Pacific Northwest
NATIONAL LABORATORY

PNNL-35697

Zero Trust Cybersecurity

Concepts and Models for Application

February 2024

Joel Doehle
Ian Johnson
Pierce Russell
Clifton Eyre
Mark Watson
Penny McKenzie

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

PNNL-35697

Zero Trust Cybersecurity

Concepts and Models for Application

February 2024

Joel Doehle
Ian Johnson
Pierce Russell
Clifton Eyre
Mark Watson
Penny McKenzie

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Acronyms and Abbreviations

CBRN	Chemical, biological, radiological, nuclear
CISA	Cybersecurity and Infrastructure Security Agency
CWMD	Countering Weapons of Mass Destruction Office
DAAS	Data, applications, assets, and services
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DoD	Department of Defense
EO	Executive Order
IT	Information Technology
IoT	Internet of Things
MFA	Multi-factor Authentication
NIST	National Institute of Standards and Technology
NPE	Non-Person Entities
NSA	National Security Agency
OT	Operational Technology
PAM	Privileged Access Management
PNNL	Pacific Northwest National Laboratory
ZT	Zero Trust
ZTA	Zero Trust Architecture

Table of Contents

1.0 Introduction

Zero Trust (ZT) is a cybersecurity paradigm centered on the idea that a network breach is inevitable and so no user or asset should be implicitly trusted. Entities on the network are continuously monitored and access-granting decisions are based on dynamic risk assessment using multiple inputs. To limit the damage from an attack, privileges and lateral access are constrained by default. ZT shifts from a historical concept of trusting entities within a robust network perimeter to one in which nothing is trusted, and sensitive resources are protected from exploitation through continuous access verification.

Originally conceived by John Kindervag in 2008, ZT has become a widely accepted concept for implementing effective cybersecurity.[10] In the federal government, the value of this concept has been recognized as well, with multiple departments and agencies articulating strategies and frameworks for shifting to a ZT cybersecurity paradigm within their organization. Executive Order 14028 formally established ZT as a fundamental element of the federal government's cybersecurity strategy and directed agencies across the government to implement a plan to adopt a Zero Trust Architecture (ZTA).[5]

To support a transition to ZT, the Department of Homeland Security (DHS) Countering Weapons of Mass Destruction Office (CWMD) partnered with Pacific Northwest National Laboratory (PNNL) to conduct a landscape survey of ZT best practices and to provide recommendations regarding how to implement a ZTA for CWMD's chemical, biological, radiological, and nuclear (CBRN) detection devices, systems, and networks. This report provides a synthesis of the concepts and models for transitioning to ZT. Successive reports will apply these models to CWMD use cases.

2.0 The Zero Trust Paradigm

The growing complexity and geographic dispersion of enterprise network elements has driven a re-evaluation of historical cybersecurity models, which focused on establishing and defending a strong perimeter and trusting the devices and users inside it. Coupled with a continued expansion of the volume and capability of malicious actors, these cybersecurity models have proven insufficient for protecting an organization's data and assets. As a result, government, industry, and academia have shifted to pursuing a model in which no entities on a network are implicitly trusted and location within the network does not provide a guarantee of resource access. This revised concept of security architecting, formalized by John Kindervag in 2008, is referred to as "zero trust." It encapsulates a growing set of principles and strategies that reduce risk of malicious action on a network through minimization of privileges and per-transaction assessment of access requests. When realized in a network via technical and policy controls, the implementation of these principles is referred to as a zero trust architecture.

Zero Trust fundamentally depends on the identification of the sensitive resources within an enterprise that require protecting. This identification is driven by the organization's mission. Paired with an understanding of the dynamic threat environment, appropriate controls are put in place to reduce the risk from access and lateral movement to an acceptable level. Kindervag delineates these resources as data, applications, assets, and services (DAAS) elements.[12] Data is managed by applications and data sensitivity varies based on organizational mission. Services, such as DNS, DHCP, and Directory Services, support the enterprise. These are critical elements and can be fragile. The physical components – e.g., IT, SCADA, and IoT systems – make up the assets on which the environment operates. Each identified element is encapsulated by a "protect surface", which forms the construct around which security controls are built to ensure zero trust access to the sensitive element.

In designing a ZTA to protect DAAS elements, Kindervag articulates four principles for guidance:[12]

- Define business outcomes
    - Articulate the goals of the business and make ZT cybersecurity an enabler
- Design from the inside out
    - Design outward from the DAAS element in the protect surface
- Determine who or what needs access
    - Minimize access using the principle of least privilege
- Inspect and log all traffic
    - Look for malicious content and unauthorized activity

This yields a ZT construct in which business outcomes (organization-specific mission) drive the security design. These drivers define the identification of DAAS that need protecting as well as the acceptable security controls to align with stakeholder risk tolerance while still accomplishing mission objectives. Security design starts at the DAAS element rather than the network perimeter. Access to each element is minimized to only those entities that need it.

Which subjects (persons and non-person entities) need access to specific resources should be determined at the most granular level possible.[6] Policies should articulate “who,” “what,” “when,” “where,” and “why.”[10,12]

- Who (which subject) should be permitted to access the resource?
- What resource is the subject allowed to access?
- When (what time of day) can the subject access the resource?
- From where can the subject access the resource?
- Why can the subject access the resource?
    - What justifies granting the subject this privilege?
- How is the subject able to access the resource?
    - What additional controls must be satisfied to grant access? E.g., review of machine compliance state, satisfying intrusion detection/prevention check.

These access specifications are formalized into policies and these policies can be incorporated into technical controls as the ZTA is built out.

In ZT, access policies and controls are dynamic, informed by the current threat landscape and based on the context of every transaction requesting the grant. As possible, authentication and authorization determinations should employ “multiple attributes (dynamic and static) to derive confidence levels” to make the decision.[7] This includes factors such as the configuration and compliance state of the device requesting access and past and recent behavioral indicators of the subject. To support this, ubiquitous logging and analysis are key elements of ZT. Centralizing logging, monitoring, and analysis, along with services such as identity and credential management is important in order to provide consistent adjudication of requests across the enterprise informed by the most up-to-date context.

The National Institute of Standards and Technology (NIST) summarizes these concepts in seven tenets of ZT.[6]

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy – including the observable state of client identity, application/service, and the requesting asset – and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.

6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

NIST includes ubiquitous security of communications, a concept common across government guidance documents. This is based on the assumption that any device or entity on the network could be compromised. As a result, communications should be protected against observation or manipulation by any malicious actor that may be in the pathway between the sender and intended recipient.

Implementing a robust ZTA takes time. Many architectures and guidance documents refer to it as a "journey."[1,3,6] Progressing requires a detailed inventory and assessment of elements that need protecting and an intentional design that enables the workflows of an organization while securing them effectively. The following sections enumerate models that assist in translating these high-level concepts into concrete actions to transition to a mature ZT footing.

3.0 Pillars of Zero Trust

One of the models used to support implementation of ZT is that of pillars. Pillars organize the aspects of a computing enterprise into focus areas in which ZT controls can be built out. Each of these pillars is also interdependent, enabling a holistic ZTA. The Cybersecurity and Infrastructure Security Agency (CISA) defines a five-pillar model as seen in Figure 1.

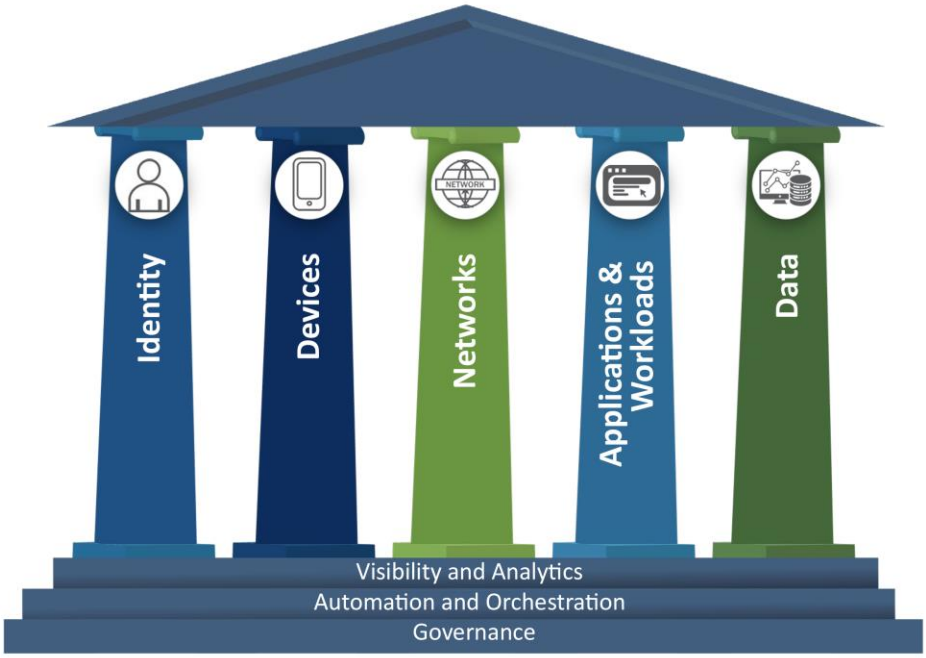

Figure 1: CISA Zero Trust Pillars[1]

The pillars include Identity, Devices, Networks, Applications and Workloads, and Data. Integrating these five pillars are the crosscutting capabilities of Visibility and Analytics, Automation and Orchestration, and Governance. These capabilities support the interoperability of the functions across the pillars.

Department of Defense (DoD) defines a seven-pillar model, shown in Figure 2.

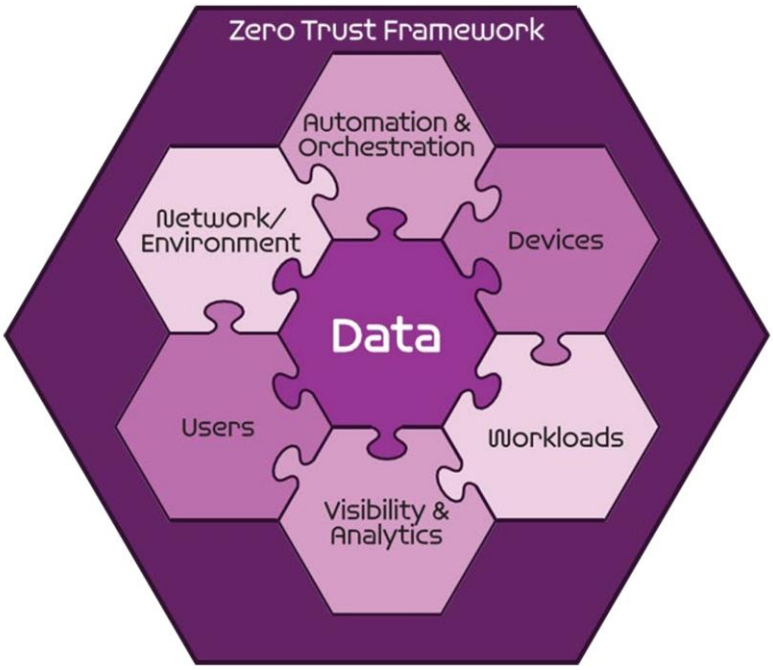

Figure 2: DoD Zero Trust Pillars[3]

The DoD model incorporates Visibility and Analytics along with Automation and Orchestration as pillars rather than cross-cutting capabilities. Data also serves a central role as the main element being protected. Governance is not explicitly called out in the model itself but is a ubiquitous element that DoD notes as “required to achieve proper integration across Pillars.”[3]

Despite these differences, the models convey consistent ideas in guiding construction of an effective ZTA. These concepts are discussed below. For simplicity, only the CISA terminology is employed.

Identity

This pillar focuses on securing the identities and credentials of users and systems and ensuring they only have access to the right resources at the right time. An up-to-date inventory of users and non-person entities is critical for enabling this pillar. Key elements of the pillar include multi-factor authentication (MFA), enterprise-wide integrated identity management, continuous identify verification, least privilege permissions, privileged access management (PAM), and dynamic, context-based authorization.

Devices

This pillar focuses on the security of end systems, whether being accessed as a resource or used to access other resources. Some key elements include endpoint protection through antivirus, data loss prevention (DLP), and intrusion detection/protection systems. Patch management with timely updates is fundamental along with an up-to-date device inventory and configuration compliance/device posture checking.

Networks

This pillar focuses on reducing risk of access and lateral movement through network configuration. Micro-segmentation is key to isolate hosts and workloads. Other elements include software-defined networking and firewalls as well as ubiquitous traffic encryption.

Applications and Workloads

This pillar focuses on security of software and processes, whether operating autonomously or by a user. Key practices include secure software development coupled with application security testing, containerization and workload isolation, DLP, encryption of data, robust access and authorization controls, and least privilege policies.

Data

This pillar focuses on security of data in storage, use, and transmission. Key elements include encryption and up-to-date inventory, categorization (for sensitivity and criticality), and labeling of data. Implementation of DLP through detection and blocking of unauthorized or malicious data transfer is also important.

Visibility and Analytics

Mature implementation of ZT is not possible without effective visibility and analytics. Up-to-date situational awareness through log analysis and behavioral analytics enables dynamic, context-based security decisions to be executed. This can include informed access authorization as well as detection and blocking of unauthorized data movement. Centralized aggregation and analysis of logs is key.

Automation and Orchestration

Automation and orchestration enable actions to be taken efficiently and timely. Patching, log collection, and incident response actions being addressed at machine speed is a key enabler of ZT.

Governance

Governance enables tailored policies and controls across the varied workflows of the enterprise. It provides for consistent, continuous enforcement and dynamic updates. Governance ensures the correct people, processes, and technologies are in place to enable ZT.

4.0 Zero Trust Maturity Models

Moving from traditional paradigms of cybersecurity to ZT is a process. Transitioning to a robust ZTA takes time and requires intentional consideration of organization-required workflows and appropriate security controls. Concepts such as continuous context-based user verification and ubiquitous log analysis can be straightforward to describe but challenging to practically implement. As such, it can be useful to view this transition as a movement toward increasing levels of ZT maturity. It won't be accomplished overnight, and it isn't just a swap out of existing technologies. However, it is an achievable goal that becomes manageable when pursued in incremental steps.

This is the philosophy articulated by CISA and DoD in their zero trust maturity models.[1,3,7] These models provide practical guidance for progressing through three phases of increasing ZT maturity. Using the pillars described in the previous section, CISA and DoD (as enumerated by NSA) articulate what it would look like for an organization to be at each level of maturity within each pillar.[1,8,9] These models provide specific examples of controls and the corresponding level of sophistication, integration, and automation of each that should be achieved for each maturity level.

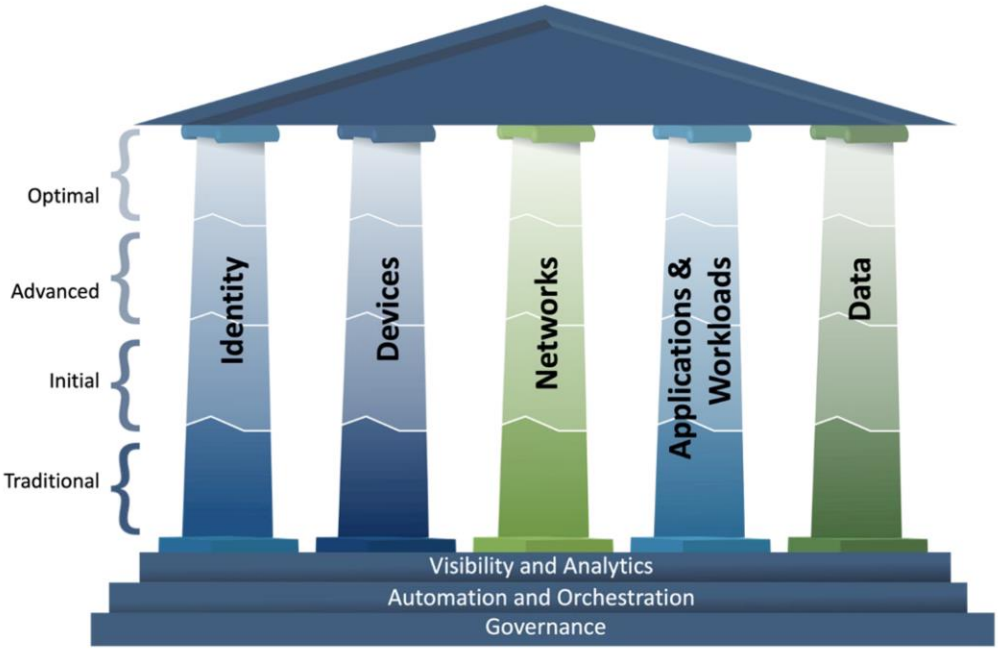

Figure 3: CISA Zero Trust Maturity Model[1]

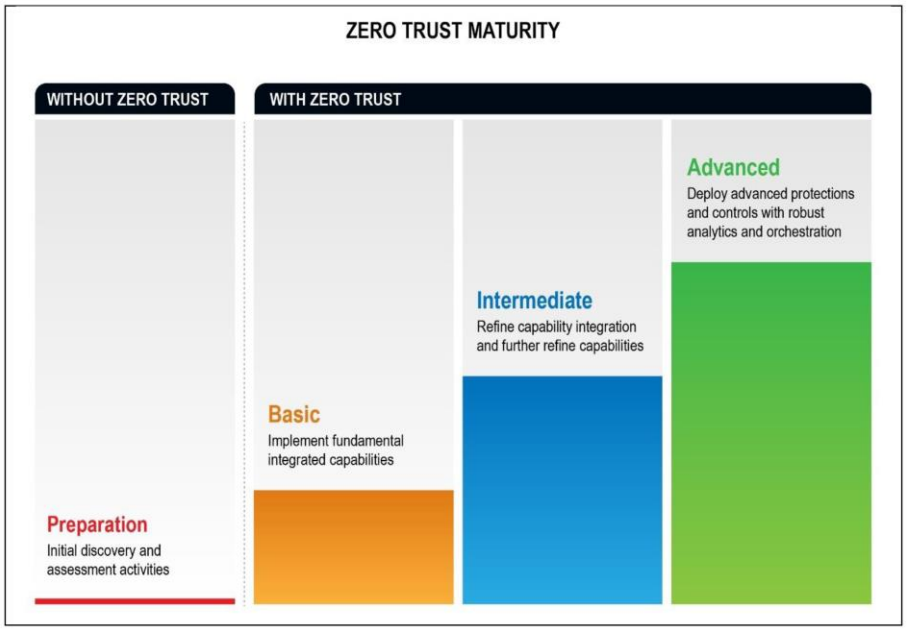

Figure 4: DoD/NSA Zero Trust Maturity Model[7]

Table 1: Phases of Zero Trust Maturity Models

CISA	DoD/NSA
Traditional	Preparation
Initial	Basic
Advanced	Intermediate
Optimal	Advanced

As seen in Figure 3, CISA labels the maturity levels as “Initial,” “Advanced,” and “Optimal.” DoD/NSA labels them “Basic,” “Intermediate,” and “Advanced” (Figure 4). Additionally, each describes a preliminary stage in which traditional cybersecurity models are in use and preparatory actions are being taken to be equipped to take the first ZT steps. As with the ZT pillars, there are nuanced differences in the models and the terminology is distinct in parts. However, the concepts are consistent and so we discuss them here in an integrated manner, using only the CISA terminology for simplicity.

4.1 Phase 1: Traditional

To make meaningful progress toward ZT, an organization must first understand its current security posture. It should inventory its DAAS elements and users and document the mission and protection requirements that will drive the implementation of security controls. An organization should assess its deployed cybersecurity technologies and policies for fulfillment of

ZT principles. Some deployed technologies may already fulfill the requirements of ZT and an organization's baseline in some ZT columns may be more advanced than in others.

Organizations in this phase often have manual-only processes for provisioning and deployment, user attribute configuration, system patching, and incident response. Integrated log collection and analysis is limited, along with centralized access management, device inventory, and policy enforcement. Authentication may include MFA or passwords and minimal data at rest or in transit is encrypted.

4.2 Phase 2: Initial

Integration and automation are key demarcations of the initial phase of ZT implementation. Organizations in this phase will be automating device configuration and patching tasks, user and service attribute configuration and updating, and policy decisions and enforcement. Integrated log collection and analysis along with limited device compliance collection to include in access decisions is beginning to be employed.

Data categorization has started and limited automated data access based on least privilege is applied. Data is encrypted in transit. Authentication is performed using MFA that may include a password as a factor. Key management policies are formalized.

4.3 Phase 3: Advanced

Phase 3 is marked by increased automation and visibility across the enterprise. This yields deeper integration of context-based insights into access decisions and faster detection and response to unauthorized or abnormal behavior. Log correlation and analysis is centralized. Data inventory and tracking is automated, along with monitoring and enforcement of policies and compliance of devices. Phishing-resistant MFA is utilized for access. Network configuration – and automated reconfiguration – enables increased isolation of devices and workflows. Encryption is ubiquitous for data at rest and in transit.

4.4 Phase 4: Optimal

The highest level of maturity is reached once an organization is fulfilling the principles of ZT throughout its enterprise. Robust analytics are in place, supporting comprehensive situational awareness and automated deployment, management, and protection of DAAS elements. Access decisions are based on user and system risk adjudication at the time of the request. Adjudication is performed continuously, not just upon initial access, and incorporates behavior-based analytics, device posture assessment, and dynamic policies. Phishing-resistant MFA is required for authentication. Identity management is integrated and centralized across the enterprise.

Security testing is integrated through application and service development-deployment-maintenance lifecycle. Applications, services, and systems are isolated through fully configured

and dynamic micro-perimeters in the network. Data categorization and labeling across applications and systems is automated and data is inventoried continuously.

5.0 References

[1] Cybersecurity and Infrastructure Security Agency. Zero Trust Maturity Model, v.2.0. April 2023. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

[2] Department of Homeland Security. Zero Trust Implementation Strategy. October 2023.

[3] Department of Defense. Zero Trust Reference Architecture, v.2.0. July 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

[4] Department of Defense. Zero Trust Strategy, v.1.0. October 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[5] Executive Order No. 14028, 86 FR 26633, 2021. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[6] National Institute of Standards and Technology (2020) Zero Trust Architecture. (Department of Commerce, Washington, D.C.), Special Publication 800-207. https://doi.org/10.6028/NIST.SP.800-207.

[7] National Security Agency. Embracing a Zero Trust Security Model, Cybersecurity Information Sheet, v.1.0. February 2021. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

[8] National Security Agency. Advancing Zero Trust Maturity Throughout the Device Pillar, Cybersecurity Information Sheet, v.1.0. October 2023. https://media.defense.gov/2023/Oct/19/2003323562/-1/-1/0/CSI-DEVICE-PILLAR-ZERO-TRUST.PDF

[9] National Security Agency. Advancing Zero Trust Maturity Throughout the User Pillar, Cybersecurity Information Sheet, v.1.1. April 2023. https://media.defense.gov/2023/Mar/14/2003178390/-1/-1/0/CSI_Zero_Trust_User_Pillar_v1.1.PDF

[10] National Security Telecommunications Advisory Committee. NSTAC Report to the President, Zero Trust and Trusted Identity Management. February 2022. https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management%20%2810-17-22%29.pdf

[11] Office of Management and Budget, Executive Office of the President. Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (2022). https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[12] ON2IT. An Introduction to Zero Trust. 2021. https://isaca.nl/wp-content/uploads/Downloads/Square%20Tables/2021/2021%2010%2013%202021%20An%20Authentic%20Zero%20Trust%20Guide.pdf

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

www.pnnl.gov