CYBERSECURITY FOR THE NUCLEAR INDUSTRY

A WHITEPAPER ON HONEYWELL'S CYBERSECURITY SOLUTIONS FOR NUCLEAR REGULATIONS

Written by the Honeywell Connected Enterprise Team

2023

Honeywell

TABLE OF CONTENTS

ABSTRACT

Nuclear power plants are critical infrastructure facilities that require high levels of security to protect against potential cyber attacks. In recent years, there has been growing concern about the vulnerability of nuclear power plants to cyber threats, as well as an increase in the number and sophistication of cyber attacks targeting these facilities. The state of cybersecurity in nuclear power plants varies widely across the globe, with some countries implementing robust security measures and others lagging behind.

Many nuclear power plants rely on legacy systems and equipment that were not designed with cybersecurity in mind, making them vulnerable to cyber attacks. Additionally, the increasing use of digital technology in nuclear power plants, such as automation and remote monitoring, has created new avenues for cyber attacks. To address these challenges, many countries have developed cybersecurity regulations and guidelines specifically for nuclear power plants, and some have established dedicated cybersecurity teams to monitor and respond to potential threats.

However, despite these efforts, nuclear power plants continue to face significant cybersecurity challenges. Some of the key challenges include the difficulty of patching and updating legacy systems, the lack of cybersecurity expertise among nuclear plant personnel, and the potential for cyber attacks to disrupt critical safety systems. As the reliance on digital technology in nuclear power plants continues to increase, addressing these challenges will be essential to ensure the safety and security of these critical facilities.

THE NUCLEAR REGULATORY COMMISSION (NRC) CYBERSECURITY DEFINES REQUIRENTS

The Nuclear Regulatory Commission (NRC) is the federal agency responsible for regulating commercial nuclear power plants and other nuclear facilities in the United States. The NRC has established a set of cybersecurity regulations designed to help protect nuclear power plants against cyber attacks and improve the safety and security of these facilities. These regulations are known as the Cybersecurity Plan (CSP) and are described in detail in the NRC's Regulatory Guide 5.71.

The NRC's CSP regulations require nuclear facility licensees to implement a comprehensive cybersecurity program that includes:

1. Access controls: Limiting access to critical digital assets to authorized personnel only.

2. Incident response and recovery: Establishing plans and procedures for responding to and recovering from cybersecurity incidents.

3. Information protection: Safeguarding digital assets, including sensitive information, from unauthorized access, disclosure, modification or destruction.

4. Monitoring and detection: Monitoring networks and systems for suspicious activity and unauthorized access.

5. Security management: Establishing a cybersecurity program-management framework, including periodic cybersecurity assessments and training programs.

The NRC's CSP regulations also require licensees to report cybersecurity incidents to the NRC promptly, provide notification to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) within a specified time frame and maintain records of cybersecurity events and incidents.

The NRC's cybersecurity regulations are designed to ensure that nuclear facilities are better protected against cyber threats, including those posed by nation-state actors and cyber criminals. The NRC regularly updates its cybersecurity regulations to keep pace with evolving threats and technologies.

1. ABOUT HONEYWELL CYBERSECURITY

As part of Honeywell Connected Enterprise, Honeywell Industrial Cybersecurity (H-ICS) is a global business unit that provides industrial cybersecurity services and solutions for industrial control systems (ICS). Following international industrial cybersecurity standards for automation systems such as IEC 62443, NRC CRP 5.71 and the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (NERC CIP), the H-ICS team has completed over 1,000 ICS-specific cybersecurity projects in a variety of industrial sectors, including nuclear power plants. In addition, team members have contributed to the development of many of these standards. With a global team of more than 100 specialists, industrial cybersecurity laboratory facilities and patented products, H-ICS is a major international player in this dynamic field that requires expertise in cybersecurity and process automation. This unique combination of skills forms the basis for the provision of services for a wide range of industrial control systems.

- Many members of the H-ICS team are certified professionals with a rare combination of years of experience in process control and cybersecurity as well as advanced cybersecurity credentials in both IT and OT environments.
- The Honeywell team has extensive experience with IEC 62443 compliance and other industry-specific regulations such as NERC-CIP and NRC 5.71, as well as experience delivering projects and services in customer ICS environments to implement cybersecurity projects designed to help nuclear power plants mitigate critical cybersecurity risks.
- Access to its Cybersecurity Center of Excellence (CoE) – State-of-the-art labs for testing and research with specialized capabilities and knowledge of control system-specific vulnerabilities and threat intelligence. The labs are located in Atlanta, Dubai and Singapore.

2. HONEYWELL SECURITY SOLUTION FOR NRC 5.71

An essential aspect of the OT Defense-In-Depth strategy is the use of more secure solutions for a standardized approach to the command, control and coordination of emergency response providing a hierarchy within the responders from the various functional business divisions. This Incident Command System (ICS) includes configuring/deploying ICS cybersecurity solutions to minimize their attack surface and enhance protections from unauthorized access in a nuclear power production facility.

Honeywell's current cybersecurity solutions include:

- Cyber risk assessments
- Cybersecurity vulnerability assessment
- OT pen testing
- Access control solutions
- Network monitoring/unidirectional gateways
- USB security solution
- Training and awareness
- DPI/IDS intrusion detection and preventions systems

3. NRC GUIDELINES FOR ASSESSMENTS

The Nuclear Regulatory Commission (NRC) requires nuclear power plant licensees to perform regular cybersecurity assessments, including penetration testing (pen testing), to confirm the current security status of their operational technology (OT) systems.

The NRC has issued various regulatory documents outlining its requirements for cybersecurity assessments and penetration testing. These include:

1. Regulatory Guide 5.71, "Cybersecurity Programs for Nuclear Facilities": This guide provides guidance on developing and implementing cybersecurity programs for nuclear facilities, including requirements for conducting regular cybersecurity assessments and penetration testing.

2. NRC Inspection Procedure 95001, "Cybersecurity Program – Inspection Procedures": This inspection procedure outlines the NRC's inspection process for evaluating a licensee's cybersecurity program, including its penetration testing activities.

3. NRC Information Notice 2016-02, "Cybersecurity Vulnerability Assessment and Penetration Testing at Nuclear Power Plants": This notice provides additional guidance on conducting cybersecurity vulnerability assessments and penetration testing at nuclear power plants, including considerations for scope, methodology and reporting.

In general, the NRC requires licensees to conduct penetration testing of their OT systems at least once every three years. The testing must be performed by qualified personnel using appropriate methods and tools. The scope of the testing should be based on a risk-based approach that takes into account the criticality and complexity of the OT systems being tested.

The NRC also requires licensees to develop and implement a comprehensive cybersecurity program that includes regular cybersecurity assessments, vulnerability management, incident response, and training and awareness programs. The program should be designed to meet the specific needs of the licensee and should be reviewed and updated periodically to ensure its effectiveness.

In summary, the NRC requires nuclear power plant licensees to conduct regular cybersecurity assessments, including penetration testing, of their OT systems to confirm the current security status of their facility. The testing should be based on a risk-based approach and conducted by qualified personnel using appropriate methods and tools. Licensees must also develop and implement a comprehensive cybersecurity program that includes regular assessments, vulnerability management, incident response and training and awareness programs.

[1] https://www.nrc.gov/security/cybersecurity.html
[2] https://www.nrc.gov/docs/ML2109/ML21095A329.pdf

3.1. HONEYWELL CYBERSECURITY RISK ASSESSMENTS

The Honeywell cybersecurity risk assessment is designed to provide a detailed industrial control system (ICS) security assessment to help operators better understand the current state of their protections for their industrial control systems against targeted attacks from skilled, motivated, and well-equipped attackers such as nation-states, terrorist groups, hacktivists and insiders. The service is designed to help operators identify critical ICS risk scenarios and use them as a basis for further analysis. The risk scenarios are designed to identify the risk controls needed to mitigate risk and meet operators' risk appetite and tolerance. Controls are analyzed based on their level of protection, detection and response capabilities.

3.2. HONEYWELL CYBERSECURITY VULNERABILITY ASSESSMENTS

Honeywell professionals can also help nuclear plants perform cybersecurity vulnerability assessments (CSVA) to evaluate their current cybersecurity technologies for their facility and recommend a roadmap for improving the security of industrial control networks so as to meet current standards. This service is designed to help operators achieve industrial cybersecurity goals, including compliance with current industry practices and regulatory standards such as TSA Pipeline, ISA99, NERC CIP, NRC CRP, CFATS and ISO/IEC27001.

The Honeywell CSVA is designed to help ICS operators achieve business goals by:

- Improving asset availability, safety and reliability,
- Reducing downtime and loss of reputation,
- Improving employee skills,
- Improving compliance with corporate and government regulations, and
- Aligning with industry standards and practices.

3.3. HONEYWELL OT PEN TESTING

Honeywell's operational technology (OT) pen testing is the process of testing the security of an organization's industrial control system and other critical OT systems to help a customer identify potential vulnerabilities and potential attack vectors. In the nuclear industry, the Nuclear Regulatory Commission (NRC) requires companies to perform regular OT pen testing to help assess the safety and security of their facilities. This involves testing systems such as SCADA, DCS and PLCs to identify potential weaknesses and vulnerabilities that could be exploited by malicious actors. The results of these tests are then used to strengthen security measures and help a facility comply with NRC regulations.

The likelihood of a successful attack is much lower in a shielded environment with custom protocols. As off-the-shelf hardware, software and network protocols form the basis for many OTs, and the need for data transmission and remote administration has increased, the demand for realistic security testing has increased dramatically.

The threat model for critical infrastructure is much smaller than that of a traditional enterprise but, in some respects, far more severe. The primary goal for pen testing by the cybersecurity team at Honeywell is to provide a simulated cyber attack for industrial customers, focusing on the availability and integrity of industrial control systems.

Honeywell strives to achieve this by building a thorough preparation phase aimed at controlling the parameters of a penetration test. Using these parameters as a strict guideline, Honeywell then engages the target nuclear plant to evaluate the objectives established in the pre-engagement phase. As a final deliverable, Honeywell provides a detailed report that is designed to outline all exploitation activities conducted by Honeywell during the pen testing exercise and associated remediation identified during such testing, taking a transparent approach to tools, tactics and techniques.

4. NRC GUIDELINES FOR ACCESS CONTROL

The Nuclear Regulatory Commission (NRC) requires nuclear power plant licensees to implement robust access controls to protect their digital assets from unauthorized access and ensure the integrity and confidentiality of sensitive information.

The NRC has issued various regulatory documents outlining its requirements for access controls for digital assets. These include:

1. Title 10 of the Code of Federal Regulations (CFR) Part 73, "Physical Protection of Plants and Materials": This regulation sets out requirements for access controls at nuclear power plants, including requirements for access authorization, background checks and access control systems.

2. NRC Inspection Procedure 71111, "Access Authorization and Physical Access Control": This inspection procedure outlines the NRC's inspection process for evaluating a licensee's access authorization and physical access control programs.

3. NRC Regulatory Guide 5.71, "Cybersecurity Programs for Nuclear Facilities": This guide provides guidance on developing and implementing cybersecurity programs for nuclear facilities, including requirements for access controls for digital assets.

In general, the NRC requires licensees to implement access controls for digital assets that are commensurate with the criticality and sensitivity of the assets. This includes requirements for access authorization, strong authentication, authorization and permissions management, and audit logging and monitoring.

Licensees must also ensure that access to digital assets is granted only to authorized personnel who have undergone appropriate background checks and security clearances. Access control systems must be designed to prevent unauthorized access, including protection against social engineering attacks, and must be regularly tested and updated to ensure their effectiveness.

In addition, the NRC requires licensees to implement procedures for managing access to digital assets in emergency situations, such as during a cybersecurity incident or physical security event.

In summary, the NRC requires nuclear power plant licensees to implement robust access controls for their digital assets designed to protect them from unauthorized access and enhance the protections for the integrity and confidentiality of sensitive information. This includes requirements for access authorization, strong authentication, authorization and permissions management, and audit logging and monitoring. Licensees are also required to ensure that access is granted only to authorized personnel who have undergone appropriate background checks and security clearances and implement procedures for managing access in emergency situations.

4.1. HONEYWELL ACCESS CONTROL SOLUTION

For industrial control systems operating within the nuclear industry, access control solutions are critical components of their overall security program. Access control refers to the process of verifying the identity of individuals and granting them appropriate levels of access to a facility or digital assets.

To implement access controls, nuclear plants can use various solutions such as biometric scanners, smart card readers and security cameras to verify the identity of individuals and grant appropriate levels of access. They can also use digital access controls such as multifactor authentication, strong password policies and role-based access controls to prevent unauthorized access to digital assets.

Honeywell's trained cybersecurity professionals can help operators plan and implement access control solutions that are third-party solutions used and approved by industrial control organizations tailored to nuclear plants that address access control security.

5. NRC GUIDELINES FOR NETWORK MONITORING/UNIDIRECTIONAL GATEWAYS

The Nuclear Regulatory Commission (NRC) requires nuclear power plant licensees to implement network monitoring and unidirectional gateways to ensure the security and reliability of their operational technology (OT) networks.

Network Monitoring Solutions

The NRC has issued various regulatory documents outlining its requirements for network monitoring and unidirectional gateways. These include:

1. NRC Regulatory Guide 5.71, "Cybersecurity Programs for Nuclear Facilities": This guide provides requirement on developing and implementing cybersecurity programs for nuclear facilities, including requirements for network monitoring and unidirectional gateways.

2. NRC Inspection Procedure 71112, "Information System Security": This inspection procedure outlines the NRC's inspection process for evaluating a licensee's information system security program, including its network monitoring and unidirectional gateway activities.

In general, the NRC requires licensees to implement network monitoring tools and techniques to detect and respond to cybersecurity threats and anomalies. These tools and techniques should be designed to identify and block unauthorized network traffic, detect malicious activity and provide alerts to security personnel in a timely manner.

Unidirectional Gateway Solutions

The NRC also requires licensees to implement unidirectional gateways, which are devices that allow information to flow in only one direction between two networks. These gateways can help prevent cybersecurity threats from spreading between networks and can protect critical OT systems from unauthorized access.

Licensees must also ensure that their network monitoring and unidirectional gateway activities are integrated into their overall cybersecurity program and are subject to regular testing and validation. The effectiveness of these activities should be regularly reviewed and evaluated to ensure their ongoing relevance and effectiveness.

In addition, the NRC requires licensees to implement procedures for responding to cybersecurity incidents that involve their OT networks, including protocols for isolating infected systems, notifying appropriate authorities and restoring network operations.

In summary, the NRC requires nuclear power plant licensees to implement network monitoring and unidirectional gateways to ensure the security and reliability of their OT networks. These activities should be integrated into the licensee's overall cybersecurity program and subject to regular testing and validation. Licensees must also implement procedures for responding to cybersecurity incidents involving their OT networks.

5.1. HONEYWELL NETWORK MONITORING/ UNIDIRECTIONAL GATEWAYS

The Nuclear Regulatory Commission (NRC) has established rigorous requirements for the protection of nuclear power plants and their operational technology (OT) networks. These requirements are designed to improve the safety and security of nuclear power plants, protect against cybersecurity threats, and provide for compliance with federal regulations. One of the key requirements of the NRC is for licensees to implement network monitoring and unidirectional gateway solutions designed to protect their OT networks from unauthorized access and cyber attacks.

Network Monitoring Solutions

Network monitoring solutions provide a critical layer of security for nuclear power plants by monitoring network traffic and detecting any anomalies or potential security threats. These solutions are designed to identify unauthorized access attempts, network attacks, malware and other security incidents. By monitoring network traffic in real time, these solutions can provide early warning of cyber threats, allowing security personnel to respond quickly and prevent potential security breaches.

A comprehensive network monitoring solution that Honeywell deploys is designed to provide the following key capabilities:

1. Network Visibility: A network monitoring solution should provide comprehensive visibility into all network traffic, including data flows, device activity and network infrastructure. This visibility should include both on-premises and cloud-based infrastructure to provide full coverage across the entire network.

2. Threat Detection: A network monitoring solution should include advanced threat detection capabilities, such as intrusion detection and prevention, malware detection and behavioral analysis. These capabilities are designed to identify potential security incidents in real time and provide alerts to security personnel, enabling rapid response and remediation.

3. Incident Response: A network monitoring solution should include incident response capabilities, such as automated response actions, threat intelligence integration and forensic analysis. These capabilities are designed to help security teams quickly identify the source of a security incident, contain it and prevent it from spreading across the network.

4. Compliance Reporting: A network monitoring solution should include reporting capabilities that are designed to enable organizations to demonstrate compliance with regulatory requirements. This includes detailed reports on network activity, security incidents and compliance-related activities.

Unidirectional Gateway Solutions

Unidirectional gateway solutions provide another layer of security for nuclear power plants by creating a physical barrier between the OT network and the enterprise network. These solutions are designed to allow information to flow in only one direction, thereby preventing unauthorized access and cybersecurity threats from spreading across the network.

Honeywell's comprehensive software unidirectional gateway solution is designed to provide the following key capabilities:

1. Physical Separation: A unidirectional gateway solution should physically separate the OT network from the enterprise network, creating an air gap between the two networks. This capability is designed to prevent any potential threats from spreading from one network to another.

2. One-Way Communication: A unidirectional gateway solution should enable information to flow in only one direction, from the OT network to the enterprise network. This capability is designed to prevent any unauthorized communication or access attempts from the enterprise network to the OT network.

3. High Throughput: A unidirectional gateway solution should support high-speed data transfer rates in order to provide efficient communication between the two networks. This is especially important for applications that require real-time data transfers.

4. Robust Security Features: A unidirectional gateway solution should include robust security features, such as secure boot, tamper-proofing and secure communication protocols. These capabilities are designed to enhance the integrity and confidentiality of information flowing between the two networks.

The Honeywell Center of Excellence offers a hardware-based data diode solution - an optically isolated waterfall data diode and a deterministic unidirectional gateway. This is an effective tool for meeting NRC requirements for access control and network segmentation. By implementing this solution, nuclear facilities can reduce the risk of cyber attacks and improve compliance with regulatory requirements.

How Monitoring and Unidirectional Solutions Solve NRC Requirements

Honeywell specializes in implementing comprehensive network monitoring solutions and unidirectional gateway solutions for the nuclear power industry that meet NRC requirements for network security and compliance. By providing visibility into network traffic, identifying potential security incidents and creating a physical barrier between the OT network and the enterprise network, these solutions help prevent unauthorized access and cyber attacks.

6. NRC GUIDELINES FOR USB SECURITY

The Nuclear Regulatory Commission (NRC) has issued guidelines and regulations for USB security designed to protect against cyber threats. The NRC's cyber regulations for USB security include:

1. Authorization and Access Control: The NRC requires that access to USB devices be restricted to authorized personnel only. Access control measures should be implemented designed to prevent unauthorized access to USB devices.

2. Encryption: The NRC recommends that all data stored on USB devices be encrypted to enhance its protection against unauthorized access or data theft. Encryption should be applied to both the USB device and the data stored on it.

3. Virus Protection: The NRC requires that all USB devices used in NRC-regulated activities be scanned for viruses and malware before use. Regular virus scans should be performed on all USB devices used in the regulated environment.

4. Physical Security: The NRC requires that USB devices be physically secured when not in use. This can include storing the devices in a locked cabinet or safe or implementing other physical security measures designed to prevent theft or unauthorized access.

5. Training and Awareness: The NRC requires that personnel handling USB devices receive training and attend awareness programs on USB security best practices. This includes safe handling, storage and disposal of USB devices.

6. Logging and Monitoring: The NRC requires that all USB device activity be logged and monitored in order to improve the ability to detect any unauthorized access or usage. This includes tracking who is accessing the devices, when they are accessed and what data is being transferred.

It's important to note that these are just some of the key regulations and guidelines issued by the NRC for USB security. Additional measures may be required depending on the specific circumstances and environment in which the USB devices are being used.

6.1 HONEYWELL USB CYBERSECURITY SOLUTIONS

Honeywell Secure Media Exhance (SMX)

The Honeywell SMX solution offering is designed to help customers mitigate the malicious or unintentional threats posed by the use of removable media in industrial process facilities. SMX is designed to verify the contents of USB drives against evergreen threat intelligence and to improve security related to open USB ports from non-checked devices.

The SMX solution includes:

- Software that is designed to provide a proactive means to identify exposure to infectious malware on removable media. This includes advanced USB-protection operating software and an unlimited number of security endpoint drivers for customers' Windows devices.
- Hardware to support USB scanning for malware before a USB drive can be connected to the network.
- SMX access to the Global Analysis, Research and Defense (GARD) Threat Engine: Honeywell technology combines homegrown detection with leading commercial tools that are designed to provide powerful, fast and accurate threat detection and protection.
- Enterprise Threat Management Portal: Management dashboard that is designed to provide improved control and visibility into the use of removable media. Features included in the portal are designed to provide the ability to create custom file policies, enable configurable alerts and manage SMX systems remotely, among others.

NERC CIP standards require that all BES Cyber Assets (BCAs) have malicious code prevention and risk mitigation plans in place for their high-, medium-, and low-impact BES Cyber Systems (BCSs). This applies not only to common generation, transmission, and distribution providers, but also to other asset owners with high-voltage switchgear or power generation equipment at their plants. Section 215 of the Federal Power Act requires the Electric Reliability Organization (ERO) to develop mandatory and enforceable Reliability Standards for review and approval by the Federal Energy Regulatory Commission (FERC). FERC-approved Reliability Standards become mandatory and enforceable in the United States pursuant to the implementation plan associated with the Reliability Standard and approved by FERC. The standard is enforceable as of July 1, 2020. Organizations subject to the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) standards (or regional equivalents such as the Alberta Reliability Standards) must have a plan in place to mitigate the risk of malicious code on removable media. In NERC's CIP standards, they are referred to as "Responsible Entities" (RE).

There are numerous threats to the cybersecurity of nuclear plants and their interconnected power grids, which consist of generation and transmission assets and their control systems, referred to as bulk electric systems (BES). Malicious software – used to compromise systems, such as through websites, email attachments, and exploitation of unpatched applications – is a significant problem. These methods rely on an existing network connection between the attacker and the target. But even if critical systems are behind firewall layers or disconnected, data must be transported back and forth. USB removable media remains the "floppy disk" for transporting firmware, patches, diagnostic files, reports, and other items into and out of industrial control systems (ICS), operational technology (OT) and BES cyber systems (BCS).

Honeywell research shows that 52% of cyber threats target removable media. Even with administrative controls such as training and policies that restrict or prohibit the use of removable USB devices, organizations can still be compromised by well-meaning employees trying to get their jobs done. Because of their ease of use, it's nearly impossible to stop using removable USB media completely.

Despite this threat, they continue to be used, and additional technical controls are needed to mitigate this risk. The most common approach taken by those responsible for USB removable media is to set up a workstation on the corporate network with an antivirus program (scan host) that detects malicious code in files stored on USB removable media.

This may meet the basic requirements of the NERC CIP, but other aspects of compliance, ease of use, timely response and effort could be improved. Antivirus software was first developed in the late 1980s and has evolved into the antivirus industry we know today. The basic premise of antivirus is to constantly detect and identify "known malicious" software (also known as "blacklisting" or "denylisting") in a database of malicious software signatures.

As code obfuscation tools hide from antivirus programs and millions of new virus variants are added daily, the signatures of denylisted antivirus programs can no longer keep up.

An antivirus scan host is insufficient for today's malicious software threats and inadequate in many areas for modern Bulk Electric System (BES) with control centers and remote locations such as power plants and substations.

Examples where Honeywell SMX help comply to NRC Cyber Regulations are:

- Portability: This could be a desktop computer in an office-only environment connected to the corporate network, which could be bypassed or not used if it is not readily available at remote locations where the work is performed (e.g., service vehicle, power plant, substation).
- Restricting unscanned removable media assumes that the scan host is always used. It may be possible to bypass the host, meaning that non-scanned USB removable media would not be detected or restricted. Technical enforcement measures on the BES cyber assets ensure that the scan host cannot be bypassed.
- Limiting or no detection of malicious hardware: Supply chain attacks are rising, and the USB specification supports hundreds of different device types. Antivirus programs can detect malicious files in mass storage but cannot identify malicious functions such as keystrokes, microphones or wireless networking in the same USB hardware.
- Policy enforcement for USB device types: Scan hosts cannot detect or prevent other types of USB devices (e.g., smartphones, network interfaces) from connecting to a BES cyber asset. Therefore, controlling USB devices is another method of containing malicious hardware.
- Detection logs are only stored locally, depending on the antivirus program and its connectivity. Therefore, additional effort (i.e., time and cost) may be required to manually collect and review these logs or detect when logging has failed.
- Limited incident notification: when a malicious code is discovered, the intent of the malicious code must be investigated per NERC CIP and NRC standards. Therefore, incident response teams should be notified immediately to determine if it is an attack attempt.

7. NRC GUIDELINES FOR TRAINING AND AWARENESS

The Nuclear Regulatory Commission (NRC) has established training and awareness requirements for individuals who have access to or are responsible for the security of nuclear facilities and materials. These requirements are designed to ensure that personnel are trained to identify and mitigate security risks and that they are aware of their role in maintaining the safety and security of nuclear facilities and materials.

The NRC's training and awareness requirements are outlined in 10 CFR Part 73, "Physical Protection of Plants and Materials." This regulation requires licensees to develop and implement a security training program that covers a wide range of topics related to nuclear security. The following are some of the key training and awareness requirements outlined in 10 CFR Part 73:

1. General Training Requirements: All individuals who have access to or are responsible for the security of nuclear facilities and materials must receive initial and annual refresher training on the following topics:

- The licensee's security program and procedures
- The role of each individual in maintaining the security of the facility
- The potential threats to the facility and materials, including acts of terrorism, theft and sabotage
- The detection and response to security incidents, including the use of security equipment and the implementation of emergency procedures

2. Cybersecurity Training Requirements: Licensees must provide training on cybersecurity threats and best practices for all individuals who have access to or are responsible for the security of digital assets related to nuclear facilities and materials. This includes training on identifying and responding to cyber attacks, maintaining the integrity and confidentiality of digital assets, and complying with federal regulations related to cybersecurity.

3. Access Authorization Training Requirements: Licensees must provide training on access authorization procedures for all individuals who have access to or are responsible for the security of nuclear facilities and materials. This includes training on the verification of identity, background checks and access controls.

4. Force-On-Force Training Requirements: Licensees must conduct regular force-on-force training exercises to test the effectiveness of their security program and procedures. These exercises simulate an actual security incident and help identify areas for improvement in the licensee's security program.

5. Awareness Requirements: Licensees must implement an awareness program to ensure that all personnel are aware of their role in maintaining the security of the facility and materials. This includes regular communication on security-related topics, such as threat assessments, security incidents and changes to security procedures.

In addition to these training and awareness requirements, licensees must also develop and implement a security plan that outlines their security program and procedures. This plan must be approved by the NRC and must include a description of the licensee's security organization, access controls, physical protection measures, cybersecurity measures and emergency response procedures.

Overall, the NRC's training and awareness requirements are designed to ensure that nuclear facilities and materials are protected against security threats. By providing personnel with the knowledge and skills needed to identify and respond to security incidents, licensees can help prevent unauthorized access and mitigate the impact of potential security breaches.

7.1 HONEYWELL TRAINING AND AWARENESS

For nuclear plants, training and awareness programs are critical components of their overall security program. The Nuclear Regulatory Commission (NRC) has established specific training and awareness requirements for individuals who have access to or are responsible for the security of nuclear facilities and materials, including:

- General Training Requirements
- Cybersecurity Training Requirements
- Access Authorization Training Requirements
- Force-On-Force Training Requirements
- Awareness Requirements

Honeywell can assist licensees with the development and implementation of security training programs that cover a wide range of topics related to nuclear security. These programs provided by Honeywell include initial and annual refresher training on the licensee's security program and procedures, the role of each individual in maintaining the security of the facility, potential threats to the facility and the detection and response to security incidents

Additionally, Honeywell cybersecurity training covers identifying and responding to cyber attacks, maintaining the integrity and confidentiality of digital assets and complying with federal regulations related to cybersecurity. Access authorization training should cover verification of identity, background checks and access controls.

Honeywell's awareness programs are an essential assistance to NRC requirements, including regular communication on security-related topics such as threat assessments, security incidents and changes to security procedures.

Honeywell's comprehensive training and awareness programs are designed to enable nuclear plants to ensure that all personnel are equipped with the knowledge and skills needed to improve the safety and security of nuclear facilities and materials. These programs can help licensee's prevent unauthorized access and mitigate the impact of potential security breaches.

8. NRC GUIDELINES FOR VULNERABILITY SCANNING

The Nuclear Regulatory Commission (NRC) has established requirements for vulnerability scanning in the context of nuclear security. Vulnerability scanning is the process of identifying security weaknesses in computer systems and networks that could be exploited by attackers.

The NRC's requirements for vulnerability scanning are outlined in 10 CFR Part 73, "Physical Protection of Plants and Materials." This regulation requires licensees to implement a program to test and evaluate the effectiveness of their security measures. This includes conducting periodic vulnerability assessments of their computer systems and networks to identify potential weaknesses.

The following are some of the key requirements for vulnerability scanning outlined in 10 CFR Part 73:

1. Frequency: Licensees must conduct vulnerability assessments at least once every 12 months or whenever there is a significant change to their computer systems or networks.

2. Scope: Vulnerability assessments must cover all computer systems and networks that could impact the safety or security of the facility or materials.

3. Methodology: Licensees must use recognized industry-standard methodologies for conducting vulnerability assessments.

4. Reporting: Licensees must maintain records of their vulnerability assessments and provide a report to the NRC on the results of the assessment, including any identified vulnerabilities and a plan for addressing them.

5. Remediation: Licensees must promptly address any identified vulnerabilities and implement corrective actions to mitigate the risk of exploitation.

In addition to these requirements, the NRC also requires licensees to implement appropriate cybersecurity controls to improve protection against potential cyber attacks. These controls may include firewalls, intrusion detection systems and access controls, among others.

Overall, the NRC's requirements for vulnerability scanning are designed to ensure that nuclear facilities and materials are adequately protected against potential security threats. By conducting regular vulnerability assessments and implementing appropriate controls to address any identified weaknesses, licensees can help prevent unauthorized access and improve their ability to mitigate the impact of potential security breaches.

8.1. HONEYWELL VULNERABILITY SCANNING SOLUTION

Vulnerability scanning is a critical component of a company's security program to comply with the Nuclear Regulatory Commission's (NRC) regulations. It involves regularly scanning systems and networks to identify potential vulnerabilities, misconfigurations and weaknesses that could be exploited by cyber attackers.

Honeywell offers two key cybersecurity solutions: Honeywell Forge Cybersecurity+ | Cyber Insights and Cyber Watch. Cyber Insights, a comprehensive vulnerability scanning program, conducts both automated and manual scans, analyzing logs to prioritize risks. It provides asset discovery, aiding in identifying all network-connected assets. On the other hand, Cyber Watch enhances cybersecurity posture by leveraging Cyber Insights capabilities for a centralized view of threats across operational sites. It facilitates quicker and coordinated responses to signs of compromise, and includes a governance portal for senior executives to monitor cybersecurity compliance organization-wide.

Vulnerability scans are designed to enable companies to proactively identify potential security weaknesses and mitigate the identified risks before they are exploited by cyber attackers. This helps to improve the safety and security of personnel and facilities, and to comply with NRC regulations.

It is important to note that vulnerability scanning is just one aspect of a comprehensive security program. It should be used in conjunction with other security measures, such as access controls, network segmentation and threat intelligence, to provide a layered approach to security.

Overall, vulnerability scanning is an essential component of a company's security program required for compliance with NRC regulations. By implementing a comprehensive vulnerability scanning program, companies can improve their ability to proactively identify and mitigate potential risks, thereby improving the overall security posture of their operations.

9. CYBERSECURITY ATTACKS

Cybersecurity attacks on nuclear power plants are a growing concern, as these attacks have the potential to cause significant harm and disruption. Nuclear power plants rely heavily on computer systems and networks to control and monitor their operations, making them vulnerable to cyber attacks.

Some of the potential consequences of a successful cyber attack on a nuclear power plant include the disruption of power generation, damage to equipment and the release of radioactive material. In addition, cyber attacks could also compromise the safety and security of personnel at the plant.

To mitigate the risk of cyber attacks, nuclear power plants must implement robust cybersecurity measures, including firewalls, intrusion detection systems and access controls. They must also conduct regular vulnerability assessments to identify potential weaknesses in their systems and networks.

Given the potential consequences of a successful cyber attack on a nuclear power plant, it is essential that these facilities take cybersecurity seriously and implement appropriate controls to protect against potential threats

This document is a non-binding, confidential document that contains valuable proprietary and confidential information of Honeywell and must not be disclosed to any third party without our written agreement. It does not create any binding obligations on us to develop or sell any product, service or offering. Content provided herein cannot be altered or modified and must remain in the format as originally presented by Honeywell. The quantified product benefits referenced are based upon several customers' use cases and product results may vary. Any descriptions of future product direction, intended updates or new or improved features or functions are intended for informational purposes only and are not binding commitments on us and the sale, development, release or timing of any such products, updates, features or functions is at our sole discretion. All product screenshots shown in this document are for illustration purposes only; actual product may vary.

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, Georgia 30308
www.honeywellforge.ai

Honeywell