



# TSA Security Directive Pipeline-2021-02D

EFFECTIVE JULY 27, 2023

Cancels and supersedes Security Directive Pipeline-2021-02C.

The SD-02D update provides consistency and incremental enhancement, rather than a major overhaul. Industries can have confidence that their efforts put toward complying with SD-02C will carry forward and not be disrupted by changing regulations.



## WHO IS THIS FOR?

Owners/operators of TSA-designated critical pipeline systems or facilities, notified before July 26, 2022.

**If TSA identifies additional owner/operators who were not previously subjected to the Security Directive Pipeline-2021-02 series, TSA will notify them and provide compliance deadlines for the requirements.**

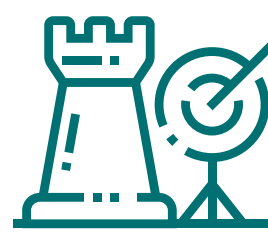
## WHAT'S NEW IN SD-02D?

Key changes in SD-02D from previous directive include:



### NEW LANGUAGE

addressing critical systems designations



### TABLETOP EXERCISES

are mandatory annually, with two objectives tested



### 30 percent of the CYBERSECURITY ASSESSMENT

PLAN must be assessed each year, with 100 percent of the plan being assessed every three years

## WHAT ARE THE REQUIREMENTS?

# 1

**CREATE A CYBERSECURITY IMPLEMENTATION PLAN** that includes the following measures:

**III.A** Identify Critical Cyber Systems.



**SD-02D UPDATE:** If TSA disagrees with any critical systems designations submitted, asset owners may be required to provide rationale for excluding systems or require that additional systems be included.

**III.B** Implement network segmentation policies and controls.



**III.C** Implement access control measures to secure and prevent unauthorized access.



**III.D** Implement continuous monitoring, and detection policies and procedures to prevent, detect, and respond to cybersecurity threats and anomalies affecting Critical Cyber Systems.



**III.E** Apply security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems consistent with the owner / operator's risk-based methodology.



**SD-02D UPDATE:** Implementation Plans amended after prior TSA approval are required to be resubmitted.

# 2

Develop and maintain a **CYBERSECURITY INCIDENT RESPONSE PLAN.**

**III.F** Have an up-to-date Cybersecurity Incident Response Plan that includes measures to reduce risk of operational disruption, and identifies the position responsible for implementing the plan.



**SD-02D UPDATE:** Must test at least 2 objectives from plan annually, and identify the positions who are active participants.

# 3

Develop a **CYBERSECURITY ASSESSMENT PLAN.**

**III.G** Develop a Cybersecurity Assessment Plan for proactively assessing and auditing cybersecurity measures.



**SD-02D UPDATE:** Include a schedule for assessing and auditing cybersecurity measures, ensuring that at least 30 percent of the policies, procedures, and capabilities in the TSA-approved Cybersecurity Implementation Plan are assessed each year, with 100 percent assessed over any 3-year period. Audit results must be provided to TSA in an annual assessment report.