Pacific Northwest
NATIONAL LABORATORY

PNNL-37516

Countering Weapons of Mass Destruction (CWMD) Zero Trust Framework

CWMD Zero Trust Principles Model

March 2025

Penny McKenzie
Mark Watson
Aubrie Kendall
Riley Maltos
Ernest Allard
Jarrett Zeliff
Ernest Tumanyan

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-37516

Countering Weapons of Mass Destruction (CWMD) Zero Trust Framework

CWMD Zero Trust Principles Model

March 2025

Penny McKenzie
Mark Watson
Aubrie Kendall
Riley Maltos
Ernest Allard
Jarrett Zeliff
Ernest Tumanyan

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

Pacific Northwest National Laboratory
Richland, Washington 99354

Abstract

The research focuses on the critical need for enhanced cybersecurity within the Countering Weapons of Mass Destruction (CWMD) Office, specifically targeting Chemical, Biological, Radiological, and Nuclear devices. Traditional perimeter-based security models are insufficient against modern cyber threats, prompting a shift toward Zero Trust principles (ZTP) that emphasize continuous verification and stringent security for all devices. Federal directives mandate the adoption of Zero Trust (ZT) across agencies, supported by guidelines from National Institute of Standards and Technology (NIST), U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), U.S. Department of Defense (DoD) and National Security Agency (NSA). The research involved mapping ZT guidance from these agencies to develop tailored CWMD ZTP. The study identified gaps and areas for improvement, including clear transitional guidance from traditional to ZT architectures and the focus on explicit cross-cutting capabilities. Design improvements are recommended to ensure increased comprehensive protection and resilience against sophisticated cyber threats for Chemical, Biological, Radiological, and Nuclear (CBRN) devices. Collaborative efforts among federal agencies are essential for the successful deployment of an optimized ZT guidance.

Summary

This research addresses the urgent need for enhanced cybersecurity within the CWMD Office, focusing on CBRN devices. Traditional security models are inadequate against modern cyber threats, necessitating the adoption of ZTP, which emphasize continuous verification and rigorous security for all devices.

Federal directives mandate ZT implementation across all agencies, supported by key documents such as National Institute of Standards and Technology SP 800-207 “Zero Trust Architecture,” CISA’s “Zero Trust Maturity Model,” the DoD’s “Zero Trust Reference Architecture,” and NSA’s “Embracing a Zero Trust Security Model.” These guidelines provide a comprehensive framework for eliminating implicit trust and ensuring continuous validation of all digital interactions.

The research involved mapping ZT guidance from CISA, NSA, and DoD to develop tailored CWMD ZTP. The study identified alignments, gaps, and differences across these models using the Derived Relationship Mapping methodology. Key findings indicate the need for clear guidance on transitional stages from traditional to higher levels of maturity for ZT architectures, emphasizing phased implementation and planning. Further, it was noticed that the explicit delineation of cross-functional capabilities was needed to ensure cohesive and integrated security measures across all pillars.

However, there is a need to address design improvements. The current CWMD ZTP needs to address specific requirements of CBRN devices more thoroughly, including the diverse technologies and operational environments they encompass. Clear and well-defined archetypes for CBRN devices would assist in that process. Finally, increased collaboration among the CISA, NSA, and DoD could result in more condensed ZT guidance for adoption.

In conclusion, adopting ZTP for CBRN devices is critical for national security. Collaborative efforts among federal agencies and targeted research to address identified gaps will optimize ZT model deployment, ensuring comprehensive protection and resilience against sophisticated cyber threats.

Acknowledgments

The Pacific Northwest National Laboratory (PNNL) would like to acknowledge the Test and Evaluation Cyber Team of CWMD Test and Evaluation (T&E) Office for their exceptional support of our work. Their forward-leaning approach to cybersecurity and commitment to ZTP have been crucial in enhancing the security of critical systems. By integrating rigorous identity verification, network segmentation, and continuous monitoring, the team has significantly contributed to the system characterization and overall cybersecurity efforts. We greatly appreciate their dedication to securing the nation and advancing ZTP within the secure system life cycle.

Acronyms and Abbreviations

ABAC	Attribute-Based Access Control
AI	Artificial Intelligence
API	Application Programming Interface
CBRN	Chemical, Biological, Radiological and Nuclear
CI/CD	continuous integration and continuous deployment
CISA	Cybersecurity and Infrastructure Security Agency
CUI	Controlled Unclassified Information
CWMD	Countering Weapons of Mass Destruction
DaaS	Data-as-a-Service
DHS	U.S. Department of Homeland Security
DLP	Data Loss Prevention
DoD	U.S. Department of Defense
DRM	Derived Relationship Mapping
DRM	Data Rights Management
EDR	Endpoint Detection and Response
HBOM	Hardware Bill of Materials
IT	Internet technology
MFA	multi-factor authentication
NIST	National Institute of Standards and Technology
NPE	Non-person entities
NSA	National Security Agency
NTIA	National Telecommunications and Information Administration
OLIR	National Online Informative References
OMB	Office of Management and Budget
SBOM	Software Bill of Materials
SDN	software-defined network
SIEM	Security Information and Event Management
UEBA	User and Entity Behavior Analytics
XDR	Extended Detection and Response
ZT	Zero Trust
ZTA	Zero Trust Architecture
ZTMM	Zero Trust Maturity Model
ZTP	Zero Trust principals

Contents

Figures

Tables

1.0 Introduction

PNNL, working with the DHS CWMD Office, is committed to applying ZTP to safeguard the nations CBRN detection devices and interconnected systems. This ZT Model Landscape Study informs the analysis and methods to develop the CWMD ZTP Model that will be leveraged in establishing benchmarks and future enhancements in planning and conducting ZTP processes, procedures, and execution activities for CWMD T&E.

1.1 Overview

With the evolving digital landscape, cybersecurity has become a critical concern for many organizations including the CWMD Office. Traditional security models, which primarily rely on perimeter defenses, are increasingly becoming inadequate in the face of sophisticated cyber threats. To address these challenges, the cybersecurity paradigm needs to shift toward a more robust and comprehensive ZT approach. ZT is grounded in the principle of "never trust, always verify," which assumes that threats can exist both inside and outside a network. Unlike conventional security models that grant trust by default, once CBRN detection devices are connected to the network, ZT requires continuous verification of every CBRN device attempting to access resources, regardless of its location.

Expanding these ZTP to CBRN devices that use cellular networks, Universal Serial Bus, remote access, and Wi-Fi adds another layer of critical security. CBRN devices, often employed in the detection, identification, and monitoring of hazardous substances, rely heavily on accurate and secure data transmission. Applying ZT ensures that these devices, whether connected via Wi-Fi or cellular networks, are continuously authenticated and verified. This approach prevents unauthorized tampering with CBRN devices, protects sensitive data transmitted by these devices, and ensures integrity in situations where data accuracy is paramount.

Wireless networks offer mobility and flexibility but are often perceived as less secure than wired networks. By integrating ZT, every CBRN device attempting to connect to a wireless network must be continuously authenticated and authorized using multiple data points such as device identity, user credentials, location, and behavior patterns. This ensures that only legitimate and verified CBRN devices gain access, reducing the risk of unauthorized access or leakage of data.

Cellular networks, which are crucial for communication for many CBRN devices, can also leverage ZTP for improved security. With the increasing reliance on cellular connectivity, it is necessary to ensure that every CBRN device and communication channel is secure. By continuously verifying the authenticity of CBRN devices, monitoring traffic patterns, and enforcing strict access controls, ZT can mitigate the risks associated with the use of cellular networks and prevent eavesdropping, data interception, and unauthorized access.

CWMD has a crucial mission that demands an adaptable ZT framework for diverse technologies and operating environments. The ZTP Model offers a framework for enhancing the security of CWMD's CBRN devices. To fully utilize the ZTP Model, it is essential to understand CBRN device roles and functions, as well as their applications across multiple agencies. While ZT guidance has been created by the DHS Cybersecurity Infrastructure Security Agency (CISA), National Security Agency (NSA), and U.S. Department of Defense (DoD) that can be applied

across all critical infrastructure sectors and serve as a cross-agency guide, their generality may pose challenges in applying ZTP for CBRN.

Each section will provide information on the development of the ZTP that provides additional information on the multi-agency ZTAs, the methodology for mapping ZTP, and identifying the similarities, differences, and gaps. This process has provided the information for the development of the CWMD ZTP that supports CBRN devices.

1.2 Guidance

The United States has underscored the importance of adopting the ZT security model across all federal agencies. The initiative is to enhance the nation's cybersecurity posture by eliminating implicit trust and continuously validating every stage of digital interactions. The recommendation for all federal agencies to implement ZT represents a significant initiative aimed at bolstering the cybersecurity defenses of the federal government. This directive is supported by several key documents and strategies: "Improving the Nation's Cybersecurity," National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, "Zero Trust Architecture,[1]" CISA's "Zero Trust Maturity Model (ZTMM),[2]" the Department of Defense Zero Trust Reference Architecture[3], and the NSA "Embracing a Zero Trust Security Model.[4]"

The Office of Management and Budget (OMB) issued the Federal Zero Trust Strategy, detailed in OMB Memorandum M-22-09,[5] dated January 26, 2022. This memorandum sets forth specific cybersecurity goals and deadlines, directing agencies to achieve a government-wide ZT architecture. The memorandum specifies key areas of focus, including identity, devices, networks, applications, and data, with prescribed milestones for each aspect.

To further support agencies in this transition, NIST has published several guidelines. The draft NIST Special Publication (SP) 800-207, "Zero Trust Architecture," provides a comprehensive framework for implementing ZTP. Additionally, NIST SP 800-53 Revision 5[6] includes controls that are essential for supporting a ZT environment.

CISA has also played a pivotal role in guiding federal agencies toward a ZT approach. CISA's ZTMM, released in April 2023, serves as a practical tool allowing agencies to assess their current ZT maturity and identify areas requiring improvement.

The DoD has been actively developing specific ZT strategies and frameworks. In July 2022, the DoD published an updated Version 2.0 to the Zero Trust Reference Architecture, which outlines the department's approach and guiding principles for implementing ZT across its complex and diverse network infrastructure. This reference architecture is intended to serve as a blueprint for DoD organizations as they transition to a ZT model.

---

[1] Rose, Scott, Oliver Borchert, Stu Mitchell, and Sean Connelly. 2020. "Zero Trust Architecture." SP 800-207. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207.
[2] Zero Trust Maturity Model." 2023. CISA. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf
[3] Freter, Robert. 2022. "Department of Defense (DoD) Zero Trust Reference Architecture." Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf
[4] NSA. 2021. "Embracing a Zero Trust Security Model." NSA. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF
[5] Young, Shalanda D. 2022. "M-22-09 MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES." OMB. https://zerotrust.cyber.gov/downloads/M-22-09%20Federal%20Zero%20Trust%20Strategy.pdf.
[6] National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Revision 5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

NSA developed five documents, “Embracing a Zero Trust Security Model,[1]” that outline the ZT maturity development for each pillar:

- Advancing Zero Trust Maturity Throughout the User Pillar,
- Advancing Zero Trust Maturity Throughout the Device Pillar,
- Advancing Zero Trust Maturity Throughout the Network and Environment Pillar,
- Advancing Zero Trust Maturity Throughout the Application and Workload Pillar,
- Advancing Zero Trust Maturity Throughout the Data Pillar.

CBRN devices, due to their critical nature and potential impact, are prime candidates for ZT implementation. These recommendations collectively emphasize the adoption of ZTA to ensure comprehensive security and integrity. CBRN devices must be continuously verified, ensuring that only authorized personnel with verified and authenticated identities have access. Devices and networks associated with CBRN must be secure, employing specialized measures such as network segmentation, endpoint security, and encryption to protect their integrity and security. Applications that interact with CBRN devices must be protected through secure coding practices and regular vulnerability assessments. Data generated and utilized by CBRN devices must be encrypted and access-controlled to maintain its confidentiality and integrity.

By using the ZT guidelines as a foundational resource, CWMD can effectively implement ZTP for CBRN devices. These guidelines are fundamental in supporting CWMD’s mission by ensuring that deployed devices are inherently trusted and secure. CWMD Test and Evaluation can employ the developed baseline ZTP to rigorously assess the security of ZT measures for CBRN devices. This evaluation for CBRN devices can reliably support mission partners in their operations.

These specific ZT policies and guidelines were explored to provide a comprehensive understanding of how ZTP can be systematically applied to enhance the security posture of CBRN devices and ultimately advance CWMD's mission objectives.

1.3 Purpose

The primary purpose of developing ZTP for CBRN devices is to establish a ZT framework capable of establishing multi-level security benchmarks for increasing maturity while systematically evaluating the unique attributes and potential vulnerabilities of these critical devices and interconnected systems. CBRN devices are essential for detecting, identifying, and monitoring hazardous substances. By integrating ZTP, CWMD can continuously authenticate and authorize devices, ensuring only legitimate and verified users have access, thus preventing unauthorized tampering and protecting sensitive data. This approach enhances threat detection and response, maintaining secure CBRN operations. The development of the ZTP establishes foundational understanding of ZT capabilities used to identify testing activities, procedures, and benchmark security controls for CBRN devices.

[1] National Security Agency. (n.d.). Embracing a Zero Trust Security Model. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_508C.PDF

1.4 Scope

This report lays the groundwork for the Zero Trust framework in CWMD T&E, outlining strategies to advance the maturity of ZT in CBRN devices and interconnected systems. Key objectives include:

(1) **ZT Model Landscape Study –** Assessing current guidelines and relationships to strengthen CWMD's Zero Trust posture by analyzing policies and frameworks from other organizations. This ZT Model Landscape Study guides the analysis and methodologies for creating the CWMD ZTP Model, which will set benchmarks and drive future improvements in planning, executing, and managing ZTP processes, procedures, and activities for CWMD T&E.

(2) **CWMD ZTP Framework –** Developing the Zero Trust Framework for CBRN technologies by evaluating existing ZT maturity for CWMD Test and Evaluation (T&E) security validation and determining next steps to enhance security requirements for future acquisitions.

2.0 ZT Model Landscape Study

A dedicated ZT model landscape study was conducted to develop CBRN-specific criteria and guide the implementation of the CWMD ZTP Model for CBRN devices. In support of the ZT model landscape study, a ZT policy crosswalk was performed between CISA, NSA, and DoD ZT guidance documents to provide insights into their strategic approaches to ZT and ZTA. The ZT policy crosswalk outlines the potential and unique contributions that each guidance document brings to the overall understanding of the multi-level approaches towards ZT maturity. The results of the ZT policy crosswalk are extensive and can be made available upon request.

2.1 Policy Mapping Approach

A ZT policy crosswalk comparison was enumerated from the derived set of guidance documents. This comparison involved some elements of NIST Derived Relationship Mappings (DRM) to assess the compatibility between each model, identifying gaps and trends. A gap refers to information or functionalities present in one model but absent in another. Compatibility involves directly comparing the functions to determine how well they align and are integrated.

The analytic process for mapping ZT guidance was further derived from DRM relationship models and concepts documented in NIST IR 8278r1[1] and NIST IR 8477[2]. Although a specific DRM model to document rationale and relationship types was not directly applied, as prescribed in NIST, use of supportive relationship definitions was included in the ZT policy crosswalk analysis of ZT guidance documents. This approach facilitated the comparison of the ZT guidance from CISA, NSA, and DoD by using CISA's guidance as the focal document and NSA and DoD as reference documents. This process aimed to highlight commonalities and gaps by comparing functions, capabilities, pillars, maturity levels, and strategies across these documents. The methodology's application helped to infer potential relationships and develop a comprehensive and integrated model for ZT implementation. While inferred connections were identified, they were not indicative of direct compliance or similarity; further verification was necessary to meet CWMD requirements and regulatory standards.

2.2 ZT Pillars and Definitions

The ZT guidelines describe the *"function"* as the specific security activity or capability that an organization should implement (e.g., "policy enforcement & compliance monitoring" or "device detection and compliance"). The ZT term *"strategy"* is defined as a higher-level guideline for how an organization will implement and integrate ZT functions across its environment. The ZT *"pillars"* are the foundational security domains or focus areas that collectively define and strengthen an organization's ZT posture.

- ***Pillars*:** The core components of a ZTA framework supporting foundational elements that reinforce functions and strategies on the principle of "never trust, always verify."

[1] Keller, N., Barrett, M., Quinn, S., Scarfone, K., Smith, M. C., & Johnson, V. (2024). *National Online Informative References (OLIR) Program: Overview, benefits, and use* (NIST Interagency/Internal Report 8278r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8278r1

[2] Fagan, M., Quinn, S., Scarfone, K., Souppaya, M. (2024). *Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines (NIST Interagency/Internal Report 8278r1).* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8477.pdf

- ***Function*:** What the security program must do (the technical or operational activity).
- ***Strategy*:** Why and how it is done, with a focus on overarching objectives, priorities, and risk reduction.

Each pillar represents a distinct dimension of security, such as identity or devices, and outlines the principles, controls, and processes needed to address threats and manage risk within that domain. When these pillars are developed and integrated together, they create a comprehensive and cohesive security strategy aligned with ZTP:

- **Identity (ID):** Verifying and managing user (i.e., human and non-human) identities rigorously.
- **Devices:** Ensuring all devices are authenticated and meet security standards.
- **Networks**: Segregating and securing networks to prevent unauthorized access.
- **Applications and Workloads:** Protecting applications from development through deployment.
- **Data:** Safeguarding data integrity and confidentiality always.

A ZTMM outlines stages of maturity reflecting the progression of ZT implementation. The following stages of maturity are examples from the different CISA, DoD, and NSA ZT guidance documents:

- **Traditional:** Manual configurations throughout an asset's lifecycle, with static security policies applied to individual components (pillars) without integration.
- **Prepare:** Initial discovery and assessment activities.
- **Initial:** Introduction of ZT concepts in select areas.
- **Advanced:** Expanded adoption with automated and integrated security practices.
- **Optimal:** Full realization of ZTA with proactive threat mitigation.

The pillar alignment process involved identifying key pillars within CISA's ZTMM as the focal document and aligning them to maturity model elements from NSA's guidance. CISA's pillars include Identity, Devices, Network, Applications and Workloads, and Data, which represent broad cybersecurity domains. The NSA’s and DoD’s ZT models were also examined to isolate guiding pillars for cybersecurity efforts. This step established a foundation for comparison.

Function alignment involved extracting specific functions from each document. The goal was to find direct function matches or overlaps, highlighting the nuances in each agency’s approach.

Maturity and strategy alignment involved correlating elements across CISA, NSA, and DoD ZT guidance. The DoD model, as compared to CISA and NSA models, did n**o**t categorize functions. This entailed recognizing similarities and integrating complementary strategies to determine ZT themes and gaps in the mapping process.

Gaps were documented and categorized for clear comparison, offering insights into potential areas for tailored CWMD ZTP guidance.

2.3 Policy and Guideline Gaps

The three core ZT federal guidance documents were compared and correlated, allowing for a more accurate identification of overlaps and discrepancies to target improvements and ensuring comprehensive guidance across various maturity models.

- **Functions vs. Capabilities:** The CISA maturity model sections within a pillar are referred to as functions, while the NSA denotes them as capabilities, highlighting a nuanced difference in terminological approach that reflects their methodological focuses. CISA's functions are clearly delineated and categorized across pillars, promoting a structured and compliance-focused architecture. NSA's capabilities are more integrated, designed to weave cross-cutting elements through various security functions, emphasizing a risk-based approach. CISA focuses on adherence to federal requirements, and NSA prioritizes a comprehensive risk management strategy.
- **Maturity Level:** The maturity levels of both agencies reflect different approaches: CISA (Traditional) and NSA (Prepare). CISA emphasizes the incremental advancement of ZT strategies and controls. This highlights the importance of integration and dynamic policy enforcement at every maturity level. Despite acknowledging the importance of planning and baseline assessments, CISA does not embed these as critical components within its maturity model; rather, they serve to guide the progression. CISA views the first maturity level as a traditional architecture with limited controls supporting a ZTA.

  NSA's ZT model prioritizes planning, assessment, and baselining, impacting how each pillar conceptualizes the pathway to advanced ZT maturity. DoD aligns with NSA's approach by emphasizing discovery and assessment strategies in their maturity level. Unlike NSA, DoD distinguishes between discovery and assessment as two separate processes within the baseline maturity level.
- **Cross-Cutting Capabilities:** NSA's approach to modeling cross-cutting capabilities reveals a difference compared to the approach taken by CISA. Instead of delineating cross-cutting functions separately, NSA weaves them through its other functions using specific word choices. This approach may lead to a less clear understanding of how these essential capabilities are addressed within the overall model.
- **Differing Focus:** When comparing the NSA's and CISA's approaches to a ZT maturity, a notable gap arises from their differing priorities. NSA emphasizes a risk perspective, focusing on identifying, assessing, and mitigating potential cybersecurity threats. NSA discusses risk-informed decisions and describes ZTA as a strategic plan that can reduce overall risk. CISA’s approach ensures clear delineation of various functions, facilitating straightforward compliance with federal mandates. NSA prioritizes a holistic risk management approach, while CISA prioritizes adherence to regulatory models.
- **Level of Guidance:** NSA provides specific and detailed guidance in their strategies. NSA focuses on specific processes, detailed steps, and technical implementations necessary for a ZTA. These include guidelines, protocols, and measures to be implemented for enhancing cybersecurity.

  CISA provides a generalized model, and high-level strategies aimed at assisting agencies in developing their ZT strategies. CISA emphasizes the broader objectives, policy mandates, and evolution of ZTP rather than detailed procedural implementations.

This difference in approach could be attributed to the distinct roles and audiences of these agencies. NSA documents are tailored for national security systems and defense-related sectors, and CISA caters to a broader range of federal civilian agencies and critical infrastructure sectors, emphasizing strategic goals and adaptable models.

2.4 Identified Gaps in Pillars

Transitioning from the identification of major gaps to a detailed examination of pillar-specific gaps and findings involves analyzing the specific challenges within each agency's model. By focusing on key functional areas and their corresponding shortcomings, a clearer understanding of the impact on the overall effectiveness and strategic alignment of ZT guidance is achieved. This analysis will provide insights into how each agency's approach to ZT needs to be adjusted or expanded to address these critical gaps.

2.4.1 Identity Pillar Gaps

- **Complexity and Usability in ZT Adoption:** Adopting ZT can be complex and overwhelming, especially for organizations new to ZT. Simplified adoption processes may lack advanced features like predictive analytics and AI-driven processes. Relying on legacy identity and access systems can slow adoption and hinder modernization.
- **Transitional and Pre-ZT Guidance:** There is often a lack of guidance for pre-ZTAs and transitional steps, making phased implementation challenging.
- **Governance and Automation in Identity Management:** Missing emphasis on governance integration with analytics-driven decision-making and a lack of focus on dynamic governance and continuous policy updates can limit identity management effectiveness. Limits on human resources and insufficient automation for real-time identity and access management hinders adaptive security measures in addition to human resource constraints on current equipment knowledge and the aging workforce.
- **Real-Time Capabilities and Adaptive Identity Security:** Real-time identity security can be difficult to implement due to complexity. Approaches focusing on foundational ZT identity principles may not emphasize real-time risk assessments or automated compliance enforcement. Lack of real-time identity verification, adaptive access management, and predictive risk mitigation reduces effectiveness for dynamic security needs.

2.4.2 Devices Pillar Gaps

- **Aligned Approach:** The emphasis on comprehensive device management, inventory maintenance, continuous compliance, and proactive threat detection and remediation highlights the importance of dynamic lifecycle management for secure endpoints, which cannot be overstated.
- **Limited Focus:** CWMD takes a basic approach to device security, focusing on fundamental Internet technology (IT) security policies rather than advanced automation for provisioning, monitoring, and threat remediation, and lacks proactive, continuous processes.
- **Asset vs. Device Perspective:** Focusing on real-time tracking and automated compliance enforcement for devices, contrasting strategies in inventory management and risk assessment between assets and devices can result in visibility and enforcement gaps.
- **Threat Protection and Compliance:** CWMD prioritizes continuous monitoring with advanced tools like Endpoint Detection and Response for automated vulnerability remediation but relies

more on self-reported device characteristics and manual enforcement, potentially delaying threat detection and resolution.

- **Automation and Centralized Management:** CWMD advocates for automated provisioning, configuration, and centralized device management for real-time risk assessments and remediation; however, it is comprehensive but less explicit about the use of advanced automation and orchestration tools.

2.4.3 Network Pillar Gaps

- **Aligned Approach:** The emphasis on robust network segmentation, dynamic traffic management, and comprehensive encryption highlights a gap in reducing lateral movement and ensuring secure connectivity.
- **Distinct Focus:** The basic approach to network segmentation and threat detection, focusing on fundamental IT security standards over advanced operational resilience, highlights a gap due to the lack of detailed, dynamic strategies.
- **Segmentation and Traffic Management:** Granular micro-segmentation with rigorous testing and policy refinement to restrict lateral movement, compared to broader, perimeter-based segmentation. This difference can impact the transition from macro to micro-segmentation and overall network agility and security.
- **Encryption and Resilience**: Emphasis on encrypting network traffic and resilient architectures. Advanced focus on automated key management and real-time analytics for threat detection, compared to foundational guidance without advanced automation. Basic compliance focus over dynamic, adaptive resilience measures.
- **Automation and Analytics:** Incorporation of centralized management and automated orchestration for network controls such as just-in-time connectivity and dynamic risk-based adjustments. Reliance on manual configuration and basic automation suggests an opportunity for integrating advanced analytics and automated response mechanisms to enhance network security.

2.4.4 Data Pillar Gaps

- **Aligned Approach:** Emphasis on data protection, integrity, and secure access. Advocates for comprehensive data security measures and reliable recovery processes. Alignment on cross-cutting capabilities like visibility, analytics, and governance.
- **DaaS Focus:** Emphasis on automation of data tagging, Data Loss Prevention (DLP), and Data Rights Management (DRM). Noteworthy mention of Data-as-a-Service (DaaS) for comprehensive data management and security.
- **Data Loss vs. Data Availability:** The focus on Data Loss Prevention (DLP) to prevent unauthorized data exfiltration, while concentrating on data availability by ensuring redundancy and accessibility through highly available data stores and off-site backups, addresses critical aspects of data security from different angles and aligns with the Confidentiality, Integrity, and Availability (CIA) triad principles.
- **Access Control:** Explicit mention of Role-Based Access Control and Policy-Based Access Control. Similar implications on automation of least privilege and dynamic access controls. Highlighting Attribute-Based Access Control (ABAC), with different focal points on identity and diverse attributes for access decisions.

- **Automation Tools and Integration:** Mention of specific tools like Software-Defined Storage, Identity Provider, and other DRM tools for phased integration and improved access controls. Focus on overall movement toward automation and use of various attributes without specifying particular tools.

2.4.5 Application and Workload Pillar Gaps

- **Application Workflow Management and Mapping:** Structured approach to application management but lacks detailed workflow mapping. No comprehensive workflow for application management, making the approach less explicit. Merging application layer controls with broader user and device security strategies, without distinct emphasis.
- **Risk Awareness and Threat Protection:** Risk-focused model prioritizing risk analysis and automation, lacking explicit application-specific threat protection customization. Less emphasis on external threats and risk-informed decision-making. No detailed, function-specific guidance for application security, treating it as part of a broader governance strategy.
- **Software and Hardware Security and Modern Development Practices:** Highlights the importance of a Software Bill of Materials (SBOM) and Hardware Bill of Materials (HBOM) in development and testing, while gaps in secure software and hardware supply chain visibility exist. Minimal attention to modern software security practices like DevSecOps and continuous integration and continuous deployment (CI/CD) pipeline management compared to detailed discussions in other approaches.
- **Application Availability and Environment Considerations:** Does not address application availability in detail, unlike models incorporating availability considerations. Insufficient focus on modern application environments, resulting in a lack of adaptability to cloud-native and microservices-based architectures.

3.0 CWMD ZTP Framework

The gathered insights from each guidance document in the ZT Model Landscape Study were utilized to develop an overall CWMD ZTP Framework. By integrating CISA, DoD, and NSA ZT guidance, a more robust and harmonized ZTP Model was developed specifically for CWMD. The guidance addresses unique CBRN security challenges, ensuring a more comprehensive approach to protecting critical data and operational environments. The CWMD ZTP will facilitate effective and efficient assessment and guidance of ZT implementation.

3.1 CWMD ZTP Core Principles

The core CWMD ZTP is centered around “never trust, always verify” and is designed to protect sensitive data and systems in an environment where threats could be internal or external. ZTP for CBRN adheres to the same concept with the addition of understanding the connection, communications, and data transfer methods for each device. CBRN devices can be very diverse and ZTP can vary on the internal or external environmental deployment factors. The minimum set of principles for CBRN include:

- **Continuous verification:** ongoing assessment and validation of access requests and user behaviors to ensure security regulations and policies are consistently upheld.
- **Least privilege:** users, systems, and processes should only be granted the minimum level of access—or permissions—necessary to perform their legitimate functions or tasks.
- **Micro-segmentation:** divide a network into smaller, more manageable segments or zones to isolate and protect sensitive data and critical applications
- **Identity and access management:** mechanisms for identifying, authenticating, and authorizing users to access CBRN systems, applications, and data.
- **Device security:** protection of endpoints such as cell phones, tablets, CBRN devices from malicious activities.
- **Network security:** protection of data that is being transmitted across CBRN networks (e.g., cellular, Wi-Fi, Bluetooth, etc.).
- **Data protection:** sensitive CBRN data is secure and only accessible to authorized users.
- **Continuous monitoring:** on-going analysis of CBRN network and system activities to identify, assess, and respond to malicious activity.

The use of ZTP in testing activities and procedures for CBRN devices will be used to verify every point of access (e.g., login, app verification, cloud, etc.) to reduce implicit trust and strengthen the security of operational CBRN. The CWMD ZTP model is designed to the validation of device configurations and user roles against security policies, promoting real-time assessments and adjustment needs. The development of testing processes for CWMD ZTP involved establishing new methodologies to continuously evaluate and verify device security, user access, and network integrity, which is included in the ZTP playbook.

The process of the CWMD ZTP involved defining the foundational pillars, naming key security functions, incorporating policies, guidelines, and best practices and by conducting thorough reviews to ensure alignment with DHS cybersecurity goals

The process began by establishing clear definitions from each pillar using the reference documentation. For instance, the data pillar uses data classification, encryption, access control, and DLP strategies and was highlighted as a key purpose for CWMD ZTP. This step ensures that the scope and security concerns specific to each pillar are comprehensively understood and adequately addressed.

The pillar function titles combined elements identified from CISA functions and NSA capability elements as outlined in the guidelines mapping analysis. When examining the Applications and Workloads Pillar, one of the CISA functions is named “Application Access,” while the NSA Workloads Pillar is “Resource Authorization and Integration.” To bridge the gaps for defining the CWMD ZT functions, the CISA and NSA titles were taken into consideration. To bridge the gaps between the two models, the identified CWMD function from the Workloads Pillar is “Application Authorization & Access.” These new function titles are documented in the function section of the CWMD ZTP for the corresponding pillar. In cases where no match was found between CISA functions and NSA capabilities, the original function name was maintained to ensure alignment and integrity with the reference documents. The DoD reference document was not included in this step of the process as it does not have defined functions or capabilities.

Strategies from each agency were aligned to the corresponding maturity stage and function. This involved ensuring that the language was consistent and recording it in the relevant section of the table. When redundant content was identified, judgment was used to either omit or modify it to reflect the collective intent of the relevant guidance between CISA, NSA, and DoD. If a strategy addressed a gap, an additional statement was added to ensure alignment. Despite having the same overall intent, different agencies' word choices in their strategies cause them to address specific aspects of ZTA uniquely. In these cases, it was either addressed as a gap or treated as redundant depending on the context of the strategy. This process was repeated until all strategies from CISA, NSA, and the DoD maturity model were integrated for each function. It was found that some of the traditional or prepare maturity level strategies were missing, so a traditional or a prepare maturity level was designed to flow within the maturity progression. The entire pillar was reviewed to confirm that all functions and strategies were included, addressing any gaps, ensuring the language flowed coherently, and maintaining the logical consistency of the model.

3.2 CWMD ZTP Model

The CWMD ZTP is specifically designed to enhance the security and resilience of CBRN detection devices through a structured approach. This model comprises five maturity levels, each aimed at progressively strengthening the security framework to protect against sophisticated threats. The levels are outlined as follows:

- **Level 0 - Traditional:** Utilizes conventional security measures, providing basic protection for CBRN detection devices with limited ZT implementation.
- **Level 1 - Prepare:** Establishes foundational strategies and planning tailored for CBRN environments, preparing systems for the integration of ZTP while assessing current capabilities.
- **Level 2 - Initial:** Initiates the deployment of foundational ZT strategies to enhance identity management and access control specific to CBRN detection systems, ensuring better protection and monitoring.

- **Level 3 - Intermediate:** Embeds advanced security techniques such as automated monitoring, enhanced situational awareness, and risk-based access controls to ensure these critical devices function securely.
- **Level 4 - Advanced:** Incorporates comprehensive, sophisticated security mechanisms, including adaptive access controls and continuous threat analytics, ensuring real-time protection and optimization for CBRN detection devices.

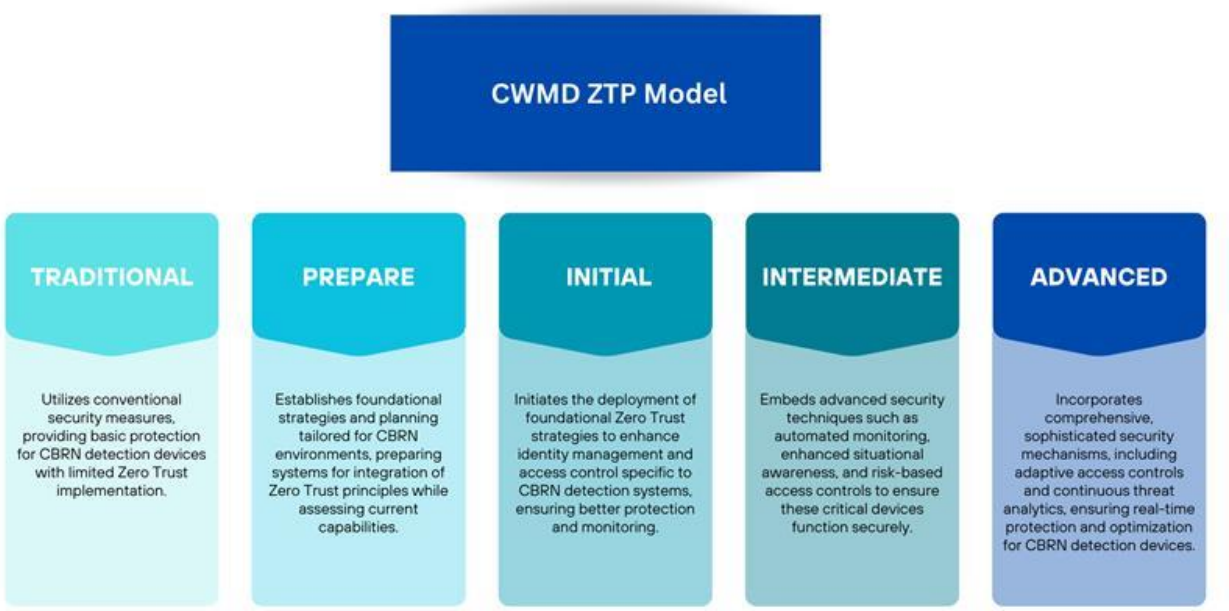

Figure 1 CWMD ZTP Model

In the figure above, the combined function names resulted in five maturity levels that best represent the progressional advancement of CWMD ZTP. ZTP Model functions and their naming conventions were derived from a variety of functions and maturity nomenclatures, necessitating the categorization, rearrangement, and alignment of the information. For example, CISA defines its levels as traditional, initial, advanced, and optimal; NSA uses preparation, basic, intermediate, and advanced; and the DoD employs discovery/assessment, baseline, intermediate, and advanced. The last three levels (i.e., Initial, Intermediate, and Advanced) are aligned in straightforward manner, but the initial maturity stages differed the most due to each agency's unique approach. The initial levels (i.e., Traditional and Prepare) were aligned to display a progressional advancement within the maturity model toward a more advanced ZTA.

3.3 CWMD ZTP Application

To use the ZTP Model, CWMD should conduct a thorough baseline assessment. The baseline will inform CBRN device maturity progression and will point to the strengths and weaknesses in the maturity toward ZTA. With the weaknesses outlined from the ZTP, CWMD can ensure that any gaps or areas that security is found to be lacking in are improved through a ZT roadmap. A ZT roadmap can be created that aligns with ZTP:

- **Identity and Access Management Overhaul:** Implement rigorous identity verification processes, using multi-factor authentication and continuous session monitoring to ensure only authorized personnel can access CBRN devices.
- **Network Segmentation:** Establish protected network zones accessible only to verified users, reducing potential attack vectors and limiting the exposure of CBRN devices.
- **Adoption of Least Privilege Access:** Enforce a least privilege approach, granting users minimal access necessary and adding an extra layer of defense against unauthorized actions.
- **Continuous Monitoring and Automated Response:** Deploy advanced monitoring tools to detect and address anomalies in real-time, ensuring swift and effective threat mitigation.
- **Data Encryption and Protection:** Use comprehensive encryption strategies to secure sensitive data both in transit and at rest, protecting it from unauthorized access or breaches.

Once the ZTP has been established and baseline assessments have been completed, the next step is to develop a comprehensive implementation plan based upon the ZT guidance. This plan should leverage a structured progression framework as seen in the DoD Zero Trust Overlays,[1] which provides a phased approach to achieving both target and advanced levels of ZT as depicted in their Zero Trust Reference Architecture. Notably, the DoD's roadmap for Zero Trust implementation is aligned with a strategic plan that sets forth clear goals and milestones for advancing ZT guidance. This structured approach operates differently from a maturity model, which focuses on assessing current capabilities and guiding their evolution. By utilizing the baseline gathered from the ZT guidance documents, CWMD can create an implementation plan that ensures a clear, practicable pathway for addressing ZT guidance for CBRN devices.

DHS CISA created their implementation plan by taking the insights garnered from the initial ZT guidance assessments and applying them to a strategic framework tailored to the DHS's unique operational environment. CISA has made notable advances in implementing ZT[2], such as their cloud security gateway and multi-factor authentication initiatives. Like DoD, CISA plans incorporate a detailed roadmap outlining specific actions, responsible parties, timelines, and resource requirements necessary to achieve incremental ZT maturity. CISA’s implementation plan addresses challenges such as resource constraints, legacy technology, and shared services environments. This alignment ensures the roadmap is grounded in practical steps that promote standardization and interoperability, essential for a cohesive ZT environment. Emphasizing continual verification, least privilege access, and adaptive threat protection, the implementation plan aligns with the principle that no part of CBRN devices is ever implicitly trusted, supporting CWMD’s mission to secure CBRN devices.

[1] Zero Trust Overlays.” 2024. DoD. https://dodcio.defense.gov/Portals/0/Documents/Library/ZeroTrustOverlays.pdf
[2] Cybersecurity & Infrastructure Security Agency. (2023, April). *Zero Trust Maturity Model Version 2*. https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf

4.0 Plan for Future Enhancements

The CWMD ZTP is designed with a broad focus, providing a comprehensive framework that can be adapted to various security contexts. However, the diverse and complex nature of CBRN devices presents an opportunity for further refinement. Each CBRN device may operate at different levels and incorporate distinct technologies, making it challenging to develop a universally applicable framework.

To enhance its effectiveness, the CWMD ZTP can benefit from the inclusion of well-defined archetypes that cater specifically to the unique requirements of CBRN scenarios. These archetypes would offer tailored guidance for customizing and applying ZTP to CBRN devices, ensuring that the specific needs associated with this diverse spectrum are fully addressed and applied in acquisition requirements. By developing these targeted archetypes, the CWMD ZTP can achieve a higher degree of precision and relevance, ultimately providing more robust and effective security solutions for CBRN environments.

To fully address the unique requirements of CBRN devices and enhance the CWMD ZTP, the following steps should be taken. A detailed inventory and categorization of all CBRN devices should be conducted. Their capabilities, vulnerabilities, and specific security needs should be assessed to understand the unique challenges each category presents. Key archetypes that represent common types of CBRN devices, technologies, and operational contexts should be identified. ZTP should be tailored to each archetype, with specific guidance on identity and access management, network segmentation, threat detection, and data protection suited to their unique requirements.

With the playbook already being created and scenarios developed, the focus should now be on finalizing these guidelines. The playbook should outline step-by-step procedures for deploying the CWMD ZTP across different archetypes, including the developed use cases and real-world examples that illustrate practical applications within various CBRN scenarios. Specialized training programs should be developed to educate personnel on managing and securing CBRN devices. Workshops and hands-on exercises should be conducted to reinforce this training, providing practical experience in applying tailored ZTP.

Advanced technologies, such as automation and artificial intelligence (AI), should be utilized to enhance threat detection, response, and policy enforcement specific to each archetype. Advanced monitoring tools designed for different CBRN devices should be deployed to ensure continuous protection and swift adaptation to emerging threats. A regular review and update process for the CWMD ZTP should be established to incorporate new findings, technologies, and evolving threats. Feedback mechanisms should be implemented to gather insights from field personnel and other stakeholders, ensuring the framework remains relevant and effective.

Collaboration among agencies like CISA, DoD, and NSA should be fostered to share knowledge, best practices, and advancements in ZT tailored to CBRN contexts. Efforts should be made to standardize practices across these agencies to ensure a harmonized approach to securing CBRN devices.

The integration of ZT guidance using the DRM method allowed for tailored ZT guidance for CBRN devices and is vital for enhancing national security by ensuring robust cybersecurity measures. The development of the cybersecurity principles, encompassing detailed guidelines from agencies such as CISA, NSA, and DoD, is crucial for addressing the complex and evolving threats targeting CWMD operations. Emphasizing adaptability, continuous verification, and

leveraging collaborative efforts can further optimize the deployment of ZT models, ensuring comprehensive protection and resilience against sophisticated cyber threats.

5.0 References

DHS. 2023. “Zero Trust Implementation Strategy.” Department of Homeland Security. https://www.dhs.gov/sites/default/files/2024-02/24_0129_cio_zero_trust_implementation_strategy_october.pdf.

Freter, Robert. 2022. “Department of Defense (DoD) Zero Trust Reference Architecture.” Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf.

Keller, Nicole, Matthew Barrett, Stephen Quinn, Karen Scarfone, Matthew C Smith, and Vincent Johnson. 2024. “National Online Informative References (OLIR) Program: Overview, Benefits, and Use.” NIST IR 8278r1. Gaithersburg, MD: National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.IR.8278r1.

NSA. 2021. “Embracing a Zero Trust Security Model.” NSA. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF.

Rose, Scott, Oliver Borchert, Stu Mitchell, and Sean Connelly. 2020. “Zero Trust Architecture.” SP 800-207. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207.

Young, Shalanda D. 2022. “M-22-09 MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES.” OMB. https://zerotrust.cyber.gov/downloads/M-22-09%20Federal%20Zero%20Trust%20Strategy.pdf.

“Zero Trust Maturity Model.” 2023. CISA. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

“Zero Trust Overlays.” 2024. DoD. https://dodcio.defense.gov/Portals/0/Documents/Library/ZeroTrustOverlays.pdf.

Appendix A – CWMD ZTP Model Template

The DHS CWMD Test & Evaluation (T&E) division collaborated with the Pacific Northwest National Laboratory (PNNL) to develop the CWMD Zero Trust Principles (ZTP) Model to evaluate and baseline security across stages of maturity for Chemical, Biological, Radiological, and Nuclear (CBRN) devices and interconnected systems. Although the DHS Cybersecurity Infrastructure Security Agency (CISA), National Security Agency (NSA), and Department of Defense (DoD) have developed ZT guidance with emphasis on zero trust strategies, architectures, and maturity models that can be leveraged across large end-to-end Information Technology (IT) environments applicable to various Critical Infrastructure sectors, its broad nature can present challenges when specifically applying ZT guidance to CBRN devices. The ZTP Model in this appendix is meant to provide a foundational maturity framework to enhance the security of CBRN devices for CWMD mission partners.

Implementing ZTPs for CBRN devices is crucial for supporting the mission of CWMD by ensuring that deployed devices are inherently trusted and secure. CWMD T&E can utilize the baseline ZTP to rigorously evaluate security controls and measures for CBRN devices. This evaluation process will reliably support mission partners in carrying out their operations effectively.

The CWMD ZTP Model is specifically designed to enhance the security and resilience of CWMD's CBRN detection devices through a structured approach. This model comprises five maturity levels (e.g., Level 0-4) and 40 Pillar Functions per level across all five pillars each aimed at progressively strengthening the security framework to protect against sophisticated threats. To fully utilize these ZTPs, it is essential to understand CBRN device roles and functions, as well as their applications across multiple agencies. The ZTP Model establishes foundational understanding of ZT capabilities used to identify testing activities, benchmark security controls and assessment procedures, identify gaps and plan actions to strengthen the overall ZT maturity for CBRN devices and interconnected systems.

The CWMD ZTP Model in this appendix is an open framework that can be further tailored from a well-defined zero trust architecture (ZTA) and archetypes represent common types of CBRN devices, technologies, and operational contexts. The ZTP is customizable to provide more robust and effective security solutions based on different archetypes and unique requirements of CBRN use cases and operating environments.

Below is a CWMD ZTP Model template. The consolidated information for the CWMD ZTP Model can potentially increase data sensitivities concerning CBRN assets supporting CWMD mission partners. The results CWMD ZTP Model and can be made available upon request, in accordance with CWMD security guidance.

A.1 Pillar Name Template

Table A.1.1 CWMD Pillar Name Template

Pillar Definitions	Pillar Function	Level 0 – Traditional	Level 1 – Prepare	Level 2 – Initial	Level 3 – Intermediate	Level 4 – Advanced
An XXX refers to an attribute or set of attributes that uniquely describes an agency user or entity, including non-person entities (NPE).	**Function Name**	• xxxxx	• xxxxx	• xxxxx	• xxxxx	• xxxx
	Function Name	• xxxxx	• xxxxx	• xxxxx	• xxxxx	• xxxx
	Function Name	• xxxxx	• xxxxx	• xxxxx	• xxxxx	• xxxx
	Cross Cutting Capability	• xxxxx	• xxxxx	• xxxxx	• xxxxx	• xxxx
	Cross Cutting Capability	• xxxxx	• xxxxx	• xxxxx	• xxxxx	• xxxx
	Cross Cutting Capability	• xxxxx	• xxxxx	• xxxxx	• xxxxx	• xxxx

Pacific Northwest National Laboratory

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

1-888-375-PNNL (7665)

www.pnnl.gov