



Hardening Department of War (DoW) Critical Operational Technology (OT) Environments with Zero Trust (ZT) Principles

Executive summary

OT systems underpin all mission-essential services and critical infrastructure. Many of these systems were engineered without consideration for today's cyber threats—threats that continue to increase in frequency, sophistication, and scale. The DoW and supporting organizations must strengthen OT environment protections to ensure resilient mission execution, safeguarding critical infrastructure from disruptive or destructive adversarial activity.

OT devices monitor and control the physical processes that enable industrial control systems (ICS), such as building automation and backup power generation. Mitigating vulnerabilities in these systems is vital to safeguarding military operations and public health. To address these challenges, this Cybersecurity Information Sheet (CSI) identifies high-impact ZT-aligned activities to strengthen the overall OT cybersecurity posture. These recommendations provide practical compensating controls that enable organizations to implement ZT outcomes despite the technical limitations of OT systems.

ZT complements, rather than replaces, existing cybersecurity and cyber hygiene practices. By assuming compromise is possible or already present, ZT continuously verifies users, devices, workflows, and communications. Applying these principles to OT strengthens protection against unauthorized access, lateral movement, and adversarial persistence. Adversaries are leveraging super intelligence (SI) capabilities to automate reconnaissance, accelerate exploit development, and conduct cyber campaigns at unprecedented speed and scale, making achieving ZT outcomes in OT systems more critical than ever.

Organizations are starting to integrate SI into OT to improve efficiency, resilience, and mission effectiveness. However, this also can inadvertently introduce new risk, attack surfaces, and disruption opportunities. SI-enabled systems need to be strategically incorporated into existing OT architectures to ensure safe operations.

Recognizing these evolving challenges, recent national policy emphasizes integrating cybersecurity, ZT, and SI governance across critical infrastructure. In line with [Executive Order \(EO\) 14409](#), [NSPM-11](#), and [NSPM-12](#), this CSI provides a practical path for hardening legacy OT. DoW ZT for OT guidance identifies 84 activities that collectively achieve comprehensive ZT capabilities; this CSI highlights 26 high-impact activities that organizations can implement now. By prioritizing key measures to secure remote access, harden smart controllers, enhance visibility, and enforce micro-segmentation, organizations can disrupt the ICS Cyber Kill Chain and successfully transition OT environments to a proactive ZT architecture.



Hardening DoW Critical OT Environments with Zero Trust Principles

Table of Contents

Executive summary	1
Introduction	3
Target audience	5
Background	5
Zero Trust	6
High-impact OT Zero Trust mitigation steps	9
Securing remote access.....	10
Protecting OT data.....	11
Inventorying OT assets	11
Enhancing OT environment visibility	12
Utilizing OT cyber threat intelligence.....	12
Hardening smart controllers	13
Strengthening networks with segmentation and monitoring	14
Securing engineering workstations and human-machine interfaces	15
Enforcing security via hardened Active Directory and Domain Controllers	16
Verifying and assessing ZT controls safely	16
Summary	17
Further reading and guidance.....	18
Works cited	19
Disclaimer of endorsement	21
Purpose	21
Contact	21
Appendix: Prioritized OT ZT Activities	22



Introduction

Operational Technology (OT) systems often maintain a service life exceeding 50 years, resulting in extensive legacy footprints that present significant modernization challenges. This longevity, while impressive from an engineering standpoint, can lead to critical cybersecurity vulnerabilities. Their age, proprietary technologies, and operational constraints also make implementing Zero Trust (ZT) capabilities, such as strong identity, segmentation, continuous monitoring, and policy enforcement, more difficult, requiring tailored approaches to achieve ZT outcomes. Many of these legacy systems are no longer supported by vendors and are unable to receive vital patches or updates. [1]

Adversarial attacks now extend beyond espionage and reconnaissance, often aiming to deny, degrade, disrupt, deceive, or destroy the United States' critical infrastructure. The consequences of such attacks vary by sector and can result in significant and widespread damage. Affected sectors may include, but are not limited to, energy, water, agriculture, public health, and government facilities. Examples include well-documented cyberattacks on the Ukrainian power grid, U.S. water infrastructure, including the Summer 2026 compromise of a Minnesota water system that prompted widespread password changes and concerns that configuration files may have been extracted, and ransomware targeting multiple sectors (e.g., Colonial Pipeline, public health and government facilities). These caused regional blackouts and damage, disrupting operations in multiple sectors. [2] These attacks pose risks to national security, the economy, and public health and safety.

Volt Typhoon, a PRC state-sponsored group linked to extensive intrusions into U.S. critical infrastructure, exemplifies the persistent threat to OT systems. Rather than seeking immediate disruption, this group focuses on cyber espionage and pre-positioning for future conflict. By maintaining long-term, covert access, Volt Typhoon aims to disable vital systems—such as power grids—at a time of their choosing to support geopolitical objectives. These intrusions typically begin with the compromise of IT networks before pivoting to OT environments. To facilitate this, the group utilizes 'living-off-the-land' (LOTL) techniques, employing native system tools to evade detection. As noted by the Cybersecurity and Infrastructure Security Agency (CISA) and other authoring agencies, Volt Typhoon conducts exhaustive pre-compromise reconnaissance to master a target's network architecture and operational protocols before striking. [3], [4] When addressing Advanced Persistent Threats (APTs), it is important to operate under the assumption that the environment is already compromised, aligning with core ZT principles.



Hardening DoW Critical OT Environments with Zero Trust Principles

These adversarial campaigns closely align with the SANS ICS Cyber Kill Chain, which describes the sequence of activities attackers use to progress from reconnaissance and initial access to manipulation of industrial processes and physical effects. [5] Rather than relying solely on perimeter defenses, Zero Trust applies continuous verification, least-privilege access, and policy enforcement throughout the environment to disrupt multiple phases of the kill chain, preventing adversaries from establishing persistence, moving laterally, or achieving operational objectives.

Attacks by nation-state actors and hacktivist groups illustrate the importance of securing OT environments and implementing ZT principles. These actors have compromised water and wastewater systems (WWS) and energy infrastructure by exploiting remote-access misconfigurations, legacy device weaknesses, and default passwords. Implementing ZT pillars and concepts—such as complex passwords, multifactor authentication, macro- and micro-segmentation, secure remote access, and continuous verification of users, devices, workloads, and machine-to-machine communications—can disrupt multiple phases of the SANS ICS Cyber Kill Chain, significantly reducing opportunities for adversaries to establish persistence, move laterally, and impact industrial processes. [6] The intent of these groups appears to be the disruption of operations, demonstration of capability, and highlighting potential for physical harm.

Similarly, campaigns by Iran-affiliated actors underscore the vulnerability of critical infrastructure to unauthorized remote access. As highlighted in joint cybersecurity advisory [AA26-097A](#), actors specifically targeted programmable logic controllers (PLCs) within the water and wastewater sector by exploiting Internet-exposed devices and default administrative credentials. These incidents further validate the requirement for a ZT-enabled architecture; by implementing policy-based access control (PBAC) based on attribute-based access control (ABAC) principles, organizations can continuously verify users, devices, assets, and resources before granting access, mitigating the primary attack vectors exploited in advanced persistent threat (APT) disruptions. [7]

These malicious campaigns illustrate the effectiveness of exploiting trusted relationships, exposed assets, and static access controls. These threats continue to evolve and are starting to use advanced super intelligence¹ (SI), including frontier models capable of automating complex analysis and decision-making, to accelerate attacks against OT environments. SI-enabled adversaries may rapidly identify previously unknown vulnerabilities, automate exploit development, generate convincing social engineering campaigns, orchestrate coordinated

¹ This guidance uses super intelligence in line with [Executive Order 14434](#).



Hardening DoW Critical OT Environments with Zero Trust Principles

attacks across numerous targets simultaneously, and optimize attack paths through complex cyber-physical environments. As SI capabilities become more accessible, critical infrastructure owners and operators should anticipate increasingly adaptive threats that target both digital systems and the physical processes they control. Since SI enables adversaries to execute these activities with greater speed, precision, and scale, Zero Trust's continuous verification, policy-based decision-making, and comprehensive visibility across human and non-human identities become increasingly essential to protect OT environments and enable resilient operations against evolving threats.

Target audience

This CSI provides guidance primarily intended for National Security System (NSS), Department of War (DoW), and Defense Industrial Base (DIB) network system owners, and the operators responsible for protecting these critical systems. Additional guidance supporting this CSI is available via the National Institute of Standards and Technology (NIST) and CISA. This guidance aligns with the [DoD Cybersecurity Reference Architecture](#) and complementary DoD Zero Trust guidance, including the [ZT Reference Architecture](#) and [ZT Strategy](#) for IT environments, as well as the [Zero Trust for Operational Technology \(OT\) Activities and Outcomes](#) guidance. [8], [9], [10], [11] It outlines methods to tailor and implement ZT concepts to strengthen system security and advance OT environments from target to advanced level maturity.

Background

[EO 14028 Improving the Nation's Cybersecurity](#), [NSPM-12 National Policy for the Cybersecurity of National Security Systems](#), and [NSM-22 Critical Infrastructure Security and Resilience](#) call for significant steps to address national security risks through implementation of IT and OT security critical functions that meet foundational ZT principles. [12], [13], [14] Additionally, [EO 14144 Strengthening and Promoting Innovation in the Nation's Cybersecurity](#) directs further actions. [15] Some of these actions include:

- Operationalizing Transparency and Security in Third-Party Software Supply Chains
- Aligning Policy to Practice
- Securing National Security Systems and Debilitating Impact Systems
- Additional Steps to Combat Significant Malicious Cyber-Enabled Activities



Hardening DoW Critical OT Environments with Zero Trust Principles

To meet these mandates, DoW NSS OT requires near-term ZT solutions that break existing cyber kill chains, achieve positive control of critical OT system processes, and establish visibility into system operations to identify and support eradication of any current and future adversary activity. These mitigation implementations must occur in legacy OT environments and components that cannot natively support many ZT Capabilities or satisfy the applicable ZT Activities and Outcomes.

OT is the foundational backbone of U.S. critical infrastructure. Unlike traditional IT, OT consists of integrated electrical, mechanical, and pneumatic control components, such as PLCs and distributed control systems (DCS) that interact with the physical world to manage power grids, water treatment, and manufacturing. [16]

The legacy nature of these systems creates a significant mission-risk paradox: while designed for decades of physical reliability, their cybersecurity architecture is obsolete. These aging assets often lack native encryption, modern authentication protocols, or the ability to be patched without disrupting essential services. This technological obsolescence, combined with physical hardware decay, creates a critical vulnerability gap. As these insecure-by-design systems are increasingly networked to meet modern efficiency demands, they become high-value targets for adversarial disruption, where a digital compromise can lead to catastrophic physical failure.

Zero Trust

ZT assumes the occurrence of adversarial breaches and uses a 'Never Trust, Always Verify' principle. Rooted in the foundational principles of [NIST SP 800-207](#), ZT represents a shift from perimeter-based security to a model that assumes no entity is trusted by default, requiring continuous evaluation of access based on identity, device posture, and session context. [17] Adopting a ZT mindset involves fundamentally reassessing organizational trust boundaries by considering the operational environment, systems, assets, users, and processes together when making cybersecurity and access decisions. It augments a traditional perimeter-based security model to a more dynamic approach and assumes no entity can be trusted by default. ZT is designed to continuously evaluate and authorize all actor actions through PBAC, using roles and attributes associated with users, devices, applications, assets, objects, and resources. This approach incorporates continuous monitoring, threat intelligence, and dynamic policy enforcement to provide comprehensive access control, segmentation, and data protection.

ZT implementation continuously evaluates and enforces authentication and authorization for comprehensive access control based on, but not limited to, actor identity, device posture, asset sensitivity, resource attributes, session context, policy requirements, and observed behavior.



Hardening DoW Critical OT Environments with Zero Trust Principles

Access decisions are dynamically adjusted through reauthentication, reauthorization, or policy updates when changes occur in the established trust or confidence level. The DoW CIO developed the ZT Framework as a comprehensive blueprint to guide DoW and its mission partners in designing, implementing, and maturing Zero Trust architectures (ZTAs) across military and defense networks. While the framework provides a foundation for advancing ZT adoption, successful implementation requires ensuring that deployed capabilities align with the underlying principles of ZT—such as continuous authorization, policy-based access control, full visibility, and dynamic decision-making—rather than solely improving existing cybersecurity hygiene practices.

The DoD CIO Zero Trust Framework utilizes **seven Pillars** to categorize the key functional domains (User, Device, Data, etc.) and **45 Capabilities** to define the specific technical requirements and security functions necessary to achieve a ZTA. This CSI identifies the **26 high-impact Activities** that serve as the tactical “How-To,” outlining the specific tasks and process changes necessary to meet many of the needed Outcomes and Capability requirements of the Zero Trust Framework to substantially reduce risk in legacy OT environments. Figure 1 shows a graphical description of the DoW ZT Pillars.

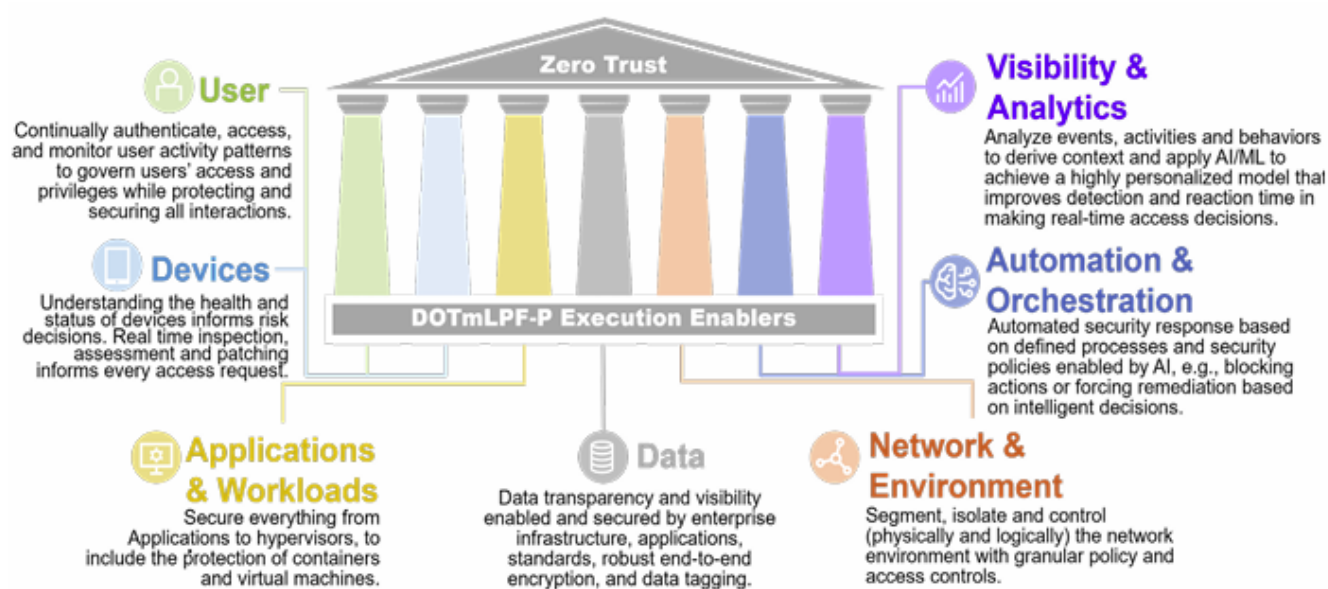


Figure 1: The seven Zero Trust Pillars

The implementation of ZT principles within a large and complex operational environment—such as a military base—necessitates rigorous planning, coordinated governance, and continuous verification that all accesses and interactions are authorized. Adopting ZT principles and



Hardening DoW Critical OT Environments with Zero Trust Principles

concepts in a large environment can be a daunting task. The following scenario illustrates the application of ZT principles.

- *Verify Explicitly:* All personnel and devices must authenticate using biometric identification, RFID badges, or multi-factor authentication (MFA) access tokens and utilize Comply to Connect (C2C) checks for their devices. For remote devices, where legacy hardware cannot natively support C2C agents, organizations should utilize proxy-based posture validation.
- *Least Privilege Access:* A cybersecurity analyst receives elevated access for two hours to patch a radar system, after which privileges expire automatically. Just-in-Time controls, limited by both time and location, are applied for all accounts and accesses.
- *Micro-Segmentation:* Systems are compartmentalized to ensure one breach does not affect all systems, similar to having bulkheads in a ship. Physical segmentation makes sure that all systems are not affected at the same time.
- *Identity-Centric Access:* All military base personnel badge scans are unique and tied to the person, which triggers alerts with automatic lockdowns when used in unauthorized areas.
- *User and Entity Behavior Analytics:* A user who normally logs in from Maryland suddenly attempts access from overseas and downloads large volumes of flight data; access is automatically revoked and flagged for investigation.

While initially designed to improve IT-based security architectures, ZT principles can address cybersecurity challenges in emerging technologies, operational environments, and expanded cyber terrain, including OT. However, many OT environments lag in their pace of ZT adoption and modernization as compared to IT environments due to the unique operational constraints, safety requirements, and extended lifecycles associated with legacy OT systems. Even though legacy OT assets may lack the native processing capability to support modern security agents, ZT implementations can evolve to be adopted in OT as part of a holistic approach that integrates cybersecurity capabilities with operational processes, governance, mission requirements, and risk-based decision-making. Technologies such as ZT-enabled gateways, ruggedized network devices, micro-segmentation, and continuous monitoring can improve the cybersecurity posture of legacy environments; however, these capabilities must be integrated within the broader operational context to enable effective authorization, access control, and protection of critical processes across hybrid IT/OT environments.



High-impact OT Zero Trust mitigation steps

Given the complexity of aging infrastructure, this CSI prioritizes 26 high-impact Activities based on their ability to provide immediate compensating control. The methodology focuses on the 'User', 'Device', 'Data', 'Network & Environment', 'Application & Workload', and 'Visibility & Analytics' pillars, selecting activities that wrap legacy assets in protective enclaves without requiring intrusive hardware modifications. By focusing on these high-impact Target Level Activities, organizations can achieve a foundational ZT posture that secures the most vulnerable mission-essential functions first.

Implementing the following 26 identified high-impact ZT target Activities mitigates critical vulnerabilities by replacing implicit trust with continuous, evidence-based verification. This improves the protection posture of legacy OT environments by strengthening the ability to verify and control authorized actions, reducing operational risk associated with unauthorized access, unapproved process flows, and unauthorized configuration changes that could impact mission-essential functions.

- **Securing remote access:** Restrict access to only authorized actors.
- **Protecting OT data:** Encrypt all outbound data to maintain confidentiality and integrity. If OT protocols do not support encryption, other options include a security broker, secure enclaves, gateways, or tunnels.
- **Inventorying OT assets:** Maintain an accurate OT asset inventory as a foundational step in building a defensible architecture.
- **Enhancing OT environment visibility:** Continuously identify and categorize OT assets and monitor network communications to establish normal operational baselines and detect abnormal or malicious activity.
- **Utilizing OT cyber threat Intelligence:** Know the adversary's tactics, techniques, and procedures.
- **Hardening smart controllers:** Secure devices, perform code and log analysis, while ensuring they meet operational (availability) requirements.
- **Strengthening networks with segmentation and monitoring:** Strengthen security controls across the OT environment, including networks, systems, devices, and other operational assets, while continuously monitoring human and non-human actors for potential threats, vulnerabilities, and unauthorized activity.



Hardening DoW Critical OT Environments with Zero Trust Principles

- **Securing engineering workstations and human-machine interfaces:** Protect engineering workstations, HMIs, controllers, applications, services, and machine-to-machine communications by enforcing appropriate authorization, least privilege, and monitoring controls to prevent unauthorized access, misuse, or manipulation of OT systems.
- **Enforcing security via hardened Active Directory and Domain Controllers:** Utilize these mechanisms to implement robust security policies across the network.
- **Verifying and assessing ZT controls safely:** Validate ZT controls using passive techniques, such as configuration audits, log analysis, and SPAN/TAP network monitoring whenever possible. Perform active testing only when necessary, during approved maintenance windows, to avoid disrupting operationally sensitive OT assets and ensure the continued safety, reliability, and availability of industrial operations.

Securing remote access

Securing remote access manages unnecessary external exposure and mediates all remote access through controlled, monitored, identity-aware access paths. When connections outside the OT environment are required, they must be secured. NSA and others have published secure remote access recommendations aimed at critical infrastructure entities with OT components. [18], [19], [20] One of the first recommendations includes removing “direct” OT environment connections to the public Internet. OT components often lack robust authentication or authorization, making connections to the public Internet a serious risk.

Other recommendations include using virtual private networks (VPNs), requiring strong passwords (**OT ZT Activity 1.8.1**), transitioning to phishing-resistant MFA (**OT ZT Activity 1.3.1**), enforcing least privilege concepts including role-based access controls (**OT ZT Activity 1.2.2**), disabling dormant accounts (**OT ZT Activity 1.2.1**), and finally implementing a privileged access management (PAM) solution (**OT ZT Activity 1.4.1**). [21]

Remote access provided to third-party vendors, original equipment manufacturers (OEMs), system integrators, and maintenance personnel presents a significant risk to OT environments and has been a common vector in confirmed OT intrusions. Such access should be treated with the same—or greater—level of scrutiny as internal remote access. Consistent with *Life Cycle Management for OT Environments Part 1* (**OT ZT Activity 1.5.1**), all third-party and OEM access should be authenticated using phishing-resistant MFA, authorized through PBACs, and limited to approved users, devices, and resources. Access should be explicitly approved, time-bound, continuously monitored, and terminated immediately upon completion of authorized



Hardening DoW Critical OT Environments with Zero Trust Principles

activities. Where feasible, vendor access should be mediated through controlled access gateways or PAM solutions that provide session recording, auditing, and real-time oversight to reduce the risk of unauthorized actions affecting mission-critical OT processes.

Protecting OT data

Communications involving OT systems should use approved encryption to protect critical data in transit and at rest, regardless of network location, with additional protections applied based on data sensitivity, operational requirements, and risk. Often the confidentiality and integrity of this data must be protected until it is processed within an authorized and monitored OT environment. OT system processes that rely on communications data are often sensitive to timing and disturbance; therefore, data manipulation, injection, and corruption adversely impact OT processes as much as changing device configurations. For example, time-sensitive OT data includes time-series industrial data directly from control systems, sensors, and assets.

Protecting data in transit should use **OT ZT Activity 5.4.3, *Protect OT Data in Transit***. Unlike the traditional IT cybersecurity concept of protecting data "in transit," which primarily emphasizes encryption of network traffic, this OT Zero Trust Activity encompasses a broader set of protections. These include ensuring availability and reliability, in addition to confidentiality, integrity, and authenticity, of communications between OT assets while accounting for the unique operational and protocol requirements of industrial environments. Encryption may be one component of this activity, but does not, by itself, satisfy the intent of the OT Zero Trust requirement. [22]

Inventorying OT assets

It is critical to develop a centralized inventory for non-person entities (NPEs) (**OT ZT Activity 2.1.1**). This inventory includes a living, regularly updated list of OT assets, such as hardware, software, network devices, and components. Asset inventories capture high-priority attributes, such as criticality, role/type, manufacturer/model, operating system or firmware version, Internet Protocol/Media Access Control address, physical location, and ports/services used. Without a comprehensive OT asset inventory, organizations cannot reliably identify the assets operating within the environment or establish an authoritative baseline for security and operational management. [23]

In conjunction with the asset baseline, it is essential to inventory users and accounts, especially service accounts, (**OT ZT Activity 1.1.1**). It is also important to account for application and code inventories (**OT ZT Activity 3.1.1**) and current device configurations (**OT ZT Activity 2.6.2**). These inventories can be conducted either manually or through an automated process. [24]



Enhancing OT environment visibility

In OT environments, system visibility comes from knowing assets (hardware, software, network components, etc.) in the inventory, along with their function, criticality, and communication pathways. Keeping operational baseline information current for the entire system is essential for managing risk, responding to incidents, and protecting operations. When defining this operational baseline, identify each OT asset, its operational function, how it contributes to the industrial process, and how it participates in communications and interactions within the OT environment. Assign roles and responsibilities for inventory and baseline ownership and upkeep. Categorize OT assets based on their criticality, operational function, and security requirements to support risk assessment, policy development, and Zero Trust implementation.

Establish and maintain an authoritative repository for OT asset inventory and operational baseline information. The repository may be implemented as a centralized system or a federated capability, provided it supports consistent asset identification, governance, and access to current inventory and operational baseline information across the OT environment. Secure data that is used in the centralized repository or system. Establish consistent patterns and standards for capturing, organizing, and presenting this information. These standards should support common naming conventions, dependency identification, and visualization of relationships among assets to improve asset understanding and enable effective ZT policy decisions. From a ZT perspective, the requirements for data labeling, as well as identifying and inventorying databases, can be found in **ZT OT Activity 4.1.1**, *OT Data Tagging Governance*, and **ZT OT Activity 4.4.5**, *Inventory Databases*.

Utilizing OT cyber threat intelligence

It is critical for DoW and Service Components to use known OT Cyber Threat Intelligence. Integrate relevant OT security data sources and telemetry feeds into security monitoring capabilities, such as an OT-focused Security Information and Event Management (SIEM) solution, to improve threat visibility, event correlation, and alerting. Where applicable, integrate SIEM capabilities with Security Orchestration, Automation, and Response (SOAR) capabilities to support coordinated analysis, workflow automation, and response actions. Integration with data collected from system access enforcement points is needed to monitor CTI-driven data alerting and response for the OT System. Additional details are provided in **OT ZT Activity 7.5.1**, *OT Cyber Threat Intelligence Program Part 1*, and **OT ZT Activity 7.5.2**, *OT Cyber Threat Intelligence Program Part 2*.



Hardening smart controllers

To operate securely and effectively, OT systems leverage smart controllers to protect, monitor, and execute processes. In legacy environments, smart controllers serve as the primary interface between the cyber and physical domains; because they lack modern onboard security, they must be shielded using external ZT controls to prevent digital compromises from manifesting as physical failures. While upgrading a device to the vendor's newest, secure model is usually the best solution, it requires engineering review, testing, outage coordination, contingency planning, and vendor support when initially implementing OT risk mitigations. Initial critical security actions are to configure the built-in security features on smart controllers and verify that device configurations align with approved functionality, operational requirements, and process logic. These activities are particularly important because smart controllers directly influence physical process operations and often serve as central points for communicating control commands between supervisory systems and field devices. Improper configuration or unauthorized changes to these devices could affect process availability, safety, or operational integrity. OT system hardening requires a risk-based approach that considers cybersecurity objectives, operational requirements, and the potential impact of security changes on safety and availability. Organizations should prioritize hardening activities that provide the greatest risk reduction while minimizing disruption to critical operations.

Patching is one component of this approach, but can be challenging in OT environments due to factors such as limited maintenance windows, system availability requirements, vendor support constraints, and potential impacts to connected devices. When patches cannot be immediately applied, organizations should evaluate compensating controls, prioritize remediation based on asset criticality and exposure, and establish planned maintenance activities to reduce risk while maintaining operational continuity. Develop a patch management plan that leverages a test or development environment to examine the downstream impacts of new patches, addresses patch windows that will have the least amount of impact on critical operations performed by the controllers, and focuses on patching controllers with the most risk exposure first. These recommendations align with **OT ZT Activity 2.5.1, *Implement Vulnerability and Patch Management Tools for OT Environments***. While vulnerability and patch management are not substitutes for ZT access enforcement, they provide important security posture information that can support ZT decision-making. Maintaining awareness of asset vulnerabilities, configuration status, and remediation progress enables organizations to make more informed policy decisions regarding access, segmentation, and risk mitigation.



Hardening DoW Critical OT Environments with Zero Trust Principles

Often, many OT systems operate with smart controllers that are still set to the vendor's default passwords and use insecure protocols to transmit instructions. As part of a secure installation and configuration process, organizations should establish and maintain approved security configurations for smart controllers and other OT devices. This includes always changing default administrative credentials, applying appropriate password policies, disabling unnecessary insecure services, and enabling secure management protocols where supported.

Many OT devices are initially deployed with default configurations that may not align with organizational security requirements. Where technically feasible, organizations should configure controllers to use secure protocols such as HTTPS, SSH, and secure OT protocols for administrative activities and remote access. These practices support **OT ZT Activity 2.6.2, *OT Device Configuration Management***, by maintaining known and controlled device configurations.

In situations where immediate operational needs prevent full implementation of secure configurations, organizations should document exceptions, evaluate associated risks, incorporate compensating controls, and establish a plan to complete required hardening activities when operational conditions permit.

Another way to reduce the potential impact of an OT cybersecurity attack is to limit the permissions of smart controller actors, aligning with **OT ZT Activity 1.7.1, *Deny by Default Policy in OT Environments***. Most controllers can limit access levels or enforce login requirements that limit endpoint controller access (i.e., view and change levels). The 'view' level is an example of enforcing least-privilege access by limiting authorized actors to monitoring the controller and system process without permitting changes to the controller's operating conditions. Some vendors will provide additional access levels for managing the smart controller's features, but for initial security needs, being able to change device configuration must be controlled and monitored in device logging.

Understanding how the smart controller is programmed and which features are enabled provides the system operator with better situational awareness of how the OT process operates, while also reducing the attack surface of the smart controller. **OT ZT Activity 3.3.1, *Binaries, Code, and Hardware Configurations for OT Environments***, recommends disabling unused logic to prevent an attacker from repurposing it for malicious activity.

Strengthening networks with segmentation and monitoring

Implement logical network segmentation to separate OT assets based on operational function, role, criticality, and communication requirements. Where supported, configure managed network infrastructure, including VLANs, routers, and firewalls, to enforce authorized communication



Hardening DoW Critical OT Environments with Zero Trust Principles

paths, restrict unnecessary traffic, and generate audit logs. These activities support **OT ZT Activity 5.4.1, *Implement Micro Segmentation***.

Auditing required protocol use can be completed through **OT ZT Activity 2.2.1, *Implement Connection Policy for OT Environments***. By defining and enforcing authorized communication protocols and connection paths, organizations can identify the use of unauthorized protocols, unexpected communication pathways, or deviations from approved operational communications, enabling investigation and appropriate response.

Deploy OT-appropriate network monitoring capabilities to continuously observe network communications and detect deviations from approved operational behavior. Where appropriate and supported, implement technologies such as intrusion detection systems (IDS), endpoint detection and response (EDR), and centralized security monitoring to improve visibility into OT activity and support timely investigation and response. Establish a baseline of expected network communications and configure monitoring capabilities to identify unauthorized protocols, unexpected communication paths, or other anomalous network behavior. These activities support **OT ZT Activity 2.7.1, *Implement EDR Tools for OT Environments***.

Securing engineering workstations and human-machine interfaces

Engineering workstations (EWs) and human-machine interfaces (HMIs) are usually built using basic IT microcomputers and displays. If not secured properly, an attacker can leverage built-in tools to attack the OT system process. Since these computers often leverage traditional operating systems, a wide range of options are available to secure and harden these computers. As ZT principles are incorporated into HMI and EW designs, overall system security can improve. Ideally, these devices should have all logging capabilities turned on; at a minimum, event logging should be enabled for access, application, and external connections (e.g., Ethernet, USB, Display, wireless, etc.). Logging recommendations are referenced in **OT ZT Activity 4.4.1, *DLP Analytics*** and are a core component of the broader ZT goal to capture and parse all system events for analysis (related to **OT ZT Activity 7.1.2, *Log Parsing in OT Environments***).

For OT processes, it is essential that organizations implement robust security measures, specifically logical segmentation and data isolation, which can be addressed with **OT ZT Activity 5.3.2, *Base/Camp/Post/Station/Segmentation***, to protect vendor software from unauthorized changes and ensure data at rest is secure from unauthorized users on the system. EW computers usually house all, or portions of, system drawings, network diagrams, standard operating procedures (SOPs), and designs, which could significantly guide attacks if not



Hardening DoW Critical OT Environments with Zero Trust Principles

properly protected. File activity monitoring for improper access or modification is addressed in **OT ZT Activity 4.4.3**, *OT File Prioritization and Monitoring*.

Once a user is authorized on an engineering workstation, access must be limited to only those functions and instructions explicitly authorized by their assigned role. Role permissions and privileges should be strongly bound to the assets, objects, and resources required to perform authorized tasks, ensuring that human users and all other process-invoking elements can execute only approved activities. Policy requirements should restrict the ability of a malicious actor from launching scripts and code from various common ingress points, such as the EWs. Limiting unauthorized user access to systems and software is supported by **OT ZT Activity 1.2.1**, *Implement Authorization and Access Management for OT Environments*. It is important to note that one of the most effective security practices is ensuring these devices are restricted for only OT system use and kept in locked locations to prevent tampering and unauthorized use.

Enforcing security via hardened Active Directory and Domain Controllers

The Domain Controller (DC) servers (e.g., Active Directory) that support OT environment user authentication must be continuously monitored, maintained, and upgraded. For a system owner and cybersecurity responder, there is hardly a more challenging scenario than an unauthorized actor moving freely throughout the network while appearing as a legitimate user. Implementing PBAC, or ABAC where applicable, helps mitigate this risk by continuously evaluating identity, role, attributes, device posture, and other contextual factors before authorizing access to specific resources and actions. This limits an actor's ability to perform activities beyond those explicitly permitted by policy, even when using compromised credentials. Hardening DCs involves a multi-faceted approach, often guided by standards like those from the Center for Internet Security (CIS), NIST, and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs). A few examples to harden DCs include implementing a tiered administration model, strong password policies and authentication, the principle of least privilege, and secure configuration through Group Policy Objects. User monitoring is referenced in **OT ZT Activity 1.7.1**, *Deny by Default Policy in OT Environments*.

Verifying and assessing ZT controls safely

Verification of hardening and related Zero Trust activities should prioritize passive assessment techniques that minimize operational risk to OT environments. System owners should rely on configuration audits, log analysis, and passive network monitoring (e.g., analysis of SPAN or TAP traffic) to validate that security controls, access policies, and network segmentation are functioning as intended. Where active assessment techniques are necessary, they should be



Hardening DoW Critical OT Environments with Zero Trust Principles

carefully planned, coordinated, and executed during approved maintenance windows, with particular care taken to avoid disruption to Level 0 and Level 1 devices and other operationally sensitive assets. This approach supports continuous validation of Zero Trust objectives while maintaining the safety, reliability, and availability of industrial operations and is supported by **OT ZT Activity 5.3.1, OT Plane Segmentation**.

Summary

The adoption of Zero Trust principles is essential for enhancing the security of legacy OT, ensuring adherence to EO 14028, EO 14409, NSPM-12, and NSM-22 guidance, while enabling defense-in-depth across critical infrastructure. While the age and limited functionality of these systems present significant challenges, the path forward lies in utilizing compensating controls that provide modern protection without requiring a total hardware overhaul.

To maintain the security of legacy OT environments, a comprehensive evaluation of current infrastructure is required, followed by the prioritization of these high-impact measures:

- Securing remote access
- Protecting OT data
- Inventorying OT assets
- Enhancing OT environment visibility
- Utilizing OT cyber threat intelligence
- Hardening smart controllers
- Strengthening networks with segmentation and monitoring
- Securing engineering workstations and human-machine interfaces
- Enforcing security via hardened Active Directory and Domain Controllers
- Verifying and assessing ZT controls safely

By focusing on these strategic priorities, organizations can bridge the architectural gap, effectively shielding legacy hardware within a resilient, verifiable ZT environment.

This CSI identifies 26 high-impact Activities from the broader ZT framework to provide organizations with a manageable starting point for transitioning from perimeter-based defenses toward a verifiable, resilient, and adaptive architecture.



Hardening DoW Critical OT Environments with Zero Trust Principles

Strategic evaluation of legacy OT combined with targeted implementation of security enhancements can drive significant improvements in system protection. Tackling legacy-specific challenges head-on with ZT mitigations can significantly enhance the system's security posture and maintain control over critical OT assets, even in the face of budget and technology constraints and evolving adversary techniques and capabilities.

Further reading and guidance

- **SANS Institute – ICS Cyber Kill Chain**

The ICS Cyber Kill Chain describes how adversaries progress from compromising IT networks to manipulating industrial control systems and physical processes.

Understanding these attack phases helps organizations identify opportunities to detect, delay, and disrupt attacks before operational impacts occur. Applying ZT principles—such as least privilege, network segmentation, secure remote access, and continuous monitoring—helps reduce adversary movement and strengthen the resilience of OT environments. [5]

- **Executive Order 14028 – Improving the Nation's Cybersecurity**

EO 14028 established the strategic direction for federal cybersecurity modernization and directly influenced the development of the Federal Zero Trust Strategy, DoD Zero Trust Strategy, and supporting implementation guidance. Organizations securing OT environments should understand EO 14028 as the policy foundation for adopting identity-centric, continuously verified, and risk-informed security architectures. [12]

- **NSA Zero Trust Implementation Guidelines (ZIGs)**

In alignment with the current DoW ZT Framework, the NSA Zero Trust Implementation Guidelines (ZIGs) are most applicable in an IT Enterprise. Future updates may address other contextual environments, including OT, Defense Critical Infrastructure (DCI), and/or Tactical/Weapons Systems. [25]

- **Operational Technology Assurance Partnership (OTAP)**

The National Security Agency (NSA) is developing the Operational Technology Assurance Partnership (OTAP), a pilot cybersecurity conformance testing program for NSS OT, to improve OT security standards and share recommendations for security policies and technical requirements for operational technology (OT) installed in National Security Systems (NSS). [26]



Hardening DoW Critical OT Environments with Zero Trust Principles

- **Adapting Zero Trust Principles to Operational Technology**

Outlines how to apply ZT in ICS and OT environments. It emphasizes continuous verification of access and identity to prevent threat actors from moving laterally across essential, physical infrastructure. [27]

- **Executive Order 14409 – Promoting Advanced Artificial Intelligence Innovation and Security**

Promotes the secure adoption of advanced SI to strengthen federal cybersecurity through SI-enabled defensive capabilities, accelerated vulnerability remediation, and enhanced protection of critical infrastructure, complementing ZT and defense-in-depth strategies. [28]

Works cited

- [1] International Society of Automation. Addressing Cybersecurity Risks in Legacy OT Systems: A Practical Guide. 2025. <https://gca.isa.org/blog/addressing-cybersecurity-risks-in-legacy-ot-systems-a-practical-guide>
- [2] The Cyber Defense Review. Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack. 2021. https://cyberdefensereview.army.mil/Portals/6/Documents/2021_summer_cdr/02_ReederHall_CDR_V6N3_2021.pdf
- [3] Cybersecurity and Infrastructure Security Agency et al. PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. 2024. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>
- [4] Microsoft Threat Intelligence. Volt Typhoon targets US critical infrastructure with living-off-the-land techniques. 2023. <https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/>
- [5] SANS Institute. The Industrial Control System Cyber Kill Chain. 2015. <https://www.sans.org/white-papers/36297>
- [6] Cybersecurity and Infrastructure Security Agency et al. Defending OT Operations Against Ongoing Pro-Russia Hactivist Activity. 2024. <https://www.cisa.gov/sites/default/files/2024-05/defending-ot-operations-against-ongoing-pro-russia-hactivist-activity-508c.pdf>
- [7] Cybersecurity and Infrastructure Security Agency et al. Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure. 2026. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a>
- [8] Department of Defense. Department of Defense (DoD) Cybersecurity Reference Architecture. 2023. <https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf>
- [9] Department of Defense. Department of Defense (DoD) Zero Trust Reference Architecture Version 2.0. 2022. [https://dodcio.defense.gov/Portals/0/Documents/Library/\(U\)ZT_RA_v2.0\(U\)_Sep22.pdf](https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf)
- [10] Department of Defense. DoD Zero Trust Strategy. 2022. <https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf>



Hardening DoW Critical OT Environments with Zero Trust Principles

- [11] Department of Defense. Department of Defense Zero Trust for Operational Technology. Zero Trust for Operational Technology Activities and Outcomes. 2025.
https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-OperationalTechnologyActivitiesOutcomes_v2.pdf
- [12] The White House. Executive Order on Improving the Nation's Cybersecurity. 2021.
<https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/se.archives.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>
- [13] The White House. National Security Presidential Memorandum/NSPM-12. 2026.
<https://www.whitehouse.gov/presidential-actions/2026/06/national-security-presidential-memorandum-nspm-12/>
- [14] The White House. National Security Memorandum on Critical Infrastructure Security and Resilience. 2024.
<https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/>
- [15] The White House. EO 14144: Sustaining Select Efforts to Strengthen the Nation's Cybersecurity. 2025.
<https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/>
- [16] National Institute of Standards and Technology. Special Publication 800-82r3: Guide to Operational Technology (OT) Security. 2023. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf>
- [17] National Institute of Standards and Technology. Special Publication 800-207: Zero Trust Architecture. 2020.
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>
- [18] National Security Agency. Stop Malicious Cyber Activity Against Connected Operational Technology. 2021.
https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/0/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF
- [19] United Kingdom National Cyber Security Centre (NCSC-UK) et al. Secure connectivity principles for Operational Technology (OT). 2026. <https://www.ncsc.gov.uk/sites/default/files/documents/ncsc-secure-connectivity-for-operational-technology.pdf>.
- [20] Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) et al. Principles of operational technology cyber security. 2024. https://media.defense.gov/2024/Oct/01/2003556960/-1/-1/0/PRINCIPLES_OF_OPERATIONAL_TECHNOLOGY_CYBER_SECURITY.PDF
- [21] Cybersecurity and Infrastructure Security Agency et al. Primary Mitigations to Reduce Cyber Threats to Operational Technology. 2025. <https://www.cisa.gov/resources-tools/resources/primary-mitigations-reduce-cyber-threats-operational-technology>
- [22] Cybersecurity and Infrastructure Security Agency. Barriers to Secure OT Communication: Why Johnny Can't Authenticate. 2026. <https://www.cisa.gov/resources-tools/resources/barriers-secure-ot-communication-why-johnny-cant-authenticate>
- [23] Cybersecurity and Infrastructure Security Agency et al. Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators. 2025. <https://www.cisa.gov/resources-tools/resources/foundations-ot-cybersecurity-asset-inventory-guidance-owners-and-operators>
- [24] Idaho National Laboratory. Achieving Visibility and Control in OT Systems: Remote Maintenance, Securing Remote Access, and the Zero-Trust Approach. 2023. https://www.cisa.gov/sites/default/files/2023-05/Achieving%20Visibility%20and%20Control%20in%20OT%20Systems%20Remote%20Maintenance%2C%20Securing%20Remote%20Access%2C%20and%20the%20Zero-Trust%20Approach_508c.pdf



Hardening DoW Critical OT Environments with Zero Trust Principles

- [25] National Security Agency. Zero Trust Implementation Guideline Primer. 2026.
https://media.defense.gov/2026/Jan/08/2003852320/-1/-1/0/CTR_ZERO_TRUST_IMPLEMENTATION_GUIDELINE_PRIMER.PDF
- [26] National Security Agency. Operational Technology Assurance Partnership: Smart Controller Security within National Security Systems. 2025. <https://media.defense.gov/2025/Apr/22/2003695617/-1/-1/0/CTR-OTAP-SMART-CONTROLLER-SECURITY-IN-NSS.PDF>
- [27] Cybersecurity and Infrastructure Security Agency et al. Adapting Zero Trust Principles to Operational Technology. 2026. https://www.cisa.gov/sites/default/files/2026-04/joint-guide-adapting-zero-trust-principles-to-operational-technology_508c.pdf
- [28] The White House. EO 14409: Promoting Advanced Artificial Intelligence Innovation and Security. 2026. <https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/>

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of War, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov

Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov

Media Inquiries / Press Desk: NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov



Appendix: Prioritized OT ZT Activities

The following ZT Activities were prioritized based on a risk-reduction methodology that emphasizes non-intrusive security overlays; these specific tasks were selected because they provide the highest degree of adversarial containment and operational visibility for legacy assets that cannot natively support modern security agents:

Table 1: Prioritized OT ZT Activities

Activity Number	OT ZT Activity Name	OT Activity Outcomes
1.1.1	Inventory Users in OT Environment	1. Identified and documented inventory of accounts across both the Operational IT and Process Control environments 2. All applications and systems with local identity stores have been identified 3. Local user, local privileged, shared, must-run, and service OT accounts have been identified for migration and/or decommissioning.
1.2.1	Implement Authorization and Access Management for OT Environments	1. Authorized Credentialing service is implemented for the Operational IT environment 2. Attributes for authentication and authorization of users are defined 3. OT credentialing service enabled to add and update attributes 4. OT privileged accounts are authorized based on roles and attributes 5. Shared group, must-run, and service OT accounts have been migrated and/or decommissioned.
1.2.2	Role Based Dynamic Access for OT Environments	1. Rules are defined for third party and remote access into the OT environment 2. Role-based enforcement of user access to the environment; Authorized Credentialing service required for Privileged accounts 3. Identified High-privileged accounts and enforced using dynamic access.
1.3.1	MFA for OT Environments	1. MFA, or approved authoritative credentialing solution, is implemented with the Authorized Credentialing Service for access.
1.4.1	Implement PAM for OT Environments Pt. 1	1. OT PAM solution implemented 2. Integration points with appropriate applications, services, and devices are identified to support interoperability across the environment 3. Applications, services, devices that can be readily integrated with the PAM solution are integrated.
1.5.1	Life-Cycle Management for OT Environments Pt. 1	1. OT Environment Identity Life-Cycle Management process developed, documented, and implemented.



Hardening DoW Critical OT Environments with Zero Trust Principles

Activity Number	OT ZT Activity Name	OT Activity Outcomes
1.7.1	Deny by Default Policy in OT Environments	1. Default permission levels have been significantly reduced, thorough audit of identity and group usage with revocation of unnecessary permissions 2. Auditing process has been automated where possible 3. Static privileged users decommissioned or had permissions reduced.
1.8.1	Initial Authentication in OT Environments	1. Authentication of users is implemented across applications per session.
2.1.1	Inventory NPEs in OT Environment	1. DoW Components have developed a centralized inventory of NPE, incorporating existing inventories through manual and/or passive discovery-based automated solutions. 2. Inventories are manually validated and audited periodically.
2.2.1	Implement Connection Policy for OT Environments	1. DoW Enterprise policy, standards, and requirements for connection policies are refined and documented. 2. Refined policies clearly dictate the frequency and scope of compliance audits to meet minimum security standards. 3. DoW Components implement and enforce compliance-based network authorization, specifically for the Process Control environment as appropriate. 4. Compliance enforcement is risk-based, prioritizing the Operational IT and Process Control environments as appropriate.
2.5.1	Implement Vulnerability and Patch Management Tools for OT Environments	1. OT Environments are maintained to current approved compliance standards, patching levels, and configuration profiles. 2. Periodic reassessments are performed for all devices to verify ongoing compliance. 3. For Process Control environments, a risk-based approach is used to mitigate vulnerabilities, particularly where patch sources are unavailable, prioritizing process reliability.
2.6.2	OT Device Configuration Management	1. Standards and policies are defined for OT device management for the Operational IT and Process Control environments. 2. Automated configuration management is enabled.
2.7.1	Implement Endpoint Detection & Response (EDR) Tools for OT Environments	1. EDR solutions are implemented for both Operational IT and Process Control environments, following system analysis to determine and prioritize automated responses.
3.1.1	OT Application and Code Inventory	1. All applications within the Operational IT environment, and the Enterprise IT and which interoperate with the Operational IT environment, are identified, categorized, tracked, and documented.



Hardening DoW Critical OT Environments with Zero Trust Principles

Activity Number	OT ZT Activity Name	OT Activity Outcomes
3.3.1	Binaries, Code, and Hardware Configurations for OT Environments	1. Application control solutions are implemented on inventoried applications.
4.1.1	OT Data Tagging Governance	1. A governing body is established to define and maintain controlled terminology, file formats, and communication protocols for interoperable data transmission, querying, and storage across communities. 2. DoW Component categorizes and analyzes their data to align with the established controlled terminology. 3. DoW Component determines and implements data tagging structures and maps based on workflow processes and operational risk, including a characterization method for all data in the OT environment. 4. Exemptions for data tagging have been submitted by the DoW Component with justification.
4.4.1	DLP Analytics	1. DLP types, recognition patterns, and analytics processes are established 2. DLP analytics process enables policy enforcement for how sensitive data is handled and shared and enables monitoring and detection of data loss events.
4.4.3	OT File Prioritization and Monitoring	1. Data and files of critical classification are actively being monitored 2. Data owners utilize File Monitoring tools to monitor files in order of established priority 3. Basic Integration is in place with a monitoring system such as a SIEM.
4.4.5	Inventory Databases	1. Databases are identified and documented within the OT Operational Environment.
5.3.1	OT Plane Segmentation	1. Traditional tiered and/or service-based plane segmentation is implemented. 2. Enforcement checks of attributes, behavior, or other data using behavioral analytics engines are established.
5.3.2	B/C/P/S Segmentation	1. Segmentation is implemented across base, camp, post, and stations using logical zones to limit lateral movement. 2. Attribute and behavior-based enforcement checks are implemented to enforce defined access policies across the base, camp, post, and stations.
5.4.1	Implement Micro Segmentation	1. Micro segmentation is implemented in the OT environment. 2. Automated policy changes are enabled following human approval.
5.4.3	Protect OT Data in Transit	1. Data is protected in transit per policy through the OT environment.



Hardening DoW Critical OT Environments with Zero Trust Principles

Activity Number	OT ZT Activity Name	OT Activity Outcomes
7.1.2	Log Parsing in OT Environments	1. Common behaviors are developed or identified, and are prioritized based on all relevant documented processes. 2. Log data has sufficient attributes to analyze the behavior model.
7.5.1	OT Cyber Threat Intelligence Program Pt. 1	1. An OT-focused CTI program is established, defining processes for identifying, analyzing, and disseminating threat intelligence. 2. The CTI program integrates relevant data feeds into the SIEM solution that is deployed in the OT environment. 3. CTI-driven data alerting and response are integrated with enforcement points across Enterprise IT, Operational IT, and Process Control environments.
7.5.2	OT Cyber Threat Intelligence Program Pt. 2	1. The OT CTI program is expanded to include authenticated, private, and controlled CTI data feeds 2. A CTI community of interest is established, identifying and engaging key stakeholders.