-mail at TSA-Surface@tsa.dhs.gov. Any comments referring to specific measures in this SD must be protected in accordance with the requirements in 49 CFR part 1520. TSA may amend the SD based on comments received. Submission of a comment does not delay the effective date of the SD or requirement to comply with the provisions of the SD C. **Submission of Documentation to TSA: O/Os' are required to submit documents in a manner prescribed by TSA. TSA will provide O/O specific instructions for submission of required documents**