TECHNICAL BRIEF

TSA Cybersecurity Mandates for Public Transportation

Arrive Early, Arrive Safe with Ordr

The United States is constantly under attack from bad actors including nation states and financial opportunists. Threats to critical infrastructure and services such as public transportation can have far-reaching impacts on the economy, public safety, and national security.

Following the 2021 ransomware attack on the Colonial Pipeline, the Transportation Security Administration (TSA) issued directives in 2022 to bolster security for U.S. pipelines. These directives were issued as part of an overarching executive order to protect critical infrastructure from "degradation, destruction, or malfunctioning of systems that control this infrastructure." [Reference: National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems (July 29, 2021).]

In October 2022, Security Directives 1580-21-01A, 1582-21-01A, and 1580/82-2022-01 were announced to include surface transportation systems and associated infrastructure such as passenger railroads and rail systems. In March 2023, an emergency amendment was added to extend the directives to TSA-regulated airport and aircraft operators.

What is at the core of these security directives? In summary, the directives mandate that impacted entities such as railroad, airline, and airport owners and operators must:

- Develop a TSA-approved implementation plan that describes the specific measures taken to achieve cybersecurity outcomes; and,
- Develop a TSA-approved assessment plan that describes how the specific measures will be assessed for effectiveness.

Specific measures outlined include the following actions:

- Implement network segmentation policies and controls to ensure that operational technology (OT) systems can continue to safely operate in the event that an information technology (IT) system has been compromised;
- Implement access control measures to secure and prevent unauthorized access to Critical Cyber Systems;
- Implement continuous monitoring and detection policies and procedures to detect cybersecurity threats and correct anomalies that affect Critical Cyber System operations; and,
- 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 in a timely manner using a risk-based methodology.

[Reference: Security Directive 1580/82-2022-01C]

INTRODUCING ORDR

Ordr is a comprehensive OT and IT asset discovery and classification solution that helps to ensure only trusted systems can access the network. Ordr calculates risk based on device type, model, operating system, and patch status, and continuously monitors communications for threat activity and anomalous behavior. Ordr then dynamically groups devices based on organizational requirements and automatically generates and provisions network segmentation policies.

The following table lists the four specific measures encompassed in the TSA mandates in more details and how Ordr helps to address each one.

TSA Measure	Cybersecurity Measure Details	Ordr Solution
1	Implement network segmentation policies and controls designed to prevent disruption of the operational technology (OT) system if the information technology (IT) system is compromised, or vice versa.	Ordr passively discovers and classifies all OT and IT devices on the network and automatically tracks the communications of all devices including IT to IT, OT to OT, and all traffic between OT and IT. Ordr dynamically generates segmentation and provisions segmentation policies to switches, wireless controllers, and firewalls to permit only safe and authorized communications between each device regardless of its type or function.
	Policies and controls: a. IT and OT system interdependencies. b. All external connections to IT and OT systems. c. Zone boundaries, including a description of how IT and OT systems	Ordr: a. Automatically tracks all communications between IT and OT systems and verifies the network interdependencies of each. b. Automatically tracks all connections to and from external systems and IT and OT systems. c. Enables the definition of zones based on device type, business function,

	are defined and organized into logical zones based on criticality, consequence, and operational necessity. d. Policies to ensure IT and OT system services transit the other only when necessary for validated business or operational purposes.	location, and other key factors like criticality and risk, and then automates the generation if inter-zone segmentation policies. d. Learns and generates policies based on minimum required access privileges to ensure IT and OT system services only communicate as required.
	Security controls for defending zone boundaries: a. To prevent unauthorized communications between zones b. To prohibit OT system services from traversing IT systems, and vice versa, unless the content is encrypted or, if not technologically feasible, otherwise secured and protected to ensure integrity and prevent corruption or compromise while the content is in transit.	**Ordr:** a. Automatically learns and monitors the network for unauthorized access and anomalous behavior. Inter-zone segmentation policies are dynamically generated and provisioned to existing zone boundaries such as firewalls. If not yet segmented, Ordr can apply threat response controls to block unauthorized communications between zones. b. Automatically tracks all connections to and from external systems and IT and OT systems and applies proactive segmentation policies to only permit authorized communications between zones or reactively respond to threats for at risk or unauthorized communications between zones.
2	**Implement access control measures, including those for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems.**	**Ordr seamlessly integrates with existing wired switches, wireless controllers, firewalls, and Network Access Control (NAC) solutions from leading vendors to implement access controls to secure and prevent unauthorized access to Critical Cyber Systems.**
	Identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems:	**Ordr automatically discovers and classifies both authenticating and non-authenticating OT and IT systems and enables access control policies**

	a. A policy for memorized secret authenticators resets that includes criteria for when resets must occur compliant with the National Institute of Standards and Technology (NIST). b. Mitigation measures for components of Critical Cyber Systems that will not fall under the above policy.	**based on trusted devices to prevent unauthorized access to Critical Cyber Systems. Ordr:** a. Does not implement authentication policies but integrates directly with identity access management (IAM) and NAC solutions to augment access control decisions for devices that support authentication and secret credentials. b. Provides compensating controls and mitigation for devices that lack the ability to provide explicit identity or authentication features like memorized secrets by accurately classifying and collecting rich contextual data about each device such as its type, function, make, model, operating system (OS) type and version, location, business role, vulnerabilities, and risk factors to control network access and prevent unauthorizes access.
	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 OT components or assets, the owner/operator must specify what compensating controls are used to manage access.	Ordr provides detailed classification and rich contextual data to augment the basic authentication capabilities of a device.
	Policies and procedures to manage access rights based on the principles of least privilege and separation of duties. Where it is not technically feasible to apply these principles, the policies and procedures must describe the compensating controls that the owner/operator will apply.	Through accurate classification and context as well as automated baselining of all device communications, Ordr ensures only trusted devices access the network and are only granted the minimum access required to safely perform their intended and authorized functions by generating and provisioning Zero Trust policies to the existing network infrastructure and security devices.

	Enforcement of standards that limit the availability and use of shared accounts to those that are critical for operations, and then only if necessary. When the owner/operator uses shared accounts for operational purposes, the policies and procedures must ensure: a. Access to shared accounts is limited through account management that uses principles of least privilege and separation of duties. b. Individuals who no longer need access do not have knowledge of the password necessary to access the shared accounts.	Ordr does not directly limit or control the use of shared accounts, but directly integrates with IAM, NAC, and other solutions that manage shared accounts. Ordr does track users that login to a given device to determine if multiple users are logging into a given device or if a single user logs into multiple devices.
	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 OT components or assets, the owner/operator must specify what compensating controls are used to manage access.	Ordr provides detailed classification and rich contextual data to augment the basic authentication capabilities of a device.
	Regularly updated schedule for review of existing domain trust relationships to ensure their necessity and establish policies to manage these relationships.	Ordr tracks all communications for each device at multiple levels to establish and continuously monitor domain trust relationships for policy and security violations.
3	**Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and correct anomalies affecting Critical Cyber Systems.**	**Ordr continuously monitors all device communications to establish baselines of safe behavior and automatically detects anomalies, suspicious activity, vulnerable communications, as well as internal and external threats. Ordr can dynamically respond to threats by quarantining an attacked or infected system, block unauthorized or high-risk communications, or limit access to vulnerable systems.**

	Capabilities to: a. Defend against malicious email, such as spam and phishing emails, to preclude or mitigate against adverse impacts to operations. b. Block ingress and egress communications with known or suspected malicious internet protocol (IP) addresses. c. Control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites. d. Block and prevent unauthorized code, including macro scripts, from executing. e. Monitor and/or block connections from known or suspected malicious command and control servers.	**Ordr:** a. Does not directly provide email security such as spam or phishing controls but can detect attempts to communicate to malicious or high-risk cites resulting from a compromise via these methods. b. Detect communications to or from known or suspected malicious Internet sites and block the ingress and egress communications via direct integration with switches, wireless controllers, NAC, and firewalls. c. Automatically detects communications to malicious websites and blocks users and devices from communicating with these sites. d. It is an agentless solution and does not directly block or prevent unauthorized code from executing on a host but can block its attempts to communicate to unauthorized systems and services following infection. e. Monitors and blocks connections from known or suspected malicious command and control servers.
	Procedures to: a. Audit unauthorized access to internet domains and addresses. b. Document and audit any communications between the OT systems and an external system that deviates from the owner/operator's identified baseline of communications. c. Identify and respond to execution of unauthorized code, including macro scripts; and implement capabilities (such as security, orchestration,	**Ordr offers procedures to:** a. Audit unauthorized access to internet domains and addresses. b. Tracks and reports on any communications between OT systems and external systems that deviate from the identified baseline of communications. Directly through its own security analytics or via integration with third-party systems identify and respond to infected systems to risk

	automation, and response (SOAR)) to define, prioritize, and drive standardized incident response activities.	rate and inform other systems or by taking immediate action to alert and block unauthorized communications following infection.
	Logging policies that: a. Require continuous collection and analyzing of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other OT and IT systems that directly connect with Critical Cyber Systems. b. Ensure data is maintained for sufficient periods, to provide effective investigation of cybersecurity incidents.	**Ordr:** a. Continuously collects and analyzes data from multiple sources such as flow data, deep packet inspection and application layer decoding, embedded intrusion detection, and anomalous behavior detection for OT, IT, and Critical Cyber Systems. b. Maintains data to provide effective investigation of cybersecurity incidents. Actual data retention periods are contingent on allocated storage.
	Mitigation measures or manual controls to ensure industrial control systems can be isolated when a cybersecurity incident in the IT system creates risk to the safety and reliability of OT systems.	Ordr enables both manual and automated response to mitigate and isolate industrial control systems as required when IT cybersecurity incidents occur and present risk to the safety and reliability of OT systems.
4	**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 owner/operator's risk-based methodology.**	**Ordr can directly or indirectly discover and track unpatched and vulnerable systems. As an agentless solution, Ordr does not directly apply patches, but integrates with industry leading patch management and mobile device management (MDM) solutions as well as vulnerability management solutions to verify critical systems are patched and dynamically update its risk calculation based on vulnerability and patch status.**
	A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current.	Ordr integrates with solutions such as Active Directory, patch management, and MDM to track patch status for numerous types of workstations, servers, and mobile

	a. automation, and response (SOAR)) to define, prioritize, and drive standardized incident response activities.	devices. Furthermore, Ordr is unique in its ability to retrieve hardware, software, and patch information for unmanaged devices and systems that do not support an agent, a common situation for OT devices. Through native OS scripts which run just once a day or upon new connection to a network, Ordr can retrieve system and patch details for OT and IT systems without an agent.
	The strategy requires: a. The risk methodology for categorizing and determining criticality of patches and updates, and an implementation timeline based on categorization and criticality. b. Prioritization of all security patches and updates on the Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities Catalog.	**Ordr:** a. Offers a flexible risk calculation methodology to facilitate prioritization of risk based on device type, business function, OS, and many other factors, as well as trigger service tickets for their remediation. b. Rates risk on multiple cybersecurity factors and feeds including the National Vulnerability Database.
	If the owner/operator cannot apply patches and updates on specific Operational Technology systems without causing a severe degradation of operational capability, the patch management strategy must include a description and timeline of additional mitigations that address the risk created by not installing the patch or update.	Ordr enables the segmentation of unpatched or non-patchable systems using existing network infrastructure, NAC, or firewall systems.

For additional information on how Ordr can accelerate compliance with TSA cybersecurity mandates for Critical Infrastructure to protect public transportation for airlines, railroads, rail systems, and pipelines, **contact us to discuss further.**