Operator Checklist

TSA Pipeline Security Directives

2021-01C and 2021-02D

WHO NEEDS TO KNOW?

Owners/operators of TSA-designated hazardous liquid and natural gas pipelines or LNG facilities.

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

01 Initially

2021-01C

- ☐ Designate a corporate Cybersecurity Coordinator and alternate (01C § X)
- ☐ Conduct Vulnerability Assessment to TSA Pipeline Security Guidelines; report results to TSA (01C § 7)
- ☐ Establish & Implement a Cybersecurity Implementation Plan (CIP) (02D § II.B)
- ☐ Develop a Cybersecurity Assessment Plan (CAP) (02D § III.G)
- ☐ Identify Critical Cyber Systems (CCS) (02D § III.A)
- ☐ Implement Network Segmentation policies and controls (02D § III.B)
- ☐ Implement local and remote Access Controls (02D § III.C)
- ☐ Implement and maintain Monitoring and Detection Program (02D § III.D)
- ☐ Implement & maintain a Patch Management Program (02D § III.E)

365 Anually

- ☐ Exercise Incident Response Plan (02D § III.F)
- ☐ Assess a minimum of 30% of CIP each year (02D § III.G.2d)
- ☐ Annually review and update CAP plan and submit to TSA for approval (02D § III.G.3)
- ☐ Annually submit CAP assessment report to TSA (02D § III.G.4)

2 YEARS Bienially

- ☐ Conduct a Cybersecurity Architecture Design Review (CADR) (02D § III.G.2b)

! 2021-01C Upon Occurrence

- ☐ Report cybersecurity incidents to CISA within 24 hours (01C § X)

network perception

ARMEXA