EXECUTIVE SUMMARY
ZERO TRUST FOR OPERATIONAL TECHNOLOGY

ZERO TRUST FOR OPERATIONAL TECHNOLOGY - SCOPE AND PURPOSE

The Department of War (DoW) Chief Information Officer (CIO) established the Zero Trust (ZT) Portfolio Management Office (PfMO) to coordinate, synchronize, and accelerate adoption of ZT architecture and cybersecurity framework across the DoW enterprise. The ZT security model transitions away from trusted networks, actors, and devices to an environment with continuous authentication and fine-grained policy enforcement. In July 2025, the Department issued DTM 25-003, "Implementing the DoD Zero Trust Strategy," which directs DoW Components to achieve, at minimum, Target Level ZT across all unclassified and classified systems (including national security systems) and control systems/Operational Technology (OT).

The following ZT guidance is underpinned by DoW policy and authoritative guidance (e.g., DoDI 8500 Series, DoD CSRA, DoD Control Systems SRG and RMF control systems overlays) [1], the adoption of NIST (e.g., NIST 800-82 rev3). This guidance represents authoritative Department guidance pertaining to ZT for OT and Control Systems and is expected to be implemented in addition to all existing cybersecurity requirements. Any questions on this guidance should be raised to the DoW CIO ZT PfMO at osd.pentagon.dod-cio.mbx.zt-pfmo@mail.mil.

The DoW ZT Roadmap, DoW ZT Reference Architecture, and DoW ZT Execution Roadmap define and layout the execution of the Capabilities, Activities, and Outcomes that will promote a common ZT implementation across DoW. The ZT for OT Activities and Outcomes build upon these guiding ZT documents, adapting them to the unique characteristics and challenges of OT environments and aligned to existing required control systems/OT cybersecurity policy and guidance [2]. As defined in NIST SP 800-82 rev3, OT includes a broad range of programmable systems and devices that interact with the physical environment or manage devices that interact with the physical environment. These systems and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems. OT environments and control systems, regularly operate where there is "a significant need for continuous and reliable operations" [3]. As such, their reliability and security are paramount to national security and economic stability. ZT requirements complement and enhance existing DoW CS Program security requirements. DoW system owners are responsible for adhering to all applicable DoW CS Program direction, including, but not limited to, the requirements in DoD Instructions (DoDI) such as DoDI 8500.01, DoDI 8510.01, the DoD Cybersecurity Reference Architecture 5.0 (CSRA), and the DoD Control Systems Security Requirements Guide and its preceding iterations (SRG).

This guidance provides a revised set of Activities and Outcomes to facilitate current and future adoption of ZT principles in OT environments, accounting for the distinct differences between Information Technology (IT) and OT practices. The ZT for OT Activities and Outcomes are aligned to the ZT for Enterprise IT Activities and Outcomes to facilitate interoperability and alignment between the two. This guidance is focused on DoW owned OT environments and control systems up to and including the point of demarcation, encompassing facility related control systems, power grids, water treatment facilities, security and life safety systems, energy management systems, transportation networks, logistics handling, and manufacturing control systems. This extends to the boundary of Weapon Systems

[1] DoD Instruction, "Cybersecurity", October 7, 2019, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf
DoD Cybersecurity Reference Architecture (CSRA)
[2] DoDI 8500 Series CS program requirements and the DoD Control Systems Security Requirements Guide (SRG) provide direction and authoritative guidance on DoD-owned OT/control systems security. ZT outcomes intend to aid system owners in appropriately tailoring and enhancing security objectives for their systems.
[3] Framing risk in OT environments is discussed in NIST SP 800-82, Guide to Operational Technology (OT) Security, September 2023, p. 46-47.
https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf
DoD Control Systems Security Requirements Guide, July 14, 2021
https://dl.dod.cyber.mil/wp-content/uploads/external/pdf/071421_Control_Systems_SRG.pdf
FRCS Overlay https://cybersecurityks.osd.mil/dodcs/HelpandResources/References/Reference%20Library/U_FRCS_Overlay_Rev%205_vF.pdf
Manufacturing Overlay
https://cybersecurityks.osd.mil/dodcs/HelpandResources/References/Reference%20Library/U_Manufacturing_Overlay_Rev%205_vF.pdf

(WS), or Defense Critical Infrastructure (DCI) as defined by the mission owner and addresses the cybersecurity and operational risks associated with these DoW-owned systems. For example, this applies to the electrical distribution system providing power to a WS, but does not cover the WS's internal targeting or firing systems. Separate guidance will be developed for WS and DCI, though it may leverage similarities to this OT guidance. This guidance does not specifically address the OT components contained within a WS or DCI.

WHY DO WE NEED ZT FOR OT ACTIVITIES AND OUTCOMES?

Applying standard IT security approaches to OT environments can be ineffective and potentially dangerous. OT environments prioritize operational availability and are distinct from Enterprise IT in their use of legacy equipment and diverse industrial protocols, process criticality, safety standards, and custom implementations. Furthermore, OT operations require a workforce with specialized engineering expertise, differing from traditional IT security teams. The ZT for OT Activities and Outcomes address these critical differences, providing a practical and effective path to ZT implementation in these vital environments.

While the core principles of ZT – data protection, strong authentication, network segmentation, and threat monitoring – apply to OT, their implementation and deployment timescales require careful consideration of OT-specific constraints and priorities. These challenges make ZT adoption more difficult in OT environments and require modifications to the Activities and Outcomes. This is particularly true for low-level process controllers, as well as for computers, workstations, servers, and switches in an OT environment.

For example, OT environments commonly prioritize availability and safety over confidentiality and integrity. In some cases, this is governed by strict safety requirements, while in other cases, it is determined by the criticality to mission operations. As a result, ZT implementation in OT environments requires thorough risk mitigation before any product deployment, often with testing on either a simulated, testbed, or real-world scenarios. OT environments also utilize distinct industrial control protocols such as DNP3, Modbus, BACnet, and PROFINET, which vary in their native capabilities for security controls.

As a result, the IT and OT Activities and Outcomes may be accomplished with vastly different approaches. While the ZT for OT Activities have some alignment with those in the Enterprise ZT for IT guidance, the ZT for OT guidance includes unique Activities tailored to the specific challenges and requirements of OT environments. Nonetheless, the ZT for IT and ZT for OT Activities and Outcomes remain closely linked, with similar outcomes for each Activity. The commonality between the ZT for IT and ZT for OT guidance facilitates phased interoperability between the ZT for IT and ZT for OT implementations. For example, credentialing, asset management, threat detection, actor role and attribution, and behavioral analytics may be initially installed locally within the OT environment; they will eventually be integrated with the comparable Enterprise IT tools and standards to provide a common approach across a Component and the DoW at large.

Lastly, it is recommended that only persons with authority over an OT environment, in close collaboration with OT operators and security professionals, should evaluate each activity in their specific environment, considering operational constraints and risk profiles to their componentry and environment. The ZT for OT Activities and Outcomes are intended to be general enough to apply broadly to all sub-types of OT environments, as the basic principles of ZT functionality are the same. For some OT environments, system owners and operators may find that certain Activities are deemed inapplicable (e.g., a standalone system may not be able to ingest threat streams). The ZT for OT Assessor or designer should document, report the justification, and remove the ZT for OT Activity from the Target Level OT requirements of that specific system. Implementation designs may be highly diverse in OT environments, but the essential ZT principles are followed, and Outcomes of the ZT for OT guidance shall be achieved.

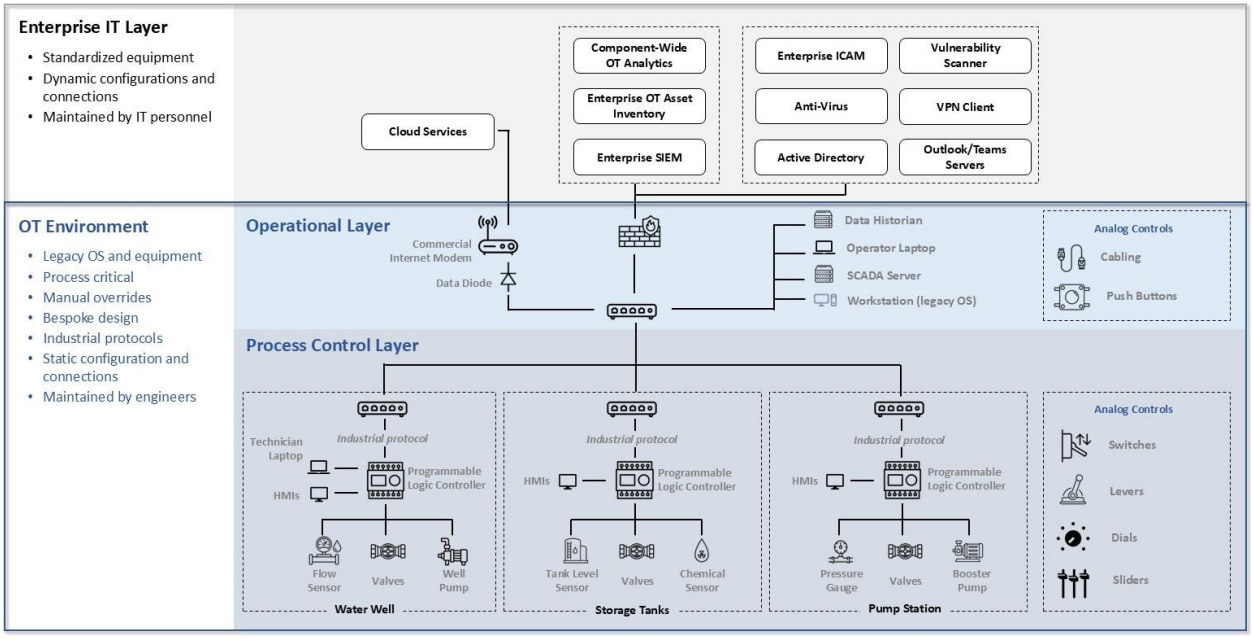
DISTINCTION BETWEEN ENTERPRISE IT AND OT ENVIRONMENTS

Established reference architectures for OT systems, such as the Purdue Model, IEC 62443, and UFC 4-010-06, serve as authoritative frameworks for classifying OT systems within the DoW. If conflicts are identified with existing

policies and instructions, it must be raised to the appropriate mission owner and/or authorizing official to bring to the DoW CIO to adjudicate and resolve. These architectures are based on a layered model, with clear boundaries between layers and specific assignments of devices to each layer. However, the ZT OT Activities and Outcomes are intended to be high-level requirements for system owners, making them more adaptable and dynamic in nature. Consequently, it is more convenient to describe OT environments using a higher-level abstraction rather than the traditional 5-layer topology. For the purposes of describing ZT principles in the OT environment, we refer to the OT environment as consisting of two layers: Operational Layer and the Process Control Layer. The Operational Layer notionally includes layers 4 and 5 of the Purdue Model, while Process Control Layer encompasses layers 0-2. This Operational Layer conceptually also includes tooling and capabilities that you would traditionally find within a Supervisory Layer (e.g., Application services, control center workstations, HMI within the OT environment) as well as an Automation layer (e.g., Controllers, Wireless Gateways within the OT environment).

This generalized description of the commonly used models provides flexibility to adapt to a wide variety of future OT environments and to accommodate alternative security reference architectures. This generalized description of the commonly used Purdue Model provides flexibility to adapt to a wide variety of future OT environments and to accommodate alternative security reference architectures. It also eliminates the need to specify how ZT solutions will be deployed to specific layers, instead allowing flexibility in implementation based on specific system configurations. This description of the OT environment does not replace the standard reference architectures. Instead, the goal is to provide a flexible and adaptable description of an OT environment when describing ZT principles and solutions.

Separating OT environments into an Operational Layer as well as a Process Control Layer gives flexibility to adapt to a wide variety of OT environments without being too prescriptive by assigning componentry, devices, and users to specific architecture levels. We believe this is a flexible and adaptable approach going forward, capturing the relevant designation for applying ZT principles. An example is provided in the figure below for a generic drinking water system.



Distinction between Enterprise IT Layer, Operational Layer, and the Process Control Layer for a generic drinking water system. [DoD CSRA 5.0](), is the authoritative DoW cybersecurity reference architectural framework. The above simplified view of control systems/OT layers illustrates the distinct differences between environments to apply appropriate security considerations.

The **Enterprise IT Layer** houses general-purpose business systems, including email servers, acquisition and asset management services, SharePoint/Teams services, Active Directory, identity credentialing services (e.g., Common

Access Card (CAC) authentication), and other services shared across the DoW Enterprise. Additionally, this contains services that facilitate analytics, threat detection, credentialing, and productivity tools. An OT environment can run without the Enterprise Layer, but the efficiency and effectiveness of its operations will often be reduced.

The **Operational Layer** contains components that can resemble Enterprise Layer components but support a vastly different mission set and are maintained through various processes. This includes components such as the Internet Protocol (IP) network with local front-end control system services, including operator workstations, network switches, process control servers, data historians, firewalls, and local control system management services (e.g., software updates, scanning, patching). For example, an Operational Layer firewall may be a similar model to an Enterprise IT Layer firewall, however, the inspected protocols and session state tracking are focused on different operations when compared. In addition, many components are based on legacy operating systems, which are configured to specific versions to support the process control environment. As a result, these components are isolated from standard Enterprise patching, scanning, and anti-virus services because changes and updates may disrupt or break the environment.

The **Process Control Layer** comprises field control devices that enable local operation of sensors, actuators, motors, and other mechanical equipment. Typically, this would contain IP-based controllers that send commands to lower-level non-IP or IP controllers, which may send serial or IP commands to sensors, valves, motors, and other mechanical devices. The layer will also include digital and analog Safety Instrumented Systems (SIS), such as fault protection systems, fuses, or pressure values. Many OT environments are isolated, with no persistent connection to any IT environments or external networks. Even so, the ZT for OT Activities and Outcomes apply equally to these environments, where insider threats, temporary device connections, data transfer media, and installed software and hardware are potential attack vectors. In some ways, isolated systems presume a false sense of security and trust in the air-gapped boundary, which makes ZT implementation necessary.

TARGET AND ADVANCED ZT ACTIVITIES

Both the Enterprise ZT for IT and ZT for OT guidance makes a distinction between Target and Advanced Level ZT Activities. In the DoW ZT Strategy document, “Target Level ZT is the minimum set of ZT capability outcomes and activities necessary to secure and protect the Department's Data, Applications, Assets, and Services (DAAS) to manage risks from currently known threats”, and “Advanced Level ZT capabilities include the complete set of identified ZT capability outcomes and activities that enable adaptive responses to cybersecurity risk and threats and offer the highest level of protection”. Target Level ZT Activities are intended to collectively provide comprehensive ZT Capabilities to prevent lateral movement in the environment. Advanced Activities are additional long-term goals that provide adaptive responses and comprehensive ZT functionality but, will not be held to the Target timeline. Advanced Activities may also require capabilities that are technically, procedurally, or policy-wise infeasible within a strict time frame. Reaching the Advanced Level does not signify the completion of ZT maturity; instead, security controls and risk mitigation strategies must continuously evolve as threat actors adapt their tactics, techniques, and procedures (TTPs) and exploit new attack vectors.

Target Level ZT Activities may require significant design, development, and testing in an OT environment, but are considered feasible and necessary to prevent adversaries from successfully attacking and moving within these environments. Implicit in the Target and Advanced Level Activity and Outcome descriptions is the assumption that implementation will maintain acceptable process control and safety performance. The activities are not OT technical implementation guidance but rather focused Outcomes that may be achieved through flexible means.

PHYSICAL SECURITY CONSIDERATIONS FOR ZT IN OT ENVIRONMENTS

The OT for ZT Activities and Outcomes framework provides a cybersecurity approach to securing adversary remote access to OT environments and control systems and focuses primarily on technical cybersecurity measures. This framework does not prescribe specific physical security controls as primary mitigation strategies, nor does it address techniques to prevent physical access, as such measures fall under the purview and expertise of Physical Security

Managers. It is critical to understand that if an adversary gains physical access, the cybersecurity controls outlined in this framework may be insufficient to prevent compromise. Components need to address physical vulnerabilities, which must be robustly addressed through appropriate physical security measures. Organizations must coordinate between cybersecurity and physical security teams to ensure comprehensive protection that addresses both remote cyber threats and physical access vulnerabilities.

OT inherently integrates digital and physical environments. OT elements – including operations centers, workstations, server rooms, controllers, human-machine interfaces (HMIs), analog actuators, and other critical components – are often distributed across numerous facilities and are accessible by both operators, and individuals outside of the OT environment's operations. In the example above, wells, tanks, and pumps could be distributed across a large geographic region and in remote locations, with physical security measures in place to protect the equipment (e.g., buildings, card access, fences).

Robust physical security measures directly enable the successful implementation of OT ZT Activities and Outcomes. For example, the mechanisms for controlling access to non-person entities (NPEs), such as HMI or remote terminal units, can rely on underlying physical controls (e.g., a locked door, perimeter fencing, surveillance). Similarly, necessitating physical actions or token safeguards can supplement authentication within the OT context. Implementers should inventory existing physical controls and consider any digital access management plans to provide a holistic ZT approach. Access control methods taken from IT, such as digital MFA, can also be used in conjunction with physical confirmation of identity to enhance session authentication further.

A layered approach is recommended to achieve the outcomes defined by the ZT for OT Activities. OT environments offer unique opportunities to leverage robust physical controls to complement digital security measures. Implementers should consider physical environment and controls as potential ways to support the application of ZT principles within OT environments. They can regard the following examples as analogous to the controls implemented in IT, but applied to the physical world:

Identity & Access Management (IAM) – Physical Analog:

- *Biometric Access Control:* Fingerprint scanners, facial recognition, or iris scanners for critical areas (analogous to MFA in IT).
- *Proximity Card Readers:* Require authorized personnel to use proximity cards to access restricted areas (this is a form of authentication).
- *Visitor Management System:* Track all visitors, verify their identity, and escort them while they are on site (similar to guest network access in IT).
- *Role-Based Physical Access:* Access levels are designed based on job function (e.g., engineers have access to control rooms, while maintenance personnel have access to equipment areas).

Network Segmentation – Physical Analog:

- *Perimeter Fencing & Barriers:* Create a physical barrier around the facility (analogous to a firewall).
- *Zoning:* Divide the facility into zones with different security levels (similar to VLANs in IT).
- *Mantrap:* A small space with two interlocking doors, used to control access to highly sensitive areas (a powerful form of micro segmentation).

Continuous Monitoring & Detection – Physical Analog:

- *CCTV Surveillance:* Monitor critical areas with cameras and record footage (analogous to SIEM logs in IT). Note that cameras should cover all access points and blind spots.
- *Intrusion Detection Systems (IDS) – Physical:* Motion sensors, door/window sensors, and glass break detectors (analogous to network IDS).
- *Environmental Monitoring:* Monitor temperature, humidity, and other environmental factors that could indicate a security breach (similar to user behavior monitoring tools)

- *Regular Security Patrols:* Conduct regular patrols of the facility to identify and address security vulnerabilities (similar to SoC threat hunting).

Data Security – Physical Analog:

- *Secure Storage:* Lock up sensitive documents and data storage devices (analogous to drive encryption).
- *Device Tracking:* Implement a system to track the location of critical assets (similar to asset management in IT).

It's essential to recognize that physical controls are not replacements for digital security measures but rather serve as complementary elements when applying ZT principles to OT. Implementors need to evaluate physical controls based on their ability to support and enhance the Outcomes defined by the ZT FOR OT Activities and Outcomes, recognizing the unique operational constraints and priorities of OT environments. Physical security guidance enables a holistic and effective ZT implementation, strengthening the resilience of critical OT environments.

ZT for OT Activities and Outcomes

OT Activity ID	OT Activity Name	Pillar	Activity Type	OT Activity Description	OT Activity Outcomes	OT Predecessor	OT Successors
1.1.1.OT	Inventory Users in OT Environment	User	Target	DoW Components establish and update a user inventory within the OT environment, manually if necessary, preparing for an automated approach in later stages. Privileged OT accounts will be identified. Both standard and privileged accounts for applications and systems with local identity stores will be identified for future migration and/or decommissioning. Shared group accounts, must-run accounts, or service OT accounts must be identified for future migration to inventory and/or decommissioning.	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.	None	None
1.2.1.OT	Implement Authorization and Access Management for OT Environments	User	Target	DoW Components implement OT or Enterprise ICAM governance, or other authorized credentialing services, in accordance with applicable policies and regulations. The authorized credentialing service establishes a set of attributes for authentication and authorization within the OT environment. Attributes are integrated with the 2.1.3.OT activity process for a complete IdP process. The OT credentialing service is enabled for adding and updating attributes for users. OT privileged access and authorization are approved and tailored as specified by the roles. For OT systems on which it is technically capable, any shared group, must-run, and service OT accounts are migrated to proper identities or are decommissioned. Any OT systems identified that cannot be migrated and/or decommisioned are tracked using a risk-based metholody for future migration and/or decommision.	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.	None	1.3.1.OT, 2.1.3.OT
1.2.2.OT	Role Based Dynamic Access for OT Environments	User	Target	DoW Components develop rules, both technical and procedural, for remote and third-party access into the OT environment. All users must have strict role-based access controls prior to access or connection into the OT environment. Remote and third-party access should be limited to the account of least privilege required to perform work. OT privileged accounts required for operations are accessed through the Authorized Credentialing Service. Identify high-privileged accounts and require these use dynamic access control.	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.	1.4.1.OT, 1.8.1.OT	4.4.1.OT
1.3.1.OT	MFA for OT Environments	User	Target	DoW Components enable or integrate the Authorized Credentialing Service with Multifactor Authentication (MFA), or an approved alternative authoritative credentialing solution, either technical or procedural, for access within the OT Environment.	1. MFA, or approved authoritative credentialing solution, is implemented with the Authorized Credentialing Service for access.	1.2.1.OT	1.3.2.OT, 1.8.1.OT
1.3.2.OT	Alternative Flexible Credentialing	User	Advanced	DoW Components shall support alternative methods of authentication that can be managed using a self-service approach. The solution will be approved and implemented following DoW Enterprise policy recommendations and guidance.	1. Authoritative Credentialing service provides user self-service alternative authentication solutions 2. DoW Component provides solutions approved per policy.	1.3.1.OT	1.3.3.OT
1.3.3.OT	Interoperate Credentialing Services	User	Advanced	DoW Component Authentication solution is extended to interoperate with DoW Approved Credentialing services.	1. DoW Component authentication solution interoperates with all approved credentialing services.	1.3.2.OT	None

OT Activity ID	OT Activity Name	Pillar	Activity Type	OT Activity Description	OT Activity Outcomes	OT Predecessor	OT Successors
1.4.1.OT	Implement PAM for OT Environments Pt. 1	User	Target	DoW Components procure and implement an OT Privileged Access Management (PAM) solution that supports all critical privileged use cases, as appropriate in the OT environment. Integration points for applications, services, and/or devices are identified to determine the status of support for the PAM solution. Applications, services, and/or devices that are able to integrate with the PAM solution are transitioned to using the solution.	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.	None	1.2.2.OT, 1.4.2.OT
1.4.2.OT	Implement PAM for OT Environments Pt. 2	User	Target	DoW Components extend integrations with the OT PAM Solution to all use cases, inclusive of all critical use cases. Applications, services, and devices that cannot integrate with the PAM solution shall be managed in a risk-based methodical approach to be migrated and/or decommissioned where operationally possible in the OT Environment.	1. OT PAM solution extended for all use cases 2. Applications, services, and devices that are not integrated with the OT PAM solution are migrated and/or decommissioned.	1.4.1.OT	None
1.5.1.OT	Life-Cycle Management for OT Environments Pt. 1	User	Target	DoW Components develop and document an Identity Life-Cycle Management (ILM) process for the OT Environment. The process is implemented for all users that access, connect, and operate with the OT Environment.	1. OT Environment Identity Life-Cycle Management process developed, documented, and implemented.	None	1.5.2.OT, 1.9.1.OT
1.5.2.OT	Life-Cycle Management for OT Environments Pt. 2	User	Advanced	DoW Components works with the DoW Enterprise to review and align the OT Environment ILM process with existing ILM processes, policies, and standards. Exceptions are identified and are managed in a risk-based methodical approach.	1. Standardized ILM processes and policies for OT environments.	1.5.1.OT	None
1.6.1.OT	Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling for OT Environments	User	Target	DoW Components procure and implement UEBA and UAM solutions that are designed specifically for OT environments for all users, PEs and NPEs, as appropriate. UEBA and UAM solutions are integrated with the Authorized Credentialing Service and configured actions prioritize safety, reliability, and resilience within the OT environment.	1. UEBA and UAM functionality is implemented for all users, PEs and NPEs, as appropriate.	None	2.3.2.OT, 7.2.6.OT, 7.3.2.OT, 7.4.1.OT
1.7.1.OT	Deny by Default Policy in OT Environments	User	Target	DoW Components conduct a comprehensive review of all user accounts and their assigned permissions, applying the principle of least privilege to revoke unnecessary access rights while maintaining the safety and reliability of OT processes. Identify and decommission static privileged accounts where possible, or reduce their permissions to the minimum required. Automate audit logging and governance processes to continuously monitor access and prepare for the implementation of more granular, attribute-based or dynamic access control mechanisms.	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.	7.2.1.OT	None
1.8.1.OT	Initial Authentication in OT Environments	User	Target	DoW Components implement authentication processes to authenticate users at the start of every session in the Operational IT environment, in the Enterprise IT environment when it interoperates with the OT environment, and in the Process Control environment via technical or procedural means, as appropriate.	1. Authentication of users is implemented across applications per session.	1.3.1.OT	1.2.2.OT, 1.8.2.OT, 3.4.1.OT, 3.4.4.OT
1.8.2.OT	Programmable Periodic Authentication in OT Environments	User	Target	DoW Components enable programmable periodic authentication requirements in the Operational IT environment, in the Enterprise IT environment when it interoperates with the OT environment, and in the Process Control environment, as appropriate on a session basis. Alternative mitigating controls, technical or procedural, must be deployed and documented when OT devices do not support periodic authentication.	1. Programmable periodic authentication of users is implemented multiple times per session 2. Alternative mitigating controls are deployed for OT devices that do not support periodic authentication.	1.8.1.OT	1.8.3.OT

OT Activity ID	OT Activity Name	Pillar	Activity Type	OT Activity Description	OT Activity Outcomes	OT Predecessor	OT Successors
1.8.3.OT	Continuous Authentication	User	Advanced	DoW Components monitor transaction-based authentications for Policy Violations. Any violations are escalated for response to the incident response process.	1. Transaction authentication monitoring detects Policy Violations and escalated for action.	1.8.2.OT	None
1.9.1.OT	Enterprise Credentialing Services Pt. 1	User	Target	The DoW Enterprise works with DoW Components to implement DoW approved Credentialing Services in a centralized and/or federated fashion in the Operational IT environment, in the Enterprise IT environment when it interoperates with the OT environment, and in the Process Control environment, as appropriate. DoW Components credentialing services interoperate with the DoW Enterprise, while also ensuring all risks involving communications between Process Control and Operational IT environments are mitigated beforehand. DoW Component local credentialing solutions are identified for future migration and decommissioning.	1. DoW Component implements approved Credentialing Services in the OT environment 2. Component Credentialing Service interoperates with DoW Enterprise approved Credentialing Authority when possible 3. Local Credentialing solutions are identified for future migration and decommissioning.	1.5.1.OT	1.9.2.OT, 2.1.3.OT
1.9.2.OT	Enterprise Credentialing Services Pt. 2	User	Target	DoW Component local credentialing solution is decommissioned and users are migrated to the DoW Approved Credentialing Authority as appropriate. All systems are assessed for compliance with this directive. Systems unable to comply due to technical or operational constraints, including Stand-Alone systems, where migration may be delayed due to inherent limitations, are subject to a documented risk assessment process to be migrated and decommissioned in the future, and compensating controls are implemented to maintain equivalent security posture. Any users that are in violation are escalated for review and remediated.	1. Local Credentialing is decommissioned and migrated to DoW Approved solution 2. Users unable to migrate are escalated and remediated.	1.9.1.OT	1.9.3.OT
1.9.3.OT	Enterprise Credentialing Services Pt. 3	User	Advanced	DoW Components shall apply authentication from DoW Approved Credentialing Authority to all OT Assets.	1. Authentication from a DoW approved Credentialing Authority has been applied to all OT Assets, enabling interoperable access across all OT componentry.	1.9.2.OT	None
2.1.1.OT	Inventory NPEs in OT Environment	Device	Target	DoW Components develop a centralized inventory for NPEs in the Operational IT and Process Control environments. Existing inventories are identified and manual and/or passive discovery-based automated solutions shall be used to update the centralized inventory. Automated inventories must be manually verified and audited periodically for accuracy as new equipment is deployed in the 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.	None	2.1.4.OT
2.1.2.OT	NPE Certificate Management for OT Environment	Device	Target	DoW Components utilize the Public Key Infrastructure (PKI) solution, or DoW approved Credentialing Authority, to deploy X.509 certificates to all supported and managed NPEs in the Operational IT environment. NPEs within the Process Control environment supporting X.509 certificates are assigned. NPEs incapable are marked for retirement or excepted using a risk based methodical approach. In addition, break-glass mechanisms are implemented to revert system to non-secure OT protocols in the event of mission critical requirement. Break-glass mechanisms must have mitigation controls in place to prevent misuse or exploitation.	1. NPEs are managed via available PKI/IdP solutions, where possible 2. DoW Components have established break-glass mechanisms to revert Process Control environment NPEs to utilize non-secure OT protocols in the event of mission critical requirements.	2.6.2.OT	2.2.1.OT, 2.4.1.OT

OT Activity ID	OT Activity Name	Pillar	Activity Type	OT Activity Description	OT Activity Outcomes	OT Predecessor	OT Successors
2.1.3.OT	NPE Credentialing Authority	Device	Target	The DoW approved Credentialing Authority, using either a centralized or federated technologies, integrates NPEs from both the Operational IT and Process Control environments. The Operational IT and Process Control IdP solution should be separate from the Enterprise IT solution. An Operational IT Device Management solution is used to track NPE integration. As appropriate, process Control NPEs shall be integrated into the PKI and/or IdP system to enable secure OT protocols (e.g., BACnet Secure Connect (BACnet/SC), DNP3 Secure).	1. NPEs from both Operational IT and Process Control environments are integrated using either centralized or federated technologies. 2. NPEs are tracked in the Operational IT environment Device Management solution, indicating whether they are integrated into the IdP and/or PKI system. 3. Process Control NPEs are integrated into the PKI and/or IdP system as appropriate to enable secure OT protocols. 4. NPEs not integrated are marked for retirement or an exception is documented with a risk-based, methodical approach.	1.2.1.OT, 1.9.1.OT	None
2.1.4.OT	Automated NPE Discovery	Device	Advanced	DoW Components automate OT network NPE discovery through the OT environment, limiting access to NPEs based on risk-based methods. OT network asset discovery shall utilize active discovery methods that are optimized to mitigate operational disturbances through configurations that avoid aggressive network scans, especially for equipment in the Process Control environment. In addition, SIEM, SOAR, and IDS solutions shall be configured to permit traffic from authorized active discovery tools to reduce false alarms.	1. NPE discovery is automated through the entire OT environment 2. Automated discovery utilizes active discovery methods, as opposed to passive discovery methods 3. The incidence of false alarms is reduced compared to Target Activities by configuring the SIEM, SOAR, and IDS solution to permit traffic from discovery tools.	2.1.1.OT	None
2.2.1.OT	Implement Connection Policy for OT Environments	Device	Target	The DoW Enterprise refines policy, standards and requirements for connection policies. Policy, standards, and requirements should specifically state how often compliance audits are conducted to ensure all NPEs meet minimum security standards. DoW Components implement and enforce compliance-based network authorization for the Operational IT environment, but only for the Process Control environment, as appropriate.	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.	2.1.2.OT, 2.3.2.OT, 2.4.2.OT, 2.5.1.OT	None
2.3.1.OT	Configuration Monitoring and Control Tools for OT Environments	Device	Target	DoW Components procure and implement configuration monitoring and control solutions for the Operational IT environment. Configuration control should ensure configuration files (e.g., ladder logic) for the Process Control environment are not altered, downloaded, or uploaded except by authorized individuals.	1. Configuration monitoring and control solutions are implemented for the Operational IT environment 2. Process Control environment configuration control solution prevents altering, downloading, or uploading unauthorized configuration files.	None	4.4.3.OT
2.3.2.OT	Integrate AV Tools for OT Environments	Device	Target	DoW Components procure and implement approved anti-virus and anti-malware solutions for supported Operational IT NPEs. NPEs without anti-virus or anti-malware solutions must be protected with mitigating controls.	1. Anti-virus and anti-malware is implemented on Operational IT NPEs 2. NPEs without anti-virus or anti-malware must be protected with other mitigating controls.	1.6.1.OT, 6.6.3.OT, 7.3.2.OT	2.2.1.OT, 2.7.1.OT

OT Activity ID	OT Activity Name	Pillar	Activity Type	OT Activity Description	OT Activity Outcomes	OT Predecessor	OT Successors
2.3.3.OT	OT Device Security Stack with C2C	Device	Advanced	DoW Components working with DoW Enterprise review current C2C policies applicability to the OT Environment. DoW Components shall prioritize applying security solutions and configurations for OT devices enabling C2C policies where possible in the OT Environment.	1. DoW Components, in collaboration with the DoW Enterprise, have reviewed current C2C policies to determine their applicability to the OT environment. 2. Based on the review, DoW Components prioritize the implementation of security solutions and configurations for OT devices that enable C2C policies, where feasible. 3. OT devices prioritized for C2C implementation have an acceptable security stack adaptation to support those policies.	None	None
2.4.1.OT	NPE Deny by Default Policy	Device	Target	DoW Components block all unauthorized remote and local NPE access to resources, including serial communications and console access, via technical or procedural controls. Identified and authorized NPEs are provided risk-based, methodical access.	1. Unauthorized remote and local NPE access and connections are blocked. 2. Physical controls are implemented to secure local NPE access.	2.1.2.OT, 7.2.1.OT	2.4.2.OT
2.4.2.OT	Managed and Limited BYOD support for OT Environments	Device	Target	Only Government Furnished Equipment (GFE) is permitted to connect to an OT Environment. GFE is provided by the system owner and any required software is scanned and approved before deployment for use in the OT environment. If non-GFE is required, and properly authorized by command authority, to connect to the OT Environment, it must follow the approved deviation process, which explicitly identifies risk tolerance levels based on situational circumstance.	1. Only GFE is permitted to connect, manage, configure, or maintain NPE in the OT environment. 2. Software deployed on GFE is scanned and approved before use in the OT environment. 3. Any non-GFE requiring connection to the OT environment must follow an approved deviation process, explicitly identifying risk tolerance levels based on situational circumstance and requiring command authorization	2.4.1.OT	2.2.1.OT, 2.4.3.OT, 2.6.1.OT
2.4.3.OT	Managed Non-OT Assets	Device	Target	DoW Components shall require non-OT assets are managed and meet standard baseline checks before authorization or connection to the OT Environment.	1. Only non-OT assets that meet mandated configuration standards allowed to access resources or connect in the OT Environment.	2.4.2.OT	None
2.5.1.OT	Implement Vulnerability and Patch Management Tools for OT Environments	Device	Target	OT Environments must maintain minimum government approved compliance standards and patching as well as be maintained to current approved configuration profiles. Any systems outside of these standards require authorization from the DoW Component through a risk based assessment approach. Periodic reassessments for compliance are performed for all devices in use. At the Process Control level, special care must be given to mitigate vulnerabilities without a patch source, while protecting safety, operational functionality, and process reliability. Similarly, risk-based testing must be performed and accepted prior to patching.	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.	None	2.2.1.OT, 2.6.1.OT, 3.2.3.OT
2.6.1.OT	Implement UEDM for OT Environments	Device	Target	DoW Components will procure and implement a UEDM solution, wherever applicable, for all identified devices. This shall include explicit configuration profiles per device.	1. UEDM solution is implemented, incorporating the requirements for configuration, vulnerability, and patch management.	2.4.2.OT, 2.5.1.OT	2.6.2.OT

OT Activity ID	OT Activity Name	Pillar	Activity Type	OT Activity Description	OT Activity Outcomes	OT Predecessor	OT Successors
2.6.2.OT	OT Device Configuration Management	Device	Target	DoW Components sets standards and policies for the device inventory and secure configuration, in conjunction with the UEDM solution and asset management tools, to enable automated configuration management control. Automated solutions for configuring devices are used only after analyzing the risk to operations.	1. Standards and policies are defined for OT device management for the Operational IT and Process Control environments. 2. Automated configuration management is enabled.	2.6.1.OT	2.1.2.OT
2.7.1.OT	Implement Endpoint Detection & Response (EDR) Tools for OT Environments	Device	Target	DoW Components procure and implement EDR solution(s) within the Operational IT, and Process Control environments as appropriate. DoW Components conduct system analysis to determine the potential automated responses within both the Operational IT and Process Control environments prioritizing safety, process reliability, and mission.	1. EDR solutions are implemented for both Operational IT and Process Control environments, following system analysis to determine and prioritize automated responses.	2.3.2.OT	2.7.2.OT
2.7.2.OT	Implement Extended Detection & Response (XDR) Tools for OT Environments	Device	Advanced	DoW Components procure and implement XDR solution(s) to all possible devices, and integration with other solutions where possible. EDR continues coverage to include the maximum number of services and applications as part of the XDR implementation. Basic analytics are sent from the XDR solution stack to the OT and/or Enterprise SIEM solution.	1. XDR solution is implemented for both Operational IT and Process Control environments 2. The maximum number of services and applications are covered by the XDR solution 3. Basic analytics from the XDR are sent to the OT and/or Enterprise SIEM.	2.7.1.OT, 7.2.2.OT	7.2.4.OT
3.1.1.OT	OT Application and Code Inventory	Applications and Workload	Target	DoW Components create an inventory of all applications. Software applications include those in use within the Operational IT environment, as well as those in use within the Enterprise IT applications when they interoperate with the Operational IT environment, including open source, commercial, and/or in-house solutions. Each Component tracks and documents the application supportability, hosted location (e.g., cloud, on-premise, hybrid), and other important data (e.g., name, version, team responsible, licensing and support, mapped dependencies).	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.	None	3.2.3.OT, 3.3.2.OT
3.1.2.OT	OT Application Control	Applications and Workload	Target	Application control solutions are applied to inventoried applications (e.g., SCADA software, control software, controller IDEs, etc.), to prevent unauthorized modifications.	1. Application control solutions are implemented on inventoried applications	3.1.1.OT	None
3.2.1.OT	Build OT DevOps Capability Factory Pt. 1	Applications and Workload	Target	The DoW Enterprise provide guidance for DevOps or DevSecOps processes, CI/CD, and Infrastructure as Code (IaC) pipelines in the Operational IT environments, and where appropriate for the Process Control applications. For DoW Components that have application development processes the guidance is applied.	1. The DoW Enterprise provides guidance for DevOps or DevSecOps processes, CI/CD, and IaC pipelines for Operational IT environments, and where appropriate for Process Control applications, to be applied by DoW Components with existing application development processes.	None	3.2.2.OT
3.2.2.OT	Build OT DevOps Capability Factory Pt. 2	Applications and Workload	Target	DoW Components that have capability development processes extend to use approved DevOps or DevSecOps processes, CI/CD, and IaC pipelines to develop new capabilities in the OT environment, as appropriate. DevOps or DevSecOps processes are also used to update existing capabilities. Continual validation functions are integrated into the CI/CD pipelines and DevSecOps processes are integrated with existing capabilities.	1. Engineering teams within the OT environment follow DevOps or DevSecOps, CI/CD, and IaC pipeline process patterns for development and deployment.	3.2.1.OT	None

OT Activity ID	OT Activity Name	Pillar	Activity Type	OT Activity Description	OT Activity Outcomes	OT Predecessor	OT Successors
3.2.3.OT	Standardized OT Application Security and XBOM Inventory	Applications and Workload	Advanced	All delivered applications and capabilities must apply approved security practices during development and ensure all security features are operable during execution. Additionally, an approved XBOM solution inventories utilized capability and application delivery.	1. All delivered applications and capabilities apply approved security practices during development 2. All security features are operable during execution 3. An approved XBOM solution inventories utilized software solutions.	2.5.1.OT, 3.1.1.OT, 3.3.2.OT	None
3.3.1.OT	OT Vulnerability Management Program Pt. 1	Applications and Workload	Target	DoW Components work with the DoW Enterprise to establish and manage an OT Vulnerability Management program. OT Vulnerability Management teams shall collaborate with a related Enterprise IT Vulnerability Management team. Vulnerability management for the OT environment shall incorporate vulnerability scope and risk to mission in prioritization decisions. Vulnerability sources can be delivered from any trusted agent, and must be consumed as an interoperable product.	1. OT Vulnerability Management program is established and managed by the DoW Component, in collaboration with the DoW Enterprise. 2. The OT Vulnerability Management program prioritizes vulnerabilities based on risk to mission and consumes vulnerability data from interoperable sources.	None	3.3.2.OT, 3.3.3.OT
3.3.2.OT	OT Vulnerability Management Program Pt. 2	Applications and Workload	Target	Standard processes are established at the DoW Enterprise level for reporting and managing the disclosure of vulnerabilities in DoW maintained or operated OT environments, for disclosure both publicly and privately. DoW Components expand the OT Vulnerability Management program to track and manage open public, controlled public, PAI and CAI, and DoW internally derived vulnerability sources.	1. Enterprise-wide processes for managing disclosure of vulnerabilities for OT environments 2. DoW Components have expanded the vulnerability management program to track and manage open public, controlled public, PAI and CAI, and DoW internally derived vulnerability sources.	3.3.1.OT	3.2.3.OT
3.3.3.OT	Binaries, Code, and Hardware Configurations for OT Environments	Applications and Workload	Target	The DoW Components manage and document approved binaries, code, and hardware configurations for the Operational IT and Process Control environments, and code reviews are conducted. Secure and reliable configuration management processes and procedures are established and adopted (e.g., to enable reverting to known-good backups). These approaches include supplier sourcing risk management, supply chain risk management, and industry standard vulnerability management.	1. Approved binaries, code, and hardware configuration developed across the OT environment are managed and documented.	3.1.1.OT, 3.3.1.OT	None
3.4.1.OT	Access Control for OT Environments Pt. 1	Applications and Workload	Target	All applications and capabilities must support a full ABAC solution. Applications, services, and devices unable to utilize ABAC are identified for future decommissioning.	1. All applications and capabilities support a full ABAC solution. 2. Applications, services, and devices unable to utilize ABAC are identified for future decommissioning.	1.8.1.OT, 5.3.1.OT	3.4.2.OT
3.4.2.OT	Access Control for OT Environments Pt. 2	Applications and Workload	Target	Access control must be enforced using digital policy with full attribution utilizing ABAC following established policies. Applications, services, and devices unable to utilize ABAC are either decommissioned or accepted using a risk-based methodical approach.	1. Policy enforcements is implemented for all possible applications, services, and devices in the Operational IT environment 2. Applications, services, and devices unable to utilize ABAC are either decommissioned or accepted using a risk-based approach.	3.4.1.OT	3.4.3.OT
3.4.3.OT	Access Control for OT Environments Pt. 3	Applications and Workload	Advanced	Confidence scoring is introduced across the attributes to create a more advanced method of authorization decision making in an automated fashion. High-Privileged OT attributes are identified for the Confidence scoring.	1. Confidence scoring is introduced and implemented to High-Privileged OT attributes.	3.4.2.OT, 5.4.2.OT	3.4.4.OT
3.4.4.OT	Access Control for OT Environments Pt. 4	Applications and Workload	Advanced	Apply confidence scoring to all DAAS, PEs, and NPEs in the OT environment.	1. Confidence scoring is applied to all DAAS, PEs, and NPEs in the OT environment.	1.8.1.OT, 3.4.3.OT	None

OT Activity ID	OT Activity Name	Pillar	Activity Type	OT Activity Description	OT Activity Outcomes	OT Predecessor	OT Successors
4.1.1.OT	OT Data Tagging Governance	Data	Target	The DoW Enterprise establishes governing body(s) for establishing controlled terminology (data and metadata), file formats, and communication protocols, which are used to ensure interoperability across communities. Data at the DoW Component level should be categorized and analyzed to align with the controlled terminology, ensuring input from appropriate Information Owners for correct alignment. DoW Components will also determine data tagging structure and maps based on workflow process, with a focus on risk of operational impact. OT environment must include a characterization method for all data.	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.	None	4.2.1.OT
4.2.1.OT	Define OT Data Tagging Patterns	Data	Target	Data tagging mandates for data within the OT environment is defined based on workflow process data types in 4.1.1.OT. The DoW Enterprise works with DoW Components to establish data tagging, labeling, and classification patterns based on industry best practices. Patterns are agreed upon, for both Operational IT data tagging and Process Control data tagging (which may be system specific), documented, and implemented in portions of the OT environment for which tagging does not interfere with critical processes.	1. Data tagging mandates for OT data are defined based on workflow process data types. 2. Data tagging, labeling, and classification patterns are established across DoW Components, instituting industry best practices and does not interfere with critical processes.	4.1.1.OT	4.3.1.OT, 4.3.2.OT, 5.1.2.OT, 6.3.1.OT
4.2.2.OT	OT Data Sharing Interoperability Patterns	Data	Target	The DoW Enterprise, collaborating with the DoW Components, develops interoperability patterns that are compliant with the established policy used for each operating mode of the OT environment. DoW Components develop methods for data sharing outside of the OT environment, considerations for secure data exchange between different Impact Levels, and including protection mechanisms for managing all OT data.	1. Interoperability patterns, compliant with established policy, are in place for data protection technologies across all operating modes of the OT environment. 2. Methods and protection mechanisms for data sharing outside of the OT environment are developed.	None	4.5.1.OT
4.2.3.OT	Document OT Storage Architecture	Data	Target	The DoW Enterprise works with DoW Components to establish storage architecture patterns and guidance, taking into consideration the data that is produced within the Operational IT and Process Control environments. DoW Components develop logical and physical architectural diagram for all storage methods. DoW Components assess their existing data storage strategies and technologies to determine the suitability for implementing storage architectures.	1. Storage architecture patterns and guidance are established by the DoW Enterprise in collaboration with the DoW Component. 2. Storage architecture considers OT-specific data requirements, both for the Operational IT environment (e.g., server configurations, network device configurations, etc.), and Process Control environment (e.g., controller logic, device configurations, PLC project files, etc.). 3. Logical and physical architectural diagrams are developed for all storage methods used by the DoW Component. 4. DoW Component assesses their existing data storage strategies and technologies to determine suitability for implementing established storage architecture patterns, including consideration of Software Defined Storage where appropriate.	None	4.7.1.OT

OT Activity ID	OT Activity Name	Pillar	Activity Type	OT Activity Description	OT Activity Outcomes	OT Predecessor	OT Successors
4.3.1.OT	Implement OT Data Tagging Tools	Data	Target	DoW Components procure and implement a data tagging solution based on the standard from activity 4.2.1.OT. A framework is established for periodic re-assessment of system risk and vulnerability. Tagging solution may leverage native capabilities of the Process Control protocols.	1. Data tagging solution is procured and implemented 2. Periodic evaluation of the system risk and vulnerabilities is performed to adjust data tagging to evolving threat landscape.E53:E55	4.2.1.OT	4.3.2.OT, 4.6.1.OT
4.3.2.OT	Data Tagging	Data	Target	DoW Components use the tagging standards developed in 4.2.1.OT to apply tags (manual or automated) using local labeling to meet minimum essential metadata criteria to enable ZT functionalities. Data tagging solution migrates over time to attribute-based pattern marking.	1. Manual and/or automated data tagging begins according to the standards established.	4.2.1.OT, 4.3.1.OT	4.5.3.OT, 4.6.2.OT
4.4.1.OT	DLP Analytics	Data	Target	DoW Components establish DLP types (e.g., Network, Endpoint, On-Premises, etc.) and recognition patterns based on data tagging solution in Activity 4.3.1.OT. A DLP analytics process is established to investigate loss type from logs, and determine severity, impact, policy enforcement, and mitigation response.	1. DLP types, recognition patterns, and analytics process 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.	1.2.2.OT	4.4.2.OT, 4.4.6.OT, 4.6.1.OT
4.4.2.OT	Establish DRM Processes	Data	Target	DoW Components establish a DRM processes, which leverage PBAC to control information use, to include information use beyond the OT environment Formal Boundary. The framework includes the development of DRM-specific use cases to better outline solution coverage.	1. DRM processes that leverage PBAC are established 2. DRM-specific use cases are developed in framework.	4.4.1.OT	4.4.6.OT
4.4.3.OT	OT File Prioritization and Monitoring	Data	Target	DoW Components identify files within the Operational IT and Process Control environments that require file monitoring and protection (e.g., controller configuration files, plant schematics, network diagrams), and establish a prioritization process for ranking severity of impact for each file type and use case. Data owners utilize File Monitoring tools to monitor, in priority order, the identified files.	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 monitoring system such as the SIEM.	2.3.1.OT, 7.2.2.OT	4.4.4.OT
4.4.4.OT	OT File Monitoring Interoperability	Data	Target	File monitoring artifacts and logs must have a standard, machine-readable formats to enable interoperability with other tools (e.g., DLP, DRM, and UEBA tools), in alignment with activity 6.6.1.OT.	1. Data and files of all regulated classifications are actively being monitored 2. A standard, machine-readable format is utilized for file monitoring artifacts and logs.	4.4.3.OT, 6.6.1.OT	None
4.4.5.OT	Inventory Databases	Data	Target	DoW Components identify, enumerate, and document databases within the OT Operational Environment.	1. Databases are identified and documented within the OT Operational Environment.	None	4.4.6.OT

OT Activity ID	OT Activity Name	Pillar	Activity Type	OT Activity Description	OT Activity Outcomes	OT Predecessor	OT Successors
4.4.6.OT	Database Activity Monitoring and Response	Data	Target	DoW Components procure, implement, and utilize Database Monitoring solutions, as appropriate, with either in-band or out-of-band solutions. Initial data monitored shall include regulated data types (e.g., CUI, PII, PHI) as appropriate for the mission environment. Logs and analytics from the database monitoring solution are fed to the SIEM. Additional data attributes are identified and used to extend the monitoring of databases as applicable.	1. Databases within the OT environment (e.g. data at rest, data exchange, transaction monitoring) is monitored. 2. Monitoring analytics is sent to SIEM. 3. Additional data attributes are identified and incorporated into database monitoring to enhance detection capabilities. 4. Along with in-band monitoring, out-of-band monitoring solutions are considered and possibly utilized.	4.4.1.OT, 4.4.2.OT, 4.4.5.OT	None
4.5.1.OT	Implement DRM and DLP Pt. 1	Data	Target	OT environment will manage DRM and DLP to the outer edge of the OT environment formal boundary as determined by the DoW Component. The consumer of the artifact(s) is expected to maintain the DRM agreement.	1. DRM and DLP are managed by OT environment to the outer edge of the OT environment formal boundary.	4.2.2.OT	4.5.2.OT, 4.5.3.OT
4.5.2.OT	Implement DRM and DLP Pt. 2	Data	Advanced	Atypical DRM behavior or occurrences are documented and reported to DoW Components or Enterprise, to perform outlier analysis and refinement of DRM rule sets. Refined rule sets utilized by DLP.	1. Outlier analysis and refinement of DRM rule sets is performed and documented against atypical DRM behavior and/or occurrences 2. DLP used with refined rule sets.	4.5.1.OT	
4.5.3.OT	DRM Response Pt. 1	Data	Target	Create data tags for response characterization, and create response process driven by newly established tags.	1. Data tags are created for DRM response characterization 2. DRM response process is driven by newly established tags.	4.3.2.OT, 4.5.1.OT	4.5.4.OT
4.5.4.OT	DRM Response Pt. 2	Data	Advanced	DoW Components implement data tags for data within databases applicable to the mission environment. Data is encrypted according to policy based on data tags.	1. Data repositories are protected using DRM. 2. Data is encrypted using data tags.	4.5.3.OT	None
4.6.1.OT	DLP Deployment	Data	Target	Newly identified attributes can be established to improve DLP outcomes. The DLP enforcement points can be controlled to the OT environment formal boundary with a combination of PBAC, DRM, and DLP, and then beyond the boundary via agreement. DLP is initially implemented with "monitor-only" and/or "learning" mode, to test outcomes with limiting impact on operations. Collaboration with cyber functions should occur with respect to any observed data loss activity.	1. DLP enforcement points are established and controlled to the OT environment formal boundary, deployed with DLP tools, and initially configured in monitor mode with standardized logging. 2. A process is established for identifying and incorporating new data attributes to improve DLP effectiveness. 3. Observed data loss activity triggers collaboration with cyber functions for investigation and response. 4. Mechanisms for extending DLP enforcement beyond the OT boundary via agreements are defined.	4.3.1.OT, 4.4.1.OT, 7.2.1.OT	5.4.3.OT, 7.2.2.OT

OT Activity ID	OT Activity Name	Pillar	Activity Type	OT Activity Description	OT Activity Outcomes	OT Predecessor	OT Successors
4.6.2.OT	DLP Operations	Data	Target	DLP solution is transitioned from testing to operations. DLP and zero trust tagging should be complimentary to achieve full access control and data loss prevention to the formal boundary. The operational model must also prescribe formalized agreements for zero trust and DLP behaviors beyond the formal boundary as determined by the DoW Component.	1. DLP solution is transitioned from testing to operations mode. 2. Tagging is integrated to achieve full access control and data loss prevention to the formal boundary. 3. Formalized agreements are established to govern zero trust and DLP behaviors beyond the formal boundary.	4.3.2.OT	None
4.7.1.OT	Manage DAAS Access with Storage Policy	Data	Target	Governance mechanisms ensure that DoW Component DAAS access policy is sufficient for Zero Trust outcomes aligned with activity 4.2.3.OT.	1. Attribute-based DAAS policy is developed with DoW Enterprise and organizational level support.	4.2.3.OT	None
5.1.1.OT	OT Granular Access Rules and Policies Pt. 1	Network	Target	The DoW Enterprise works with DoW Components to create granular access rules and policies, technical and procedural, in the Operational IT environment, and within the Enterprise IT environment when services are provided to the OT environment. Associated ConOps shall be developed to align with the access rules and policies. DoW Components will implement these access rules and policies into existing solutions to improve initial risk levels and ensure future interoperability.	1. Granular access rules and policies are established for the Operational IT environment, and for the Enterprise IT environment when applicable 2. ConOps are developed 3. Access rules and policies are implemented.	None	5.1.2.OT, 5.2.1.OT, 5.3.1.OT
5.1.2.OT	OT Granular Access Rules and Policies Pt. 2	Network	Target	Data flow patterns are defined. DoW Components apply data tagging patterns to enable granular access to the OT environment, as appropriate.	1. Data flow patterns are defined, which cover both persistent and ephemeral data. 2. Data tagging patterns are applied.	4.2.1.OT, 5.1.1.OT	5.2.2.OT, 5.3.1.OT
5.2.1.OT	Define OT Communication Pathway APIs	Network	Target	When SDN or alternate communication pathways are specified, the DoW Enterprise works with the DoW Components to identify the necessary APIs and other programmatic interfaces. Automated policy management through APIs should be tested before deployment, to minimize risk to OT operations.	1. Necessary APIs and other programmatic interfaces for specified communication pathways (including SDN) are identified and tested prior to deployment to minimize risk to OT operations.	5.1.1.OT	5.2.2.OT
5.2.2.OT	Implement OT Programmable Infrastructure	Network	Target	DoW Components implement the programmable communication pathways to enable automation tasks in the Operational IT environment, as appropriate. Segmentation Gateways and Authentication Decision Points are integrated into the SDN or alternative networking infrastructure. All components of each programmable pathway shall output their logs into a standardized repository (e.g., SIEM, Log Analytics, syslog) for monitoring and alerting.	1. Programmable communication pathways are implemented in the Operational IT environment. 2. Segmentation Gateways and Authentication Decision Points are integrated into SDN. 3. Logs are output into standardized repository.	5.1.2.OT, 5.2.1.OT, 6.6.2.OT, 7.2.1.OT	None
5.2.3.OT	Information Flow Mapping Across OT Planes	Network	Target	Develop detailed information flow map inclusive of all planes and actions (e.g., data, control, management planes). Analytics and NetFlow from the updated infrastructure is automatically fed into operations centers and analytics tools.	1. Detailed information flow map is developed. 2. Analytics are automatically fed to operations centers and analytic tools.	None	5.3.2.OT, 5.4.2.OT, 6.1.1.OT

OT Activity ID	OT Activity Name	Pillar	Activity Type	OT Activity Description	OT Activity Outcomes	OT Predecessor	OT Successors
5.3.1.OT	OT Plane Segmentation	Network	Target	DoW Components implement plane segmentation (e.g., control, data, management planes) using traditional tiered and/or service-based architectures, as it applies to connected devices and systems within the Enterprise IT, Operational IT, and Process Control environments. Proxy and/or enforcement checks are integrated with communication pathways based the access policies defined in 5.1.1.OT and 5.1.2.OT.	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.	5.1.1.OT, 5.1.2.OT	3.4.1.OT, 5.4.1.OT
5.3.2.OT	B/C/P/S Segmentation	Network	Target	DoW Components implement B/C/P/S segmentation using logical zones, limiting lateral movement across missions and geographically separated DoW Components. Proxy and/or enforcement checks are integrated with the communication pathways based on the defined access policies.	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.	5.2.3.OT	None
5.4.1.OT	Implement Micro Segmentation	Network	Target	DoW Components implement Micro segmentation communication pathways into the Operational IT and Process Control environments, enabling basic segmentation of network addresses, VLANs, devices, endpoints, services, ports, and protocols. Basic automation is accepted for IT systems for policy changes, including API decision-making. OT systems will queue and notify proposed changes for human approval. Virtual hosting environments also implement Micro segmentation at the host/container level.	1. Micro segmentation is implemented in the OT environment. 2. Automated policy changes are enabled following human approval.	5.3.1.OT	5.4.2.OT
5.4.2.OT	Application and Device Micro Segmentation	Network	Target	DoW Components apply Micro segmentation communication pathways for all information flow, including logical network zones (e.g., VLANs, IP subnets), roles, attributes and conditional-based access control for all PEs, NPEs, and endpoints, privileged access management services for network resources, and policy-based control on API access, as appropriate.	1. Micro segmentation is implemented across all information flow, utilizing role, attribute, and condition-based access controls for PEs, NPEs, and endpoints, privileged access management services for network resources, policy-based control on API access, and logical network zones.	5.2.3.OT, 5.4.1.OT	3.4.3.OT
5.4.3.OT	Protect OT Data In Transit	Network	Target	DoW Components shall use protection of data in transit per policy, and include common use cases.	1. Data is protected in transit per policy through the OT environment.	4.6.1.OT	None
6.1.1.OT	Policy Inventory and Development	Automation and Orchestration	Target	DoW Enterprise works with DoW Components to catalog and inventory existing access control policies and standards across OT system environments, including role-based access controls and policies dictating operational availability and Disaster Recovery Plans/Business Continuity Plans. Policies and standards are updated as needed.	1. Policies have been collected in reference to applicable compliance and risk 2. Policies have been reviewed and updated as needed.	5.2.3.OT	None
6.1.2.OT	Attribute-Driven Access Profiles	Automation and Orchestration	Target	DoW Components support DoW Enterprise in establishing rules, which are prioritized over local rules, as appropriate. DoW Components develop attribute-driven access profile rules for mission/task and DAAS, using appropriate cross-pillar data.	1. Enterprise rules are established. 2. Component scoped, attribute-driven profile(s) are created for mission/task and DAAS	None	6.1.3.OT, 7.4.1.OT
6.1.3.OT	Enterprise Security Profile for OT Environments Pt. 1	Automation and Orchestration	Target	DoW Components establish minimum attributes to drive security and privacy policies. DoW Components create rules to ensure security, privacy, and integrity is aligned and in compliance with Enterprise policy.	1. Minimum attributes are established to drive security and privacy policies 2. Rules are created to ensure alignment with Enterprise policy.	6.1.2.OT	6.1.4.OT

OT Activity ID	OT Activity Name	Pillar	Activity Type	OT Activity Description	OT Activity Outcomes	OT Predecessor	OT Successors
6.1.4.OT	Enterprise Security Profile for OT Environments Pt. 2	Automation and Orchestration	Advanced	DoW Components implement all security and privacy rules to ensure sufficient policy coverage.	1. All security and privacy rules are implemented to ensure sufficient policy coverage.	6.1.3.OT	None
6.2.1.OT	Process Automation Analysis	Automation and Orchestration	Target	DoW Components identify, enumerate, and document all operational processes and procedures that can be executed both manually and in an automated fashion, and identify candidates for automation.	1. Automatable operational processes and procedures are identified 2. All operational processes and procedures are enumerated.	None	None
6.2.2.OT	Tool Interoperability for OT Environments	Automation and Orchestration	Advanced	DoW Enterprise works with DoW Components to establish and prioritize baseline integration and interoperability between applicable SOAR, SIEM, and other security solutions within OT environments. Where possible, environment integration shall be done with DoW Enterprise solutions and policy services, while maintaining a human in the loop capability.	1. Baseline integration and interoperability between applicable SOAR, SIEM, and other security solutions within OT environments is established 2. Prioritization of integration efforts is completed, based on risk and operational impact. 3. Integration with DoW Enterprise solutions and policy services is prioritized and implemented where feasible.	6.5.2.OT	None
6.3.1.OT	Implement OT Data Tagging and Classification Tools	Automation and Orchestration	Advanced	DoW Components evaluate data-driven analytic approaches, such as Machine Learning solutions or equivalent capabilities, as needed to increase capability for orchestrated workflows and risk management processes. Solutions are tested with existing tagged and classified data repositories to establish baselines with a supervised approach to continually improve analysis.	1. Implemented data tagging and classification tools are integrated with analytic tools, utilizing existing tagged and classified data repositories. 2. A supervised learning approach is established to establish baselines and continually improve the accuracy and effectiveness of data-driven analysis.	4.2.1.OT	None
6.5.1.OT	OT Response Automation Analysis	Automation and Orchestration	Target	Identify and enumerate all workflow processes that are potential optimization candidates, to improve response automation using advanced analysis techniques. Manual tasks are assessed for possible automation, or partial automation that maintains a human-in-the-loop. Remaining manual processes are documented for exception and are periodically revaluated for possible automation.	1. All workflow processes are identified and enumerated. 2. Manual processes are assessed for automation. 3. Remaining manual processes are documented for exception and are periodically revaluated for possible automation.	None	None
6.5.2.OT	Implement SOAR Tools in OT Environment	Automation and Orchestration	Target	DoW Components work with DoW Enterprise to develop a standard set of requirements for OT SOAR solutions to operate in OT environments. DoW Components use approved requirements to procure and implement SOAR solutions in the OT environment, while maintaining a human in the loop capability to prevent mission impact or risk of life.	1. Develop requirements for SOAR tool 2. Procure SOAR tools.	6.6.2.OT, 6.7.1.OT, 7.2.1.OT	6.2.2.OT
6.5.3.OT	IAC within OT Environments	Automation and Orchestration	Advanced	DoW Components review existing manual and automated processes to prioritize Infrastructure as Code (IAC) development for automation within the OT Environment.	1. When possible IAC principles are applied to automate workflow capabilities 2. Manual processes are automated when possible.	None	None

OT Activity ID	OT Activity Name	Pillar	Activity Type	OT Activity Description	OT Activity Outcomes	OT Predecessor	OT Successors
6.6.1.OT	API Patterns for OT Environments Pt. 1	Automation and Orchestration	Target	The DoW Enterprise works with DoW Components to establish an API standard (or equivalent automated interchange mechanism) which outlines the approved patterns and protocols for tooling inclusive of the OT environment. The standard should prioritize ensuring the safety, reliability, and resilience of the OT Environment with the diverse OT componentry implemented.	1. API standard is established for tooling.	7.2.1.OT	4.4.4.OT, 6.6.2.OT
6.6.2.OT	Tool Compliance Analysis for OT Environments	Automation and Orchestration	Target	Automation and orchestration tooling and solutions are reviewed to identify existing APIs that they provide. These APIs are analyzed for compliance with existing API machine-readable patterns and protocols established by DoW Enterprise, or the necessary modifications are documented to achieve alignment.	1. Existing APIs within automation and orchestration tooling are assessed for compliance with established DoW Enterprise API standards. 2. Non-compliant APIs are documented with necessary modifications to achieve alignment with DoW Enterprise standards.	6.6.1.OT	5.2.2.OT, 6.5.2.OT, 6.6.3.OT
6.6.3.OT	API Patterns for OT Environments Pt. 2	Automation and Orchestration	Target	DoW Components ensure that all applications and services implement API protocols as appropriate. Enterprise and/or Operational IT environments shall prioritize interoperation with APIs. Applications and services that are unable to interoperate are scheduled for eventual retirement, and alternative equivalent capability solutions for operational gaps must be identified.	1. API calls and schemas are implemented at prioritized areas within the OT environment 2. Applications and services that cannot meet standardization are marked for eventual retirement 3. Alternative equivalent capability solutions are identified.	6.6.2.OT	2.3.2.OT, 6.6.4.OT
6.6.4.OT	API Patterns for OT Environments Pt. 3	Automation and Orchestration	Advanced	DoW Components ensure that all applications and services implement API protocols. Applications and services that were marked for retirement are decommissioned. If decommissioning presents an operational gap, an alternative must be implemented.	1. All applications and services implement the standard API calls and schemas. 2. Applications and services that cannot meet API standardization requirements are either retired or replaced with alternative solutions.	6.6.3.OT	None
6.7.1.OT	Incident Response Guidance for OT Environments Pt. 1	Automation and Orchestration	Target	DoW Enterprise works with DoW Components to establish cybersecurity incident response guidance utilizing threat feeds from 7.5.1.OT. DoW Components establish appropriate incident response processes for OT environments based on each environment's standard operating procedures.	1. Threat events are identified. 2. Incident response workflows for threat events are developed. 3. DoW Component establishes and documents OT-specific incident response processes, aligned with the Enterprise guidance and their existing standard operating procedures.	7.5.1.OT	6.5.2.OT, 6.7.2.OT
6.7.2.OT	Incident Response Guidance for OT Environments Pt. 2	Automation and Orchestration	Advanced	DoW Components identify and establish extended incident response guidance for advanced response types in alignment with 7.2.3.OT. This includes developing and incorporating incident response playbooks for any event to support OT engineers and security managers. Enrichment data sources are used for existing workflows to identify emerging, evolving, and advanced threat events.	1. Guidance for advanced threat events are developed; Advanced Threat events are identified 2. Enrichment data is utilized for advanced incident response.	6.7.1.OT, 7.2.3.OT	None
7.1.1.OT	Scale Considerations for OT Environments	Visibility and Analytics	Target	DoW Components are required to analyze current OT infrastructure and resource capabilities and capacities for adopting zero trust functionality, and project a growth curve aligned with planned mission needs. The team works with existing Continuity of Operations teams to ensure continuous mission support.	1. Future scaling needs are determined for current conditions, as well as for mission growth and emergencies.	None	None

OT Activity ID	OT Activity Name	Pillar	Activity Type	OT Activity Description	OT Activity Outcomes	OT Predecessor	OT Successors
7.1.2.OT	Log Parsing in OT Environments	Visibility and Analytics	Target	DoW Components identify and prioritize collection of all log, event, alert, and flow sources in the Operational IT and Process Control environments within the OT environment, and for data flow to the Enterprise IT and external environments. DoW Components and DoW Enterprise, with vendor support, map existing vendor log content and create a DoW Enterprise machine consumable pattern. The established DoW Enterprise pattern is provided as a contract element for vendor capability alignment.	1. Rules developed for each log format. 2. All log, event, alert, and flow sources are identified in the OT environment and are collected and mapped.	None	7.1.3.OT, 7.2.5.OT, 7.3.1.OT
7.1.3.OT	Log Analysis in OT Environments	Visibility and Analytics	Target	DoW Components work with DoW Enterprise to develop common behaviors, and identifies and prioritizes behaviors based on all relevant documented processes, including distinct operating modes. Ensure log data has sufficient attributes to analyze the behavior model.	1. Common behaviors are developed or identified, and are prioritized based on all relevant documented processes. 2. Log data has sufficient attributes to analyze behavior model.	7.1.2.OT	7.2.6.OT, 7.3.1.OT, 7.3.2.OT, 7.4.1.OT
7.2.1.OT	OT Infrastructure Incident Response Isolation	Visibility and Analytics	Target	DoW Components will ensure that the interconnections between Enterprise IT, Operational IT, and Process Control infrastructure are designed to be disconnected physically or logically during a detected incident to prevent any further intrusion or damage. The infrastructure must prevent reconnection until the incident is cleared. A controlled recovery procedure for testing and validation is used during reconnection to maintain system integrity and reduce the risk of recurring issues.	1. Enterprise IT, Operational IT, and Process Control infrastructure can be physically or logically disconnected in a safe and reliable manner, and this capability is regularly tested and validated to ensure effectiveness during incident response. 2. Controlled recovery procedure testing and validation process to maintain system integrity is used.	None	1.7.1.OT, 2.4.1.OT, 4.6.1.OT, 5.2.2.OT, 6.5.2.OT, 6.6.1.OT, 7.2.2.OT
7.2.2.OT	Threat Alerting for OT Environments Pt. 1	Visibility and Analytics	Target	DoW Components procure and implement a SIEM solution, or integrate, with an Enterprise SIEM. Data feeds are ingested, identified from the CTI program established in 7.5.1.OT, to develop rules and alerts for the OT environment.	1. SIEM solution is procured and implemented for OT environment. 2. Data feeds are ingested. 3. Rules and alerts are developed for the OT environment.	4.6.1.OT, 7.2.1.OT 7.5.1.OT	2.7.2.OT, 4.4.3.OT, 7.2.1.OT, 7.2.5.OT
7.2.3.OT	Threat Alerting for OT Environments Pt. 2	Visibility and Analytics	Target	DoW Components expand threat alerting and develop deviation anomaly rules to detect advanced threats utilizing the data feeds established in 7.2.2.OT.	1. Threat alerting is expanded by incorporating data feeds resulting in a measurable increase in the number of detected threat indicators. 2. Deviation anomaly rules are developed and implemented to detect advanced threats and reduce false positive rates.	7.2.2.OT, 7.5.1.OT	6.7.2.OT, 7.2.4.OT
7.2.4.OT	Threat Alerting for OT Environments Pt. 3	Visibility and Analytics	Advanced	Threat Alerting is expanded to include advanced data sources, such as UEBA and UAM. These advanced data sources are used to develop and improve anomalous and pattern activity detections and event triggers.	1. Identify Triggering Anomalous Events 2. Implement Triggering Policy. 3. Anomalous and pattern activity detections are developed and continuously improved using data from UEBA and UAM, resulting in a reduction in undetected threats.	2.7.2.OT, 7.2.3.OT	None

OT Activity ID	OT Activity Name	Pillar	Activity Type	OT Activity Description	OT Activity Outcomes	OT Predecessor	OT Successors
7.2.5.OT	OT Asset ID and Alert Correlation	Visibility and Analytics	Target	All PEs and NPEs in SIEM are identified and correlated to alerts in order to provide security teams with accurately detailed information and asset IDs. Event visualization indicates which asset ID is affected by detected event.	1. All PEs and NPEs within the SIEM are identified and correlated to alerts, providing security teams with accurately detailed information and asset IDs. 2. Event visualization clearly indicates the affected asset ID for each detected event. 3. Automated responses are developed based on asset ID, enabling faster and more targeted incident response.	7.1.2.OT, 7.2.2.OT	None
7.2.6.OT	OT Baselines	Visibility and Analytics	Target	DoW Components develop a subject/attribute baseline approach based off of typical patterns and behaviors from activity 7.3.2.OT.	1. Subject/attribute baseline are established.	1.6.1.OT, 7.1.3.OT, 7.3.2.OT	7.3.1.OT, 7.4.1.OT
7.3.1.OT	Implement Analytics Tools for OT Environments	Visibility and Analytics	Target	DoW Enterprise works with DoW Components to develop and provide minimum requirements for Analytics Tools capabilities to analyze all data. Any analytic tools under consideration by DoW Components for implementation shall be subject to these requirements.	1. Minimum requirements for analytic tools are developed.	7.1.2.OT, 7.1.3.OT, 7.2.6.OT	7.3.2.OT
7.3.2.OT	Establish OT Baseline Behavior	Visibility and Analytics	Target	DoW Components utilize analytics tools developed for OT environments to analyze baseline operational behavior patterns across the entire OT environment, and to identify patterns and deviations from the normal baseline.	1. Analytics tools are utilized to establish baseline behavioral patterns for OT environment, and deviations from these baselines are identified and investigated to proactively detect anomalous activity and potential threats. 2. UEBA capabilities improve the accuracy of threat detection by reducing false positives and identifying previously undetected malicious activity.	1.6.1.OT, 7.1.3.OT, 7.3.1.OT	2.3.2.OT, 7.2.6.OT
7.4.1.OT	OT Environment Baseline and Profiling	Visibility and Analytics	Target	DoW Components, utilizing the developed OT baselines, create threat profiles to assess the level of risk of deviations from normal baseline. Threat profiles should be used for prioritization of events and integrated into access profile rules developed for system triage.	1. Threat profiles are developed to assess level of risk. 2. Events are prioritized based on developed threat profiles.	1.6.1.OT, 6.1.2.OT, 7.1.3.OT, 7.2.6.OT	None
7.5.1.OT	OT Cyber Threat Intelligence Program Pt. 1	Visibility and Analytics	Target	The DoW Enterprise works with DoW Components to develop an OT CTI program. The CTI program identifies and integrates common data feeds with an OT SIEM solution for improved alerting and response. Integrations with enforcement points are created to monitor CTI-driven data alerting and response for the Enterprise IT, Operational IT, and the Process Control environments.	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.	None	6.7.1.OT, 7.2.1.OT, 7.2.2.OT, 7.5.2.OT
7.5.2.OT	OT Cyber Threat Intelligence Program Pt. 2	Visibility and Analytics	Advanced	DoW Components expand their CTI program to develop a community of interest that includes identified stakeholders. Authenticated, private, and controlled CTI data feeds are integrated into the OT SIEM solution and utilized by the appropriate PEPs.	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.	7.5.1.OT	None

APPENDIX A: Acronyms and Definition Sources

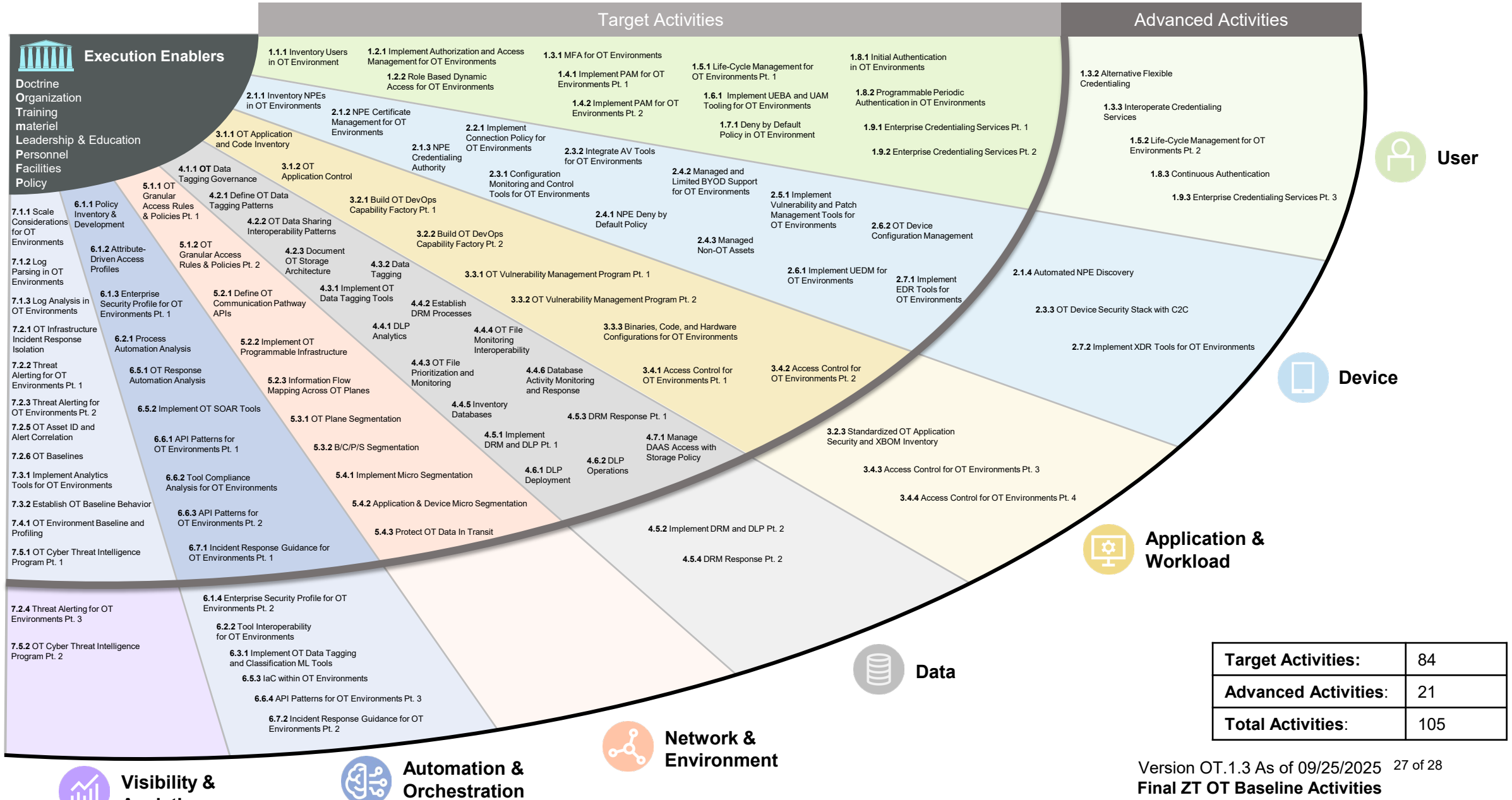
Acronyms	Glossary		
Abbreviation	**Term**	**Definition**	**Source**
ACI	Advanced Cyber Industrial Control Systems	A term from the paper "Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of War (DoW) Industrial Control Systems (ICS)". Generally mentioned as "ACI TTP" to describe Tactics, Techniques, and Procedures used by advanced malware suites that threaten ICS systems.	ACI TTP for DoW ICS
ABAC	Attributed-Based Access Control	An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions.	CNSSI 4009
B/C/P/S	Base, camp, post, and station	Any type of military installation, camp, post, or station that is geographically defined within a fence line.	10 USC § 2801(c)(4) (adapted)
BYOD	Bring Your Own Device	Personal or non-government devices used for work-related activities.	NIST SP 800-207
CI/CD	Continuous Integration Continuous Delivery	Continuous integration (CI) refers to the practice of automatically and frequently integrating code changes into a shared source code repository (e.g., committing and pushing code to a branch via Git). Continuous delivery/deployment (CD) is the process of building, testing, and publishing those changes to a runtime environment (e.g., an Azure DevOps pipeline that takes recently merged code, compiles it into a build artifact, then uploads it to a production environment).	NIST SP 800-215
CMMC	Cybersecurity Maturity Model Certification	Department of War program aimed at ensuring defense contractors and subcontractors are properly securing sensitive information.	32 CFR Part 170
ConOps	Concept of Operations	Verbal and graphic statement of an organization's assumptions or intent in regard to an operation or series of operations of a specific system or a related set of specific new, existing, or modified systems.	CNSSI 4009
CTI	Cyber Threat Intelligence	Collecting, analyzing, and disseminating information about cyber threats to help organizations prepare for, prevent, and respond to cyberattacks.	NIST SP 800-160 Vol. 2 Rev. 1
CUI	Controlled Unclassified Information	Sensitive information that does not meet the criteria for classification but must still be protected.	Executive Order 13556; DoDI 5200.48
DAAS	Data, applications, assets and services	(Not to be confused with DoW Defense Automatic Addressing System or Desktop as a Service). DAAS is a Zero Trust term that refers to all resources that are critical to an organization. DAAS are generally accessible by users, devices, etc. Data is usually sensitive and is thus placed into classification levels (e.g., CUI, PII, etc.). Assets are devices or systems (e.g., IT systems, SCADA systems, IoT devices) that may be critical to the organization's mission. Applications are software that utilize data and/or control assets. Services refer to the protocols used to communicate between DAAS (e.g., Active Directory, HTTP, DNS).	DoW ZTRA 2.0
DevSecOps	Development Security Operations	A process capability that improves the lead time and frequency of delivery outcomes through enhanced engineering practices; promoting a more cohesive collaboration between Development, Security, and Operations teams as they work towards continuous integration and delivery.	NIST SP 800-215
DLP	Data Loss Prevention	A systems ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of NSS information.	NIST SP 800-82 Rev. 3; NIST SP 800-215
DODIN	DoD Information Network	Set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policymakers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.	CNSSI 4009
DRM	Digital Rights Management	Technology used to control and manage access to digital content, protecting it from unauthorized use, modification, and distribution.	DoW ZTRA 2.0
EDR	Endpoint Detection and Response	Technology that monitors and responds to threats on endpoint devices in real-time.	[adapated industry term]
FCI	Federal Contract Information	Non-public data, not intended for public release, that is provided or generated for the U.S. government under a contract to deliver goods or services.	48 CFR § 52.204-21
FIM	File Integrity Monitoring	Security process and technology that tests and checks operating system (OS), database, and application software files to determine whether have been tampered with or corrupted.	NIST SP 800-115 (adapted)
FRCS	Facility Related Control Systems	Systems that monitor and control equipment and systems in Department of War facilities. These systems include (non-exhaustive): Building control systems, Utility control systems, Electronic security systems, Fire and life safety systems, and HVAC systems.	UFC 4-010-06
IAC	Infrastructure as Code	The process of managing and provisioning an organization's IT infrastructure using machine-readable configuration files, rather than employing physical hardware configuration or interactive configuration tools.	NIST SP 800-172
IDE	Indegrated Development Environment	Software for building applications that combines common developer tools into a single graphical user interface.	[common industry term]
ICAM	Identity, Credential, and Access Management	The set of security disciplines that allows an organization to enable the right entity to access the right resource at the right time for the right reason. It is the tools, policies, and systems that allow an organization to manage, monitor, and secure access to protected resources. These resources may be electronic files, computer systems, or physical resources such as server rooms and buildings.	CNSSI 4009
ICS	Industrial Control System	A collection of devices, controllers, software, etc. used to monitor industrial processes. SCADA could be arguably described as a type of ICS.	CNSSI 4009; NIST SP 800-82 Rev. 3
IdAM	Identity and Access Management	A security framework that enforces access control to users and/or devices in order to ensure that they have appropriate access to resources.	NIST SP 800-203

IdP	Identity Provider	A service which provides state/status determination and access to Identity and Credential information. It may also provide baseline user/NPE access roles.	CNSSI 4009; NIST SP 800-63-3; FIPS 201-3
IoT	Internet of Things	Generally refers to networked embedded devices that serve one specific purpose (e.g., smart thermostats, IP cameras).	NIST SP 800-215
IR	Incident Response	The remediation or mitigation of violations of security policies and recommended practices.	CNSSI 4009
MFA	Multifactor Authentication	An authentication system or an authenticator that requires more than one authentication factor for successful authentication. Multi-factor authentication can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors.	CNSSI 4009
ML	Machine Learning	A subfield of artificial intelligence that focuses on enabling computer systems to learn from data without explicit programming.	NIST SP 800-55v1
NPE	Non-Person Entity	An entity with a digital identity that acts in cyberspace but is not a human actor. This can include an autonomous service or application, hardware devices (e.g. smart sensors), proxies, and software applications (e.g. automated bots for repetitive tasks).	CNSSI 4009
OT SDN	Operational Technology Software Defined Network	A specific implementation of SDN that is deployed on an operational technology.	[adapted industry term]
PAM	Privileged Access Management	A class of solutions that help secure, control, manage and monitor privileged access to critical assets. (Example: PAM for administrator/sudo privileges could mean that a user has to re-enter their credentials before performing a privileged action (i.e., installing software), then that action would be logged).	[adapted industry term]; ISO/IEC 27002:2022 (adapted)
PBAC	Policy-Based Access Control	A form of access control that uses an authorization policy that is flexible in the types of evaluated parameters (e.g., identity, role, clearance, operational need, risk, heuristics).	CNSSI 4009
PE	Person Entity	The role a human actor (i.e. User) performs when accessing IT assets with a specific identify.	CNSSI 4009
PKI	Public Key Infrastructure	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Framework established to issue, maintain, and revoke public key certificates.	CNSSI 4009
PLC	Programmable Logic Controller	A configurable device (generally an embedded device) that acts as the physical interface between the site and ICS/SCADA systems. (Example: a PLC can be programmed to take readings from a temperature sensor, convert those values to a certain unit, and then send those values over to a SCADA server.)	CNSSI 4009
SBOM	Software Bill of Materials	A formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product.	NIST SP 800-218
SCADA	Supervisory Control and Data Acquisition	A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated.	CNSSI 4009; NIST SP 800-82 Rev. 3
SDC	Software Defined Compute	A framework to manage, provision, and deploy computational resources (e.g., a rack of servers in a data center) via centralized code and/or configuration, rather than having to configure each resource manually. Software Defined Compute is another way to describe the industry standard term, Infrastructure-as-Code (IoC).	[adapted industry term]
SDN	Software Defined Network	An approach to manage the control plane of network devices (e.g., firewalls, managed switches, routers, etc.) via a centralized configuration rather than having to configure each device manually. The SDN may expose an API to allow other entities (network devices, scripts, etc.) to read/configure it automatically.	NIST SP 800-207
SDP	Software Defined Perimeter	A firewalling approach defined by the Cloud Security Alliance for protecting a network. It focuses on enforcing access control for both discoverability and accessibility to any given resource (e.g., requiring an authorized identity before a user can ping a device on a network). This serves as an alternative to the traditional "fixed/static perimeter" model (i.e., firewall rules) which may solve the problem of isolating internal devices, but may not be able to granularly enforce identify-based access control per endpoint/device.	NIST SP 800-207; NIST SP 800-215
SDS	Software Defined Storage	Storage architecture that decouples storage software from its underlying hardware, enabling flexible and dynamic management of storage resources.	NIST SP 800-209
SIEM	Security Information and Event Management; Security Incident and Event Management	The SIEM aggregates security and event data from across the environment.	NIST SP 800-92; NIST SP 800-128; NIST SP 800-209
SOAR	Security Orchestration Automated Response	A security strategy that has evolved in recent years to automate the incident response process.	NIST SP 800-215
TTP	Tactics, Techniques, and Procedures	A term borrowed from US Army but used in cybersecurity to describe adversarial behavior of cyberthreat actors, in three increasing levels of detail: 1) Tactics are a general description of the threat behavior, 2) Techniques are a slightly more detailed description of a tactic, and 3) Procedures are a highly detailed, step-by-step description of a technique.	CNSSI 4009
UAM	User Activity Monitoring	The technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing U.S. Government information in order to detect insider threat and to support authorized investigations.	CNSSI 4009
UEBA	User and Entity Behavior Analytics	cybersecurity approach that uses advanced analytics to monitor and detect anomalies in the behavior of users and other entities within an organization's network.	NIST SP 800-215
UEDM	Unified Endpoint and Device Management	Integrated approach to managing and securing various endpoints like desktops, laptops, smartphones, tablets, and IoT devices from a single console utilizing deployable agents or using agentless native OS management control features.	NIST SP 800-215 (adapted)

XDR	Extended Detection and Response	Solution that extends the capabilities of Endpoint Detection and Response (EDR) to encompass a wider range of security layers beyond just endpoints.	[adapted industry term]
	Actor, NPE Actor, PE Actor	All-encompassing term to refer to any person entity, non-person entity, user, group, device, resource, or asset that acts upon the system.	CNSSI 4009 (adapted)
	Confidence Scoring	A method used in cybersecurity to assess the reliability or probability that a detected alert, event, or indicator represents a genuine threat. It's a numerical value assigned to signify how certain a system is that something malicious is occurring.	This document
	Control Plane	Layer of the network architecture responsible for controlling traffic sent to a network device, and managing network routing protocols (e.g., STP, BGP, ICMP).	NIST SP 800-207
	Data Plane	Layer of the network architecture responsible for handling traffic sent through a network device, and for forwarding data packets between devices in the network.	NIST SP 800-207
	Information Owner	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, classification, collection, processing, dissemination, and disposal.	NIST SP 800-37 Rev. 2
	Formal Boundary - also known as Authorization Boundary	All components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected.	CNSSI 4009; NIST SP 800-137
	Impact Level	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.	NIST SP 800-30 Rev. 1
	Management Plane	Layer of the network architecture responsible for managing traffic to the network device that is intended to configure, manage, or monitor the network device (e.g., SSH, SNMP, HTTP).	NIST SP 800-128 (adapted)
	Non-response task	A "non-response task" in automation refers to a situation where an automated process encounters an unexpected issue or lack of response from a system it is trying to interact with, forcing it to pause or stop execution until manual intervention is required to resolve the problem and continue the automation process.	This document
	Non-OT device	For the purposes of this document, non-OT devices can be understood as operational IT infrastructure requiring temporary access to ZT compliant Process Control or Operational IT environments. In the context of 2.4.3.OT Managed Non-OT Assets, it refers to non-GFE BYOD equipment deemed absolutely necessary to perform a task.	This document
	Operational IT Environment	Operational IT environment consists of an Internet Protocol (IP) network with local front-end control system services, including operator workstations, network switches, process control servers, data historians, firewalls, and local control system management services. Generally Levels 4/5 of the Purdue model.	This document
	Process Control Environment	Contains the field control devices that provide local command and control of sensors, actuators, motors, and other mechanical equipment. Generally refers to levels 0-3 of the Purdue model.	NIST SP 800-82 Rev. 3 (adapted)
	Response task	A "response task" in automation refers to a specific action or set of actions that are automatically triggered by a predefined event or condition, designed to initiate a response to that event, often within a larger automated workflow, like in incident response systems where a response task might involve isolating a compromised system upon detecting a security threat.	This document
	DoW Approved Credentialing Authority	An entity formally authorized to issue credentials that enable secure access to DoW information systems and resources.	This document

Definition Sources		
Reference	**Title**	**Description**
32 CFR Part 170	Cybersecurity Maturity Model Certification (CMMC) Program	CFR - National Defense - Cybersecurity Maturity Model Certification (CMMC) Program.
48 CFR § 52.204-21	Basic Safeguarding of Covered Contractor Information Systems	CFR - Federal Aquisition Regulations System - Basic Safeguarding of Covered Contractor Information Systems.
ACI TTP for DoW ICS	Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of War (DOW) Industrial Control Systems (ICS)	Abstract: "This ACI TTP is designed to enable managers of ICS networks to Detect, Mitigate, and Recover from nation-state-level cyber attacks (strategic, deliberate, well-trained, and funded attacks to support greater strategic objectives)."
CNSSI 4009	Committee on National Security Systems (CNSS) Glossary	Abstract: "...Contains definitions of terms used by the Department of War (DoW), Intelligence Community (IC), and Civil Agencies (e.g., National Institute of Standards and Technology (NIST))."
DoDI 5200.48	DoD Instruction 5200.48 - Controlled Unclassified Information	Abstract: "Establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DoW..."
DoW ZTRA 2.0	Department of War (DoW) Zero Trust Reference Architecture	Abstract: "The Reference Architecture (RA) establishes a framework that provides guidance via architectural Pillars and Principles."
Executive Order 13556	Controlled Unclassified Information	Abstract: "This order establishes an open and uniform program for managing information that requires safeguarding or dissemination controls."
FIPS 201-3	Personal Identity Verification (PIV) of Federal Employees and Contractors	Abstract: "This document establishes a standard for a Personal Identity Verification (PIV) system that meets the control and security objectives of Homeland Security Presidential Directive-12."
IEC 62443		Series of standards that address cybersecurity of OT control systems.
NIST SP 800-218	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	Abstract: "This document recommends the Secure Software Development Framework (SSDF) – a core set of high-level secure software development practices that can be integrated into each software development life cycle (SDLC) implementation."
NIST SP 800-215	Guide to a Secure Enterprise Network Landscape	Abstract: "This document is meant to provide guidance to this new enterprise network landscape from a secure operations perspective."
NIST SP 800-209	Security Guidelines for Storage Infrastructure	Abstract: "This document provides an overview of the evolution of the storage technology landscape, current security threats, and the resultant risks."
NIST SP 800-207	Zero Trust Architecture	Abstract: "This document contains an abstract definition of zero trust architecture (ZTA) and gives general deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture."
NIST SP 800-203	2017 NIST/ITL Cybersecurity Program Annual Report	Abstract: "This annual report highlights the research agenda and activities in which ITL Cybersecurity Program was engaged during FY 2017."
NIST SP 800-160 Vol. 2 Rev. 1	Developing Cyber-Resilient Systems: A Systems Security Engineering Approach	Abstract: "NIST Special Publication (SP) 800-160, Volume 2, focuses on cyber resiliency engineering—an emerging specialty systems engineering discipline applied in conjunction with systems security engineering and resilience engineering to develop survivable, trustworthy secure systems."
NIST SP 800-128	Guide for Security-Focused Configuration Management of Information Systems	Abstract: "The focus of this document is on implementation of the information system security aspects of configuration management, and as such the term security-focused configuration management (SecCM) is used to emphasize the concentration on information security."
NIST SP 800-115	Technical Guide to Information Security Testing and Assessment	Abstract: "The guide provides practical recommendations for designing, implementing, and maintaining technical information security test and examination processes and procedures."
NIST SP 800-92	Guide to Computer Security Log Management	Abstract: "This publication seeks to assist organizations in understanding the need for sound computer security log management."
NIST SP 800-82 Rev. 3	Guide to Operational Technology (OT) Security	Abstract: "The document provides an overview of OT and typical system topologies, identifies common threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks."
NIST SP 800-63-3	Digital Identity Guidelines	Abstract: "The guidelines cover identity proofing and authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks."
UFC 4-010-06	Unified Facilities Criteria - Cybersecurity of Facility-Related Control Systems	Abstract: "UFC 4-010-06 provides requirements for incorporating cybersecurity into the design of facility-related control systems."

APPENDIX B: Zero Trust Fan Chart for Operational Technologies



Target Activities:	84
Advanced Activities:	21
Total Activities:	105

APPENDIX C: Distinction Between Enterprise IT and OT Environments