

**TSA Security Directive  
Pipeline-2021-02B**

**Table of Implementation Timeframes**

SECTION	MEASURE	DUE DATE
	Certification of completion for required measures.	Within 7 days of completing the requirements in sections II.B.1., II.B.2., II.B.3., II.C.1., and II.D.1. owner/operators must submit a statement of completion to TSA.
II.B.1.a.	Implement and complete a mandatory password reset of all passwords within Information Technology systems (such as corporate remote access, and Virtual Private Networks).	No later than August 25, 2021.
II.B.1.b.	Implement and complete a mandatory password resets of all equipment within Operational Technology systems, to include Programmable Logic Controllers. If it is not technically feasible within 120 days, an alternative procedure under Section 5 must be approved by TSA.	No later than November 23, 2021.
II.B.1.c.	For equipment within Information and Operational Technology systems that do not permit password resets, the Owner/Operator must develop a plan, including a timeline, for replacing the designated equipment. A copy of this plan must be completed and provided to TSA.	No later than November 23, 2021.
II.B.1.d.	Require supervisors of individuals with elevated privilege accounts/permission to verbally confirm and document with users of all such accounts their account ownership and continued need for access to Information and Operational Technology systems.	No later than August 25, 2021.
II.B.1.e.	Implement a schedule for verification of continued need at least every 90 days after the verbal confirmation required by II.B.1.d. The Owner/Operator must maintain documentation establishing date of last verification.	Every 90 days after completing II.B.1.d.
II.B.2.a.	Apply multi-factor authentication for non-service accounts accessing Information and Operational Technology systems in a manner compliant with the most current version of NIST Special Publication 800-63B, Digital Identify Guidelines, Authentication and Lifecycle Management standards for use of multifactor cryptographic device authenticators.	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.

**TSA Security Directive**  
**Pipeline-2021-02B**  
**Table of Implementation Timeframes**

II.B.2.b.	<b>Implement network segmentation sufficient to ensure the Operational Technology system can operate at necessary capacity even if the Information Technology system is compromised by, at a minimum:</b>	
II.B.2.b.	i. Identifying Information and Operational Technology network inter-dependencies;	No later than January 22, 2022 as measure involves both Information and Operational Technology Systems.
II.B.2.b.	ii. Implementing and maintaining capability for network physical and logical segmentation between Information and the Operational Technology systems sufficient to ensure the Operational Technology system can continue to operate even if the Information Technology system is taken offline because it has been compromised;	No later than January 22, 2022 as measure involves both Information and Operational Technology Systems.
II.B.2.b.	iii. Defining a demilitarized zone and using firewall rules, physical separation, and other tools to eliminate unrestricted communication between the Information and Operational Technology systems;	No later than January 22, 2022 as measure involves both Information and Operational Technology Systems.
II.B.2.b.	iv. Organizing Operational Technology systems assets into logical zones, such as isolating unrelated sub-processes, by taking into account criticality, consequence, and operational necessity;	No later than January 22, 2022.
II.B.2.b.	v. Monitoring and filtering traffic between networks of different trust levels, such as between the Information Technology and the Operational Technology system, by defining appropriate communication conduits between the logical zones and deploying security controls to monitor and filter network traffic and communications between logical zones;	No later than January 22, 2022 as measure involves both Information and Operational Technology Systems.
II.B.2.b.	vi. Prohibiting Operational Technology system protocols from traversing the Information Technology system unless expressly through an encrypted point-to-point tunnel;	No later than January 22, 2022 as measure involves both Information and Operational Technology Systems.
II.B.2.b.	vii. Developing workarounds or manual controls to ensure industrial control system networks can be physically isolated when the Information Technology system creates risk to the safe and reliable Operational Technology system processes.	No later than January 22, 2022 as measure involves both Information and Operational Technology Systems.

Pipeline-2021-02B

Table of Implementation Timeframes

II.B.2.c.	Review and update (or develop, if necessary) log retention policies to ensure that they include policies and procedures for log management; include a secure log management infrastructure; and specify how long log data must be maintained, consistent with NIST standards.	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.
II.B.2.d.	<b>Employ filters sufficient to:</b>	
II.B.2.d.	i. Identify malicious email traffic, spam and phishing emails and inhibit them from reaching end users;	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.
II.B.2.d.	ii. Prohibit ingress and egress of communications with known malicious Internet Protocol addresses for Information Technology systems and all Operational Technology with external connectivity;	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.
II.B.2.d.	iii. Prevent users and devices from accessing malicious websites by implementing Uniform Resource Locator block lists and/or allowlists;	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.
II.B.2.d.	iv. Control access from the Operational Technology system to external internet access using an allowlist; and	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.
II.B.2.d.	v. Investigate any communication between the Operational Technology system and an outside system that deviates from the identified baseline of communications and ensure it is necessary for operations.	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.
II.B.2.e.	Set antivirus/anti-malware programs to conduct weekly scans, with on-access and on-demand scans, of Information and Operational Technology systems and other network assets using current signatures.	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.

**TSA Security Directive**  
**Pipeline-2021-02B**  
**Table of Implementation Timeframes**

II.B.2.f.	<b>Establish passive Domain Name System capabilities that are consistent with currently recognized standards and, at a minimum, include the following actions:</b>	
II.B.2.f.	i. Implementing software analytics that allow Owner/Operators to rapidly determine which host sourced each Domain Name System-query.	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.
II.B.2.f.	ii. Maintaining a current list of domains that are frequently visited or searched for by legitimate users within their systems that are not already included in commercially available top one million domain lists; and	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.
II.B.2.f.	iii. Developing and/or updating policies and procedures requiring investigation of the reputation of the domains that are only rarely queried for and/or accessed by legitimate users within their organization, to determine if the communication with these domains carries an inappropriate level of risk to the organization.	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.
II.B.2.g.	<b>Ensure the following, with respect to all security software updates and patches—</b>	
II.B.2.g.	i. For operating systems, applications, drivers, and firmware on Information Technology systems:	
II.B.2.g.	i.a) For patches and updates that are listed on CISA's Known Exploited Vulnerabilities Catalog ( <a href="https://www.cisa.gov/known-exploited-vulnerabilities-catalog">https://www.cisa.gov/known-exploited-vulnerabilities-catalog</a> ) and have a NIST Base Score of "Critical" (under the Common Vulnerability Scoring System) the patch/update must be installed within 15 days of its availability.	Installed within 15 days of its availability for Informational Technology Systems.
II.B.2.g.	i.b) If the owner/operator is unable to install the patch/update for a "Critical" vulnerability within 15 days, it must do the following:	
II.B.2.g.	i.b) 2. install the patch/update within 30 days of its listing on the Known Exploited Vulnerabilities Catalog.	No later than 30 days of its listing for Informational Technology Systems.
II.B.2.g.	i.c) All other updates and patches must be installed within 30 days of availability.	No later than 30 days of its availability for Informational Technology Systems.

**TSA Security Directive**  
**Pipeline-2021-02B**  
**Table of Implementation Timeframes**

II.B.2.g.	ii. For operating systems, applications, drivers, and firmware, on Operation Technology systems, software updates and patches must be tested within 35 days of update patch availability and installed within 35 days of testing validation. Patches not installed must be included on a cumulative list that includes operational and other risk-based considerations justifying the determination not to apply the patch.	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.
-----------	---	--

II.B.2.h.	<b>Implement a “zero trust” policy that provides layers of defense to prevent unauthorized execution by taking the following actions, as applicable, to the Owner/Operator’s Information and Operational Technology systems:</b>	
II.B.2.h.	i. If using Microsoft Office, fully disable macro use and user-based approval across the organization for Microsoft Office products (such as Word, Excel) using Group Policy. Macros determined necessary for business functionality may be enabled on a case-by-case basis only after implementing additional host-based security controls and network monitoring;	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.
II.B.2.h.	ii. Apply application allowlisting to Information and Operational Technology systems and then implement software restriction policies, or other controls providing the same security benefits, to prevent unauthorized programs from executing;	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.
II.B.2.h.	iii. If not already incorporated into system-change management, update application allowlisting no less frequently than quarterly to remove applications no longer in use;	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.
II.B.2.h.	iv. Monitor and/or block connections from known malicious command and control servers (such as Tor exit nodes, and other anonymization services) to Internet Protocol addresses and ports for which external connections are not expected (such as ports other than virtual private network gateways, mail ports, or web ports);	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.

**TSA Security Directive**  
**Pipeline-2021-02B Table of**  
**Implementation Timeframes**

II.B.2.h.	v. Implement Security, Orchestration, Automation, and Response, as applicable. If the Owner/Operator determines these capabilities are not applicable, they must document which aspects of the system do not apply the capability and their justification for excluding these operations;	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.
II.B.2.h.	vi. Require implementation of signatures to detect and/or block connection from post-exploitation tools.	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.
II.B.2.i.	Organize access rights based on the principles of least privilege and separation of duties, such as user and process accounts limited through account use policies, user account control, and privileged account management, compliant with the most current version of NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations.	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.
II.B.2.j.	For any group accounts, establish a written process to review operational need for the account, document justification, maintain a list, ensure memorized secret authenticators are compliant with NIST SP 800-63B, maintain list of personnel who have or had access to group accounts, and dates of last password resets. Within no more than 7 days after a user of a group account leaves the Owner/Operator's employment, the Owner/Operator must rotate memorized secret authenticators for the group account.	No later than October 24, 2021 for Informational Technology Systems. No later than January 22, 2022 for Operational Technology Systems.
II.B.3.	Owner/Operators shall remove all trust relationships, such as identity stores between the Information and Operational Technology systems. Separate and dedicated identity providers shall be implemented for the Information and Operational Technology systems, if they do not already exist.	No later than January 22, 2022.
II.C.1.	Owner/Operators must develop and adopt a Cybersecurity Contingency/Response Plan that includes measures to reduce the risk of operational disruption, or other significant business or functional	No later than August 25, 2021.

**Pipeline-2021-02B**

**Table of Implementation Timeframes**

	degradation to necessary capacity, should their pipeline or facility experience a cybersecurity incident.	
II.C.2.e.	Conduct situational exercises to test the effectiveness of procedures, and personnel responsible for implementing measures, in the Cybersecurity Contingency/Response Plan, no less than annually.	Every 12 months.

II.D.1.	Owner/Operators must schedule a third-party evaluation of the Owner/Operator’s Operational Technology system design and architecture, to be conducted within 12 months from the effective date of this Security Directive, which 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.	Schedule review no later than January 22, 2022. Conduct review no later than July 26, 2022.
---------	--	--