PNNL-37273

Zero Trust Strategies for Chemical, Biological, Radiological, and Nuclear Detection Systems

D.1 Cyber Scenarios

January 2025

Penny McKenzie
Mark Watson
Travis Ashley
Jarrett Zeliff
Ernest Allard
Beau Morton
Aubrie Kendall
Riley Maltos
Ernest Tumanyan
Eshan Singh

U.S. DEPARTMENT OF ENERGY

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

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

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

Zero Trust Principles for Chemical, Biological, Radiological, and Nuclear Detection Systems

D.1 Cybersecurity Scenarios

January 2025

Penny McKenzie
Mark Watson
Travis Ashley
Jarrett Zeliff
Ernest Allard
Beau Morton
Aubrie Kendall
Riley Maltos
Ernest Tumanyan
Eshan Singh

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

Pacific Northwest National Laboratory
Richland, Washington 99354

Summary

The evolving landscape of cybersecurity necessitates a paradigm shift to a Zero Trust (ZT) model, which assumes breaches and continuously verifies trust. This approach reshapes how trust boundaries are established, focusing on identities, devices, networks, applications, and data, rather than solely relying on perimeter defenses such as firewalls. Central to this transformation is the National Institute of Standards and Technology's (NIST) Special Publication 800-207, outlining the Zero Trust Architecture (ZTA), along with Executive Order 14028, which mandates federal agencies to adopt ZT principles. Complementary to these efforts, the Cybersecurity and Infrastructure Security Agency (CISA) developed the Zero Trust Maturity Model (ZTMM), providing a framework with five pillars and three cross-cutting capabilities to guide agencies toward enhanced cybersecurity maturity.

In support of these initiatives, the DHS Countering Weapons of Mass Destruction Office (CWMD) is applying ZT principles to secure Chemical, Biological, Radiological, and Nuclear (CBRN) detection systems. Recognizing the diverse deployment models and network connectivity of these systems—from stationary, non-networked units to mobile, cloud-connected devices—the Pacific Northwest National Laboratory (PNNL) is developing cybersecurity scenarios specifically for CBRN environments. These scenarios examine various configurations and technological capabilities, offering insights into the application of ZTMM pillars in enhancing the security postures of CBRN devices.

The cybersecurity scenarios presented by PNNL are hypothetical, crafted to explore theoretical situations and stimulate discussion on the potential use or compromise of CBRN detection systems in varied contexts. These narratives are illustrative and do not reference any real events or actual networks. Instead, they employ generalized reference models to highlight concepts and potential issues within CBRN security, focusing on how Zero Trust strategies can be adapted to address these challenges effectively. Key components of the scenario framework include:

- **Device Section:** Identifies the make and model of the CBRN detection system and details its detection capabilities to illustrate the application of sensor technologies.

- **Scenario Section:** Presents a fictitious deployment model and a case study of how CBRN detection systems might be utilized in the field.

- **Communication Section:** Discusses the on-board communications and networking capabilities, highlighting how the CBRN detection system collects sensitive data and transmits it over networks.

- **Configuration Section:** Discusses how the CBRN detection system collects sensitive data and transmits network traffic.

- **Zero Trust Pillar & Strategy:** Identifies the applicable relationship to the ZTMM and adapted ZT strategies for the specified cybersecurity scenario.

PNNL's scenario-based approach thoroughly explores how Zero Trust principles can be adapted to the unique demands of CBRN systems. By simulating distinct operational contexts and potential threat vectors, these scenarios identify best practices for securing CBRN devices, ensuring robust access controls, data protection, and continuous monitoring. The insights

derived from these scenarios are crucial for strengthening the Zero Trust security posture of CWMD's CBRN devices, enabling proactive identification of weaknesses that can lead to potential vulnerabilities and improved resilience against cyber threats.

Acronyms and Abbreviations

ALARA	As Low As Reasonably Achievable
CBRN	Chemical, Biological, Radiological, and Nuclear
CISA	Cybersecurity and Infrastructure Security Agency
CWA	Chemical Warfare Agents
CWM	Countering Weapons of Mass Destruction
EO	Executive Order
FCEB	Federal Civilian Executive Branch
FTI	Fourier Transform Infrared
LTE	Long Term Evolution
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PDA	Personal Digital Assistant
PNNL	Pacific Northwest National Laboratory
REBS	Rapidly Employable Bio-identification System
RIID	Radioisotope Identification Device
SAM	Spectroscopic Advanced Measurement
TIC	Toxic Industrial Chemicals
TIMON	Toxic Industrial Monitor
TLS	Transport Layer Security
VPN	Virtual Private Network
ZT	Zero Trust
ZTA	Zero Trust Architecture
ZTMM	Zero Trust Maturity Model

Contents

1.0 Introduction

Zero Trust (ZT) represents a transformative shift in cybersecurity management, emphasizing an “assume breach” mentality rather than the traditional “trust but verify” approach. This shift encourages organizations to reevaluate how trust boundaries are established within their networks. Historically, these boundaries relied heavily on perimeter defenses like firewalls. Once inside the perimeter, users were often automatically trusted, which has led to more significant vulnerabilities over time. A misconfigured firewall or a zero-day exploit could allow a threat actor access to critical resources. Zero Trust addresses this challenge by redefining trust boundaries around identities, devices, micro-segmented networks, applications, and data.

In 2020, the National Institute of Standards and Technology (NIST) published the Special Publication (SP) 800-207 [2] on Zero Trust Architecture (ZTA) as part of a broader strategy to modernize federal cybersecurity, aligning with the Federal Information Security Modernization Act [3]. This publication introduced seven fundamental principles for ZTA. Building on this foundation, Executive Order (EO) 14028 [4] was enacted in 2021, mandating that all federal agencies conform to a standardized level of ZT. The Office of Management and Budget (OMB) followed up with the M-22-09 memorandum, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,” [5] which required Federal Civilian Executive Branch (FCEB) agencies to develop ZT implementation guidance by the end of FY24. The NIST SP 800-207 framework served as the cornerstone for these efforts, with individual agencies tailoring guidance based on their unique assets.

For the U.S. Department of Homeland Security, the Cybersecurity and Infrastructure Security Agency (CISA) introduced the Zero Trust Maturity Model (ZTMM) [1]. This model is structured around five key pillars: identity, devices, networks, applications and workloads, and data, alongside three cross-cutting capabilities: visibility and analytics, automation and orchestration, and governance. The ZTMM offers a framework for assessing current ZT capabilities and planning improvements, enabling organizations to achieve higher levels of ZT maturity based on these eight foundational principles. Crucially, the ZTMM applies across all critical infrastructure sectors, serving as cross-agency guidance.

The DHS Countering Weapons of Mass Destruction Office (CWMD) employs Chemical, Biological, Radiological, and Nuclear (CBRN) detection systems to mitigate threats involving hazardous substances. Zero Trust (ZT) principles, as outlined in OMB M-22-09 and supported by CISA's ZTMM, can enhance the security framework of these detection systems. However, the integration of ZT with CBRN systems presents challenges due to the varied deployment models and technological capabilities. Some CBRN systems are stationary with no network connectivity, while others are mobile, streaming real-time data to cloud-based infrastructures. Therefore, understanding the application of ZTMM pillars to CBRN systems involves analyzing archetypical deployments and network architectures, facilitated by the development of tailored cybersecurity scenarios. These scenarios, akin to the “device scenarios” published in PNNL-36036, Application of Zero Trust Cybersecurity to CWMD Device Scenarios [6], provide critical insights into adapting ZT strategies for diverse CBRN environments. By considering these device scenarios, we can ensure that each CBRN detection system adheres to ZT principles, regardless of its operational context or connectivity model.

2.0 Zero Trust Strategies Tailored for CBRN

This section delves into the five pillars of the Zero Trust Maturity Model (ZTMM) and presents a representative set of Zero Trust (ZT) strategies tailored for supporting CBRN devices and systems. Below, the core ZT strategies are highlighted in bold. While these strategies do not directly correspond to the specific functions outlined in the ZTMM, they offer a hybrid perspective that integrates some of the fundamental principles and technical concepts from the ZTMM functions across each pillar. The list of ZT strategies for each pillar is not exhaustive, meaning each CBRN device will not have a complete ZTMM profile. Instead, these strategies are abstracted principles derived from the ZTMM functions and cross-cutting capabilities, intended for a preliminary assessment of the high-level technological capabilities of CBRN detection systems. These core functions are summarized to enhance the security posture of CBRN devices and systems.

2.1 Identity Pillar

CBRN detection systems must ensure robust verification of operator identities when accessing the devices. This can be implemented through integrated graphical user interfaces or via connections established through smart devices. Additionally, the data repository, which stores collected data, should authenticate identities before allowing access to cloud resources. A critical aspect for the identity pillar relates to the methods used for authentication and access control.

Trust boundaries should be defined based on user identities, allowing access to resources appropriate to their roles. Identity and access management typically relies on a combination of authentication credentials and visibility mechanisms. For CBRN systems, it is important that identities are specifically linked to the operators managing the equipment.

- **User Authentication:** CBRN devices should employ mechanisms such as multi-factor authentication (MFA) to ensure only authorized personnel can access or operate the equipment.
- **Identity Management:** Permissions should be aligned with risk-based attributes, including user roles, to restrict access within CBRN systems to only the necessary functions.
- **Visibility and Analytics Capability:** Continuous identity verification is crucial, with systems in place to monitor user behavior patterns. This helps detect anomalies that may indicate potential credential compromise or unauthorized access.

2.2 Devices Pillar

Secure configuration of CBRN detection systems should align with the established trust boundaries surrounding these devices. Each device must be configured to function securely within its deployment environment. This involves hardening device settings by blocking unnecessary ports and services while maintaining endpoint detection and monitoring capabilities. Device-level authentication plays a vital role in ZT strategies, as detailed in the accompanying cybersecurity scenarios.

Effective asset management is crucial for identifying and safeguarding devices within the network, along with addressing their unique requirements. By defining trust boundaries around CBRN devices, verification processes can ensure that only authenticated identities access these resources.

- **Resource Access:** Implement device authentication and authorization to ensure that all CBRN devices authenticate themselves before network access, preventing unauthorized or rogue connections.
- **Endpoint Threat Detection and Response:** Emphasize that devices are consistently updated, patched, and compliant with security policies before they are granted access to network resources.
- **Device Detection and Compliance:** Apply compliance-aligned configurations and hardening practices, such as disabling unnecessary services and ports to prevent exploitation.
- **Safe Device Pairing:** Conduct device pairing in a secure environment before deploying to incident sites, significantly mitigating the risk of man-in-the-middle attacks during the pairing process.

2.3 Networks Pillar

Key ZT mechanisms within the Network pillar focus on network segmentation and the use of encryption across trust boundaries. CBRN detection systems, when connected to networks or integrated with building control systems, benefit significantly from network segmentation. This technique isolates these critical environments and secures communications for collected data. CBRN devices may connect to a building’s infrastructure or communicate via wireless networks. Under a ZT model, all network traffic within the perimeter should be secured and thoroughly examined, operating under the assumption that a breach has already occurred.

- **Network (Macro) Segmentation and Micro-Segmentation:** Demonstrate the separation of CBRN devices into dedicated network segments and service-specific segments to effectively manage data flow and minimize exposure to potential threats.
- **Traffic Encryption:** After mapping data flows to understand where data is stored and processed, prioritize the use of encryption protocols to safeguard data in transit between CBRN devices and control systems, protecting it from interception and tampering.
- **Visibility and Analytics Capability:** Implement continuous network monitoring through real-time monitoring and intrusion detection systems to effectively identify and respond to any suspicious network activities involving CBRN devices.

2.4 Applications and Workloads Pillar

Managing application security involves establishing trust boundaries around access points. For CBRN devices, applications are often the primary mechanism for data collection and transfer, underscoring the critical importance of accessibility and security. Therefore, ZT principles should be applied to these applications to protect sensitive information effectively.

- **Application Authorization and Access:** Utilize continuous access authorization with real-time risk analysis and behavioral analytics to prevent unauthorized access to CBRN applications.

- **Secure Application Development and Deployment:** Ensure that applications for CBRN devices are developed using secure coding practices to prevent vulnerabilities such as code injection or buffer overflows. Additionally, employ continuous integration and delivery practices to maintain ongoing security improvements.

- **Application Threat Protections:** Implement measures like application whitelisting for CBRN devices, limiting them to run only approved and signed applications, thereby preventing the execution of unauthorized software.

- **Application Security Testing:** Conduct regular updates, patch management, and periodic security testing to ensure that applications and workloads on CBRN devices are up to date. Promptly apply patches to address any security vulnerabilities.

- **Accessible Applications:** Ensure that authorized users and devices can access necessary applications without compromising security.

2.5 Data Pillar

CBRN devices collect sensitive information, which may be stored on the device or transmitted to centralized repositories. Securing communications is crucial to protect this data in both scenarios. By drawing trust boundaries around the data, additional verification is required for access to ensure its security and integrity.

The sensitive data collected by CBRN detection systems must be protected and accessible only to authorized users. This is typically achieved at a minimum through encryption and identity verification of users attempting to access data resources using access controls.

- **Data Encryption:** Ensure that sensitive data collected or stored by CBRN devices is encrypted, safeguarding confidentiality, and preventing unauthorized access both at rest and during transmission.

- **Visibility and Analytics Capability:** Implement data integrity checks using methods like checksums, hashes, or digital signatures to verify the integrity of data processed by CBRN devices, detecting any unauthorized alterations.

- **Data Access Control:** Enforce strict access permissions and maintain thorough auditing for sensitive data to ensure that only authorized personnel can view or manipulate critical information.

- **Data Availability and Loss Prevention:** Utilize redundant data stores to maintain access to historical data and implement data loss prevention solutions to ensure continued availability.

3.0 Integration of Mobile Communication Technologies for CBRN Devices

The integration of dedicated mobile applications for Chemical, Biological, Radiological, and Nuclear (CBRN) devices allow users to modify settings such as detection thresholds, alert configurations, and operational modes through a user-friendly interface. These advanced communication technologies enhance the management and operational efficiency of CBRN devices.

Mobile applications enable quick and efficient adjustments to device parameters through Bluetooth, Wi-Fi, or other wireless technologies. This instant connectivity establishes a connection with the device, minimizing downtime and operational interruptions. Changes made on the application are synchronized with the device immediately, ensuring it operates with the most current settings. Users can also manage and adjust device settings remotely, providing flexibility for field operations where direct access to the device is not feasible. Mobile applications offer advanced functionalities such as built-in diagnostic tools for troubleshooting and monitoring device health, user permissions, access levels, data management, logging, and storing of data.

- ***Bluetooth:*** Configuration changes can be made through direct pairing with a smartphone, tablet, or other Bluetooth-enabled devices. This connection starts by launching a dedicated app designed to interface with the CBRN device. Once the app is launched, the user initiates the pairing process, establishing a wireless Bluetooth connection between the devices. This connection enables users to make necessary adjustments to the device settings, supporting immediate configuration management and ensuring rapid response to changing conditions.

- ***Cloud/Web Portal:*** CBRN devices offer cloud-based web portals that can be managed using cell phones, tablets, or laptops through dedicated apps and can be managed by the manufacturer. These web portals, accessible from any internet-connected device, provide a centralized platform for device management. By using dedicated apps, users can log in to the cloud-based portals to view the status of their CBRN devices and make configuration changes as needed. This setup allows for quick access and real-time monitoring, ensuring that the devices function correctly and respond to current conditions. The cloud infrastructure supports real-time monitoring capabilities, enabling users to oversee multiple devices simultaneously. This approach enables the managing of CBRN devices and allows for prompt implementation of configuration changes and updates across all connected devices.

- ***Remote Updates:*** Remote updates can be managed using cell phones, tablets, or laptops through dedicated apps. For sophisticated remote management systems, users can push updates to multiple devices concurrently, ensuring all CBRN devices are running the most current software versions. This centralized update mechanism supports proactive measures, maintains optimal performance, and enhances the efficiency of remote device management.

The integration of dedicated mobile communication technologies for CBRN devices should align with Zero Trust principles across the key pillars.

- ***Identity Pillar:*** strong authentication like multi-factor authentication (MFA) is essential, yet not all systems enforce it, potentially leaving vulnerabilities.

- ***Devices Pillar:*** requires secure and authenticated connections between mobile devices and CBRN devices, which some legacy systems lack.

- ***Network Pillar:*** relies on encrypted communications to protect data, though inconsistent implementation can present risks.

- ***Applications and Workloads Pillar***: only vetted applications should be used, but the presence of unauthorized applications can undermine security.

- ***Data Pillar:*** requires robust logging and encryption practices, yet data management often falls short in comprehensive logging and monitoring.

Transitioning to practical applications, we explore how these principles should be implemented in various Zero Trust cybersecurity scenarios, demonstrating the need of a Zero Trust approach in real-world contexts.

4.0 CBRN Zero Trust Cybersecurity Scenarios

The cybersecurity scenarios detailed in this section are hypothetical and intended solely for illustrative purposes. They have been carefully crafted to explore theoretical contexts and stimulate discussion on the various ways CBRN detection systems might be utilized or compromised. These narratives do not refer to actual events or existing networks but instead utilize generalized reference models to focus on concepts and potential issues within the realm of CBRN security.

By employing these hypothetical scenarios, we highlight the use cases and challenges associated with integrating cyber technologies into CBRN detection systems. This approach allows for a comprehensive examination of potential risks and vulnerabilities without being tied to specific devices or incidents. It encourages discussion that emphasizes critical thinking and proactive strategies for enhancing cybersecurity measures, all while maintaining confidentiality and avoiding unintended connections to real-world situations.

Each cybersecurity scenario is anchored around a deployable CBRN detection system and follows a standardized format for consistency. The “Scenario” section presents a fictitious, hypothetical deployment model and a case study of how the CBRN detection systems might be used in the field. The “Communication” section discusses the on-board communications and networking capabilities. The “Configuration” section includes how the CBRN detection system collects sensitive data and transmits network traffic. Finally, the “Zero Trust Pillar & Strategy” section identifies the applicable relationship to the ZTMM and adapted ZT strategies for the specified cybersecurity scenario.

4.1 Handheld Radioisotope Identification Device

Device: Handheld Radioisotope Identification Device (RIID)

Scenario: In efforts to enforce nuclear non-proliferation, RIID devices can be used for routine screenings in New York City’s subway systems. While some stations are equipped with stationary radiation portal monitors, officers also require handheld devices to conduct scans beyond fixed checkpoints and throughout the subway system. These officers can utilize these handheld RIIDs, can integrate with an Android smartphone for the graphical user interface via Bluetooth and uses location services for GPS tracking and mapping radiation data. When suspicious materials are identified within the subway system, RIIDs can be used to scan for radiation while maintaining safety protocols such as ALARA (“As Low As Reasonably Achievable”). To minimize exposure, officers may need to maintain a safe distance from potential radioactive sources. By connecting smartphones wirelessly through Bluetooth, operators can remain several meters away. The RIID can be positioned remotely to scan suspicious material while the smartphone is used to operate it at a distance. Data collected from the RIID can be transferred to a workstation for analysis or, alternatively, RIID devices with mobile technologies (i.e., smartphone or other mobile application) can connect over Wi-Fi or 4G LTE to email the data to a central repository. To ensure the integrity and security of data transmissions, continuous network monitoring is employed to detect unauthorized access or anomalies in communication channels, and Transport Layer Security (TLS) v1.3 is used for secure wireless communications.

Communications: The use of TLSv1.3 ensures that network communications are encrypted when transmitting over cellular or Wi-Fi connections, maintaining the integrity and security of the network environment. With Bluetooth capability, SAM can pair with multiple smartphones, thanks to newer Bluetooth versions that support multi-pairing.

Configuration: Identity management for SAM is facilitated through the mobile device's login interface. For real-time data streaming to the cloud, authentication is required to access the database for uploading collected data. This underscores the critical role of credential management for both RIID and mobile devices interfacing with cloud-based systems as central data repositories.

Zero Trust Pillar & Strategy: Based on this cybersecurity scenario, the following ZT pillars and strategies were identified:

- Identity – User Authentication; Identity Management
- Devices – Safe Device Pairing
- Networks – Traffic Encryption
- Applications and Workloads – Application Authorization and Access
- Data – Data Availability and Loss Prevention

4.2 Spectroscopy Gas Analyzer

Device: Portable Spectroscopy Gas Analyzer.

Scenario: Late one night at a chemical storage facility, a security guard notices a strange odor and promptly alerts the HAZMAT team. Equipped with an Fourier Transform Infrared (FTIR) gas analyzer, the team arrives to evaluate the situation. From a secure distance, the team leader connects the portable device to a rugged personal digital assistant (PDA) device via Bluetooth, allowing real-time monitoring of gas levels. Suddenly, the PDA displays dangerous chemical readings and triggers an alert mechanism prompting an automated response for an emergency evacuation. However, no visible signs of a leak are present. Unbeknownst to the team, a cybercriminal has compromised the Bluetooth communications channel, injecting false data to create undue panic. Meanwhile, at the command center, analysts try to perform further diagnostics by connecting the portable device to a PC, only to discover the USB interface is not secured. Access to the USB port presents a hardware limitation and weakness that leads to a vulnerability. Exploiting this vulnerability, the attacker manipulates stored data to conceal their activities. To prevent such incidents, it is critical to ensure secure Bluetooth pairing, encrypted data transfers, and stringent device authentication for safe and uninterrupted operations.

Communication: The portable FTIR gas analyzer utilizes Bluetooth for wireless operations. It is primarily controlled through a PDA running Windows Mobile Professional, which communicates with the analyzer via Bluetooth, enabling wireless functionality.

Configuration: The PDA is equipped with FTIR gas analyzer software, providing a user-friendly interface for instrument control, real-time data monitoring, and diagnostics. For enhanced capabilities, the portable device could also be connected to a Windows-based PC.

Zero Trust Pillar & Strategy: Based on this cybersecurity scenario, the following ZT pillars and strategies were identified:

- Identity – User Authentication
- Devices – Safe Device Pairing
- Applications & Workloads – Accessible Applications

4.3 Wearable Radioisotope Identification Device

Device: Wearable Radioisotope Identification Device

Scenario: During a New Year's Eve celebration in a major city, local law enforcement is equipped with a wearable RIID device, which functions as a small personal radiation detector (PRD) device, to enhance radiological threat detection amid the large crowds. As the festivities unfold, an officer receives an alert on their connected smartphone, indicating a potential radiological source via the discreetly carried wearable device. The officer communicates the alert to the command post without disturbing the public, relying on the device's secure Bluetooth connection to stream real-time data. Backup arrives, and the team cautiously moves the crowd away to investigate further. The RIID detection device enters confirmation mode, identifying the detected isotope as benign, stemming from a harmless source.

Throughout the event, the wearable device enables officers to maintain a vigilant security presence, ensuring the celebration remains safe and secure for all attendees.

Communication: The wearable RIID interacts with the user's connected smartphone, allowing for adjustment of settings, monitoring of readings, and performing firmware updates as needed. Data is streamed from the wearable RIID device to the mobile device's display, providing status updates and alerts regarding the sensor and any detected radiological sources. Connectivity via Bluetooth or USB underscores the importance of secure device authentication and communication to prevent unauthorized access. Users are encouraged to consistently perform firmware updates and secure configurations to mitigate vulnerabilities.

Configuration: Compact enough to fit in a user's pocket, these devices are designed to efficiently detect radiological signals nearby. They are set for continuous automatic scanning and transmit real-time radiological data to the connected mobile device. Upon detecting a radiation source, the device can switch to confirmation mode to accurately identify the detected isotope.

Zero Trust Pillar & Strategy: Based on this cybersecurity scenario, the following ZT pillars and strategies were identified:

- Identity – User Authentication
- Devices – Safe Device Pairing
- Networks – Traffic Encryption
- Applications & Workloads – Accessible Applications

4.4 Tabletop Biofluorescence Biological Detection and Identification System

Device: Tabletop Biofluorescence Biological Detection and Identification System

Scenario: On a busy holiday weekend in a mailroom, staff members are equipped with an automated biological detection and identification device centrally staged in the mail operations area due to increased concerns of biological threat agents being sent through the mail system. The device is utilized to detect potentially harmful pathogens before personnel meet them, ensuring their safety. The device conducts automated testing using bioassay tickets, which allows for uninterrupted sampling over several months. This continuous monitoring is crucial in quickly identifying and responding to any biological threats, providing an essential layer of safety for mailroom operations during peak periods.

Communication: Bio detection data is transmitted through an Ethernet connection to an onboard computer. This setup underscores the need for secure interfaces and protocols to protect the integrity and confidentiality of the data. The onboard system is potentially vulnerable to cyber threats, particularly if devices are left unattended for extended periods without receiving security updates.

Configuration: Secure configuration is crucial for the biological detection and identification device, especially during long periods of unattended operation. Mailroom personnel may not notice abnormal behavior or faults, making the device susceptible to tampering that could interfere with data communications without being detected**.**

Zero Trust Pillar & Strategy: Based on this cybersecurity scenario, the following ZT pillars and strategies were identified:

- Devices – User Authentication (Access Control)
- Applications and Workloads – Application Authorization and Access

4.5 Passive Toxic Chemical Air Monitoring System

Device: Passive Toxic Chemical Air Monitoring System

Scenario: A network of passive toxic chemical air monitor system devices is deployed at an industrial complex to detect toxic industrial chemicals (TICs) and chemical warfare agents (CWAs) at low detection levels. These devices are strategically positioned near storage warehouse air ventilation systems and key locations such as the storage areas, operational control rooms, and equipment maintenance zones to ensure comprehensive chemical monitoring.

In the centralized control room, operators use a secure web interface to receive real-time data from the chemical detection system. The operators can quickly identify chemical threats, assess sensor readings, and respond effectively to safeguard personnel and the facility. When a threat is detected, the toxic chemical air monitoring system can automatically activate ventilation protocols or isolate affected areas, mitigating potential harm.

This deployment ensures a rapid and coordinated response to chemical threats, reinforcing the base's safety measures with advanced detection and autonomous corrective action capabilities.

Communication: TIC and CWA monitoring is conducted in real-time through a web interface that transmits data to a remote computer in a centralized control room. Operators in the control room can use the interface to assess current sensor readings, identify detected substances, log data, and adjust settings as needed. This setup ensures efficient management of the safety system. Communication between the chemical detection devices and the control room is secured through an encrypted web interface to protect sensitive CBRN data.

Configuration: The toxic chemical air monitor system’s capability to autonomously activate environmental controls highlights the importance of network segmentation to manage data flow and reduce exposure to threats. It can be configured to operate in autonomous mode, enabling automatic responses such as activating ventilation protocols or redirecting airflow to mitigate potential airborne threats. The web user interface can also be integrated with other building control systems to effectively manage air ventilation based on detected conditions.

Zero Trust Pillar & Strategy: Based on this cybersecurity scenario, the following ZT pillars and strategies were identified:

- Identity – User Authentication
- Devices – Endpoint Threat Detection and Response
- Networks – Encrypted Communication
- Applications and Workloads – Secure Application Development and Deployment

4.6 Rapid and Autonomous Bio identification System

Device: Rapid and Autonomous Bio identification System

Scenario: At a busy international airport, several rapid and autonomous bio identification system devices are deployed as essential elements of the airport's security infrastructure to monitor for airborne biological pathogens and threats. These units are strategically installed near ventilation systems and in high-traffic areas such as terminals and boarding gates.

As passengers move through the airport, the bio identification system continuously analyzes the air for pathogens in real time. This constant monitoring is critical for early detection of potential biological threats, enabling the airport to respond swiftly to any detected pathogens. Upon identification of a possible threat, the bio identification system immediately alerts airport security and health response teams through its central control room communication system.

The system's rapid response capabilities allow for the immediate implementation of safety protocols, such as isolating affected areas, adjusting ventilation, and enhancing air filtration systems to prevent the spread of pathogens. These measures not only protect the health and safety of travelers and staff but also help maintain the smooth operations of the airport by minimizing disruptions.

Communication: The bio identification system transmits data to a central control room through cellular, Ethernet, or Wi-Fi connections. When a potential biological threat is detected, the system automatically alerts response teams and initiates predefined safety protocols, such as isolating affected areas and enhancing air filtration systems to mitigate the spread of pathogens. The bio identification system is designed to be lightweight and low power, requiring minimal maintenance and service updates.

Configuration: The bio identification system is configured to begin monitoring and transmitting data once powered on, eliminating the need for operator intervention. Sampling rates can be adjusted according to operational needs, allowing for flexible and efficient monitoring tailored to different risk environments**.**

Zero Trust Pillar & Strategy: Based on this cybersecurity scenario, the following ZT pillars and strategies were identified:

- Identity – User Authentication (Access Control)
- Networks – Encrypted Communications
- Applications and Workloads – Secure Application Development and Deployment
- Data – Data Encryption

4.7 Portable Radioisotope Identification Device

Device: Portable Radioisotope Identification Device

Scenario: In preparation for a marathon in a large city, authorities receive intelligence suggesting the possibility of a nuclear threat. To counter this, they deploy the handheld RIID devices throughout the urban environment to scan for radiological threats. These handheld devices are supported by multiple charge packs to extend the lifespan of surveillance operations. Additionally, the device's ability to perform remote viewing operations using GPS and reach back via web applications allows for seamless coordination across different deployment locations. This feature enables authorities to efficiently cover more ground, enhancing their ability to detect and respond to potential threats swiftly.

Communication: The handheld RIID device is equipped with USB, Bluetooth, and Wi-Fi interfaces to facilitate data transfer and connectivity. It also includes 32GB of internal memory for storing field data, ensuring comprehensive data capture during operations.

Configuration: To ensure operational integrity, the handheld RIID device relies on a secure onboard webserver application and web interface for interacting with sensor readings. These applications and interfaces must undergo regular security assessments and updates to address potential vulnerabilities, ensuring the device remains secure and effective in detecting radiological threats.

Zero Trust Pillar & Strategy: Based on this cybersecurity scenario, the following ZT pillars and strategies were identified:

- Identity – User Authentication

- Applications and Workloads – Application Authorization and Access; Application Threat Protections

4.8 Portable Gas Analyzer

Device: Portable Gas Analyzer

Scenario: At a critical infrastructure site, a staff member reports the suspicion of a gas leak. In response, first responders are dispatched with the portable multi-gas analyzer to identify and measure any potential hazardous gases present. The portable multi-gas analyzer device is quickly set up to scan the affected area, while responders maintain a safe distance by controlling the device with a tablet. This setup allows them to perform real-time analysis of gases such as hydrogen sulfide, ammonia, and methane, which could pose a risk to onsite workers.

As the device analyzes the air, it provides immediate feedback on the presence and concentration of any hazardous gases. This rapid identification is crucial for first responders to assess the severity of the situation and determine appropriate countermeasures to protect those at the site. The portable multi-gas analyzer's ability to be stationed for continuous measurement also ensures ongoing monitoring while the situation is addressed.

Communication: Data from the portable multi-gas analyzer can be accessed through USB, Ethernet, Bluetooth, and Wi-Fi connections. The device can be remotely operated using a virtual private network (VPN) via a workstation or supplied tablet running proprietary software. This software generates alerts if hazardous compounds are detected, facilitating immediate response actions.

Configuration: The portable multi-gas analyzer relies on proprietary software and VPNs for remote interaction and alerting users to potential threats. This setup underscores the importance of applications in guiding workflows for detecting and responding to hazardous materials, ensuring personnel receive timely notifications of any detected risks.

Zero Trust Pillar & Strategy: Based on this cybersecurity scenario, the following ZT pillars and strategies were identified:

- Applications and Workloads – Traffic Encryption & Data Mapping

4.9 Portable Handheld Gamma Spectrometer

Device: Portable Handheld Gamma Spectrometer

Scenario: At Border Patrol checkpoints, the portable handheld gamma spectrometer plays a crucial role during cargo inspections for radiological detection. Positioned strategically near inspection bays, the spectrometer device offers real-time identification and analysis of radioactive materials, aiding compliance with safety protocols. Its high-resolution gamma spectrometry allows for precise isotope identification, enabling swift and accurate threat assessments as shipments cross the border.

Using the spectrometer device, officers can quickly screen cargo for any radiological threats, providing comprehensive spectrometry data that informs their decision-making process. This capability ensures that potentially hazardous materials are identified and addressed efficiently, minimizing risks and maintaining border security.

Communication: The handheld spectrometer transmits critical radioactive material data through Bluetooth and Wi-Fi to a centralized command system. To protect this data from unauthorized access or interception, encryption is used during transmission. Measures such as checksums or digital signatures are implemented to verify data integrity, ensuring it remains unaltered. Strict access controls are also enforced, permitting only authorized personnel to access sensitive information, and ensuring compliance with safety protocols.

Configuration: Operators configure the device and its communication settings directly on the spectrometer device, utilizing its wireless capabilities to transmit spectrometry data to the central command system. This setup fosters effective collaboration between on-site teams and remote analysts, allowing for timely decision-making and ensuring any potential threats are addressed promptly. The integrated approach enhances the efficiency and effectiveness of radiological threat detection at border checkpoints.

Zero Trust Pillar & Strategy: Based on this cybersecurity scenario, the following ZT pillars and strategies were identified:

- Identity – User Authentication
- Devices – Safe Device Pairing
- Networks – Encrypted Communications
- Applications and Workloads – Application Authorization and Access; Regular Updates and Patch Management
- Data – Visibility and Analytics Capability

4.10 Fixed-Site Spectroscopic Portal Monitoring System

Device: Fixed-Site Spectroscopic Portal Monitoring System

Scenario: An industrial facility on the outskirts of a city deploys a fixed-site spectroscopic portal monitoring system to ensure robust perimeter security. This monitoring system is used to monitor pedestrians and vehicles for radioactive materials using a series of detector modules. To maximize coverage, gamma and neutron detector modules are strategically mounted around the facility's perimeter. Wi-Fi is employed as the primary communication method for data transmission between the detectors and the supervisor monitoring system, making network security a top priority.

A technician manages the operation of the spectroscopic system through a web interface on a laptop running Windows 10 with proprietary software. This setup allows the technician to configure the system for visible and audible alarms and provides options for viewing dose rate measurements, count rates, or spectral plots. With Wi-Fi enabled, data is transmitted to a supervisor computer, where personnel actively monitor for radiological threats.

Communication: The portal monitoring system relies extensively on Wi-Fi for transmitting sensitive information about radiological threats between the detector modules and the central monitoring system. Ensuring that this data is encrypted during transmission is vital to prevent unauthorized access or interception, preserving the integrity and confidentiality of the information.

Configuration: Technicians use specialized software to configure the system's alarms, dose rate measurements, and spectral plots, thus managing sensitive data. Implementing data integrity checks is essential to maintain accuracy, ensuring that the data remains correct and unaltered during both transmission and storage. This comprehensive approach enhances the facility's ability to detect and address potential radiological threats effectively.

Zero Trust Pillar & Strategy: Based on this cybersecurity scenario, the following ZT pillars and strategies were identified:

- Data – Data Availability and Loss Prevention
- Applications & Workloads – • Application Authorization and Access, Accessible Applications

5.0 Conclusion

The cybersecurity scenarios for CBRN detection systems were designed to illustrate specific examples of Zero Trust (ZT) functions and strategies from a device-centric perspective, focusing on the ZT pillars: Identity, Devices, Networks, Applications and Workloads, and Data. These scenarios were not based on real-world networks and are not intended to represent actual implementations. Instead, they were constructed using segmented technical concepts to develop high-level archetypes of ZT principles. These cybersecurity scenarios serve as potential use cases to facilitate discussions on configuring CBRN devices to align with ZT pillars. By employing these hypothetical scenarios, the use cases and challenges associated with integrating cyber technologies in CBRN devices are highlighted.

The outlined next steps represent a strategic approach to strengthening the security of CBRN devices through Zero Trust principles. This ensures a robust defense against potential threats and effective management of security incidents, contributing to a stronger overall security posture.

1. **Develop a Device Manual Zero Trust Taxonomy:** We will create a comprehensive taxonomy specific to CBRN devices, detailing Zero Trust (ZT) principles and controls applicable at the device level. This taxonomy will provide a structured reference for implementing ZT strategies across diverse CBRN systems, ensuring consistency and clarity in our security measures.

2. **Identify Zero Trust Security Controls:** We will map out specific security controls that align with ZT principles for each CBRN device type. This includes controls related to identity verification, access management, network segmentation, data encryption, and device configuration. Clear guidelines will be defined to implement and enforce these controls consistently across the organization.

3. **Develop a Zero Trust Playbook:** We will create a detailed playbook outlining procedures and protocols for implementing and maintaining ZT security measures in CBRN environments. The playbook will include scenarios for incident response, mitigation strategies, and contingency planning, enabling personnel to respond effectively to security incidents.

4. **Test Zero Trust Controls:** We plan to conduct systematic testing of ZT controls across CBRN devices to evaluate their effectiveness and identify potential gaps. This process will involve simulated attacks and stress tests to ensure that the controls can withstand various threat scenarios, maintaining the integrity, confidentiality, and availability of device operations.

The comprehensive plan to enhance the security of CBRN detection systems through the implementation of Zero Trust (ZT) principles marks a critical evolution in securing sensitive environments. By developing a device manual zero trust taxonomy, systematically testing zero trust controls, identifying, and mapping relevant security measures, and creating a detailed zero trust playbook, a strong foundation is established for robust threat detection and mitigation. Focusing on operational readiness and proactive security strategies ensures that systems not only withstand current threats but are adaptable to future challenges.

As part of future development efforts, the creation of a web-based tool for logging and analyzing security data will provide CWMD with centralized, efficient capabilities for real-time monitoring, prompt alerting, and comprehensive reporting. This tool will empower CWMD to maintain an up-to-date security posture through actionable insights, ultimately enhancing the capacity to respond to and manage security incidents effectively. The transfer of this tool to CWMD will be conducted seamlessly, with thorough documentation and training provided, enabling a smooth transition, and ensuring that these advanced security capabilities are fully integrated into operations.

6.0 References

[1] 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.

[2] Federal Information Security Modernization Act (FISMA) of 2014 (Public Law 113-283; December 18, 2014). https://www.govinfo.gov/content/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf

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

[4] Office of Management and Budget (OMB), Executive Office of the President. Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 26, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[5] 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.

[6] Pacific Northwest National Laboratory (PNNL). Application of Zero Trust Cybersecurity to CWMD Device Scenarios, PNNL-36036. May 2024.

[16] Bubble Technology Industries FlexSpec X8400. https://www.bubbletech.ca/product/flexspec-fixed-site-system/

Pacific Northwest National Laboratory

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

1-888-375-PNNL (7665)

www.pnnl.gov