UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR MATERIAL SAFETY AND SAFEGUARDS
OFFICE OF NUCLEAR REACTOR REGULATION
WASHINGTON, DC 20555-001

August 14, 2019

NRC INFORMATION NOTICE 2019-04: EFFECTIVE CYBER SECURITY PRACTICES TO PROTECT DIGITAL ASSETS OF BYPRODUCT MATERIALS LICENSEES

ADDRESSEES

All U.S. Nuclear Regulatory Commission (NRC) byproduct materials licensees that possess risk-significant quantities of radioactive material and NRC master materials licensees. All Agreement State Radiation Control Program Directors and State Liaison Officers.

PURPOSE

The NRC is issuing this information notice (IN) to inform licensees of the results of an assessment conducted by the NRC staff on the potential need for cyber security requirements for byproduct materials licensees and to communicate effective cyber security practices to protect digital assets.

The information in this IN is not an NRC requirement; therefore, the NRC requires no specific action or written response. The NRC is providing this IN to the Agreement States for their information and for distribution to their applicable licensees, as appropriate.

BACKGROUND

In 2013, the NRC staff assessed the need for cyber security requirements for byproduct materials licensees as part of its overall strategy to ensure that both reactor and nonreactor licensees are providing adequate protection against cyber security threats. In 2014, the Radiation Source Protection and Security Task Force, chaired by the NRC, recommended the U.S. Government agencies "assess the adequacy of and coordinate strategies for preventing and mitigating cybersecurity vulnerabilities related to Category 1 and Category 2 radioactive sources." The 2018 Radiation Source Protection and Security Task Force Report (ADAMS Accession No. ML18235A370 (package)) reported on the NRC's assessment.

DISCUSSION

In the assessment, the NRC staff considered the need for protection from cyber threats to digital assets in the following four usage categories: digital devices that support the physical security of licensees' facilities; equipment with software-based control, operation, and automation features; computers used to maintain source inventories, audit data, and records necessary for compliance with security requirements; and digital technology used to support incident response communications and coordination.

The NRC staff concluded that the categories of licensees evaluated in this assessment do not solely rely on digital systems to ensure safety or security. Generally, licensees apply a

defense-in-depth approach to safety and security by using measures that include nondigital features such as doors, locks, barriers, human resources, and operational processes in addition to any digital assets. In addition, computers used to maintain source inventories, audit data, and records necessary for compliance with security requirements often use encryption, password protection, and other methods of limiting access to digital records to those who have a need to know. As a result, the NRC staff determined that a compromise of the digital assets used in these applications would not cause a direct dispersal of risk-significant quantities of radioactive material[1] or exposure of individuals to radiation without a concurrent and targeted breach of the safety, security, and physical protection measures in force for these licensees. The NRC staff also determined that the current cyber security threat that these licensees face does not warrant the development of new regulations related to the protection of risk-significant quantities of radioactive material against cyber security threats.

Although changes to the regulations are not necessary, the NRC staff concluded that awareness of mechanisms and practices that can provide protection against cyber security threats may be valuable to licensee operations and procedures. As a result, the enclosure to this IN contains effective practices for licensee awareness. The NRC staff also determined that providing a means to share relevant information resources with licensees would be prudent because the cyber security threat landscape is constantly evolving. The "Conclusion" section of this IN provides information on how to access these resources.

CONCLUSION

Implementation of the requirements found in 10 CFR Part 37 provides reasonable assurance of adequate protection of public health and safety when considering the potential consequences of a wide array of attack modes, including cyber. The enclosure to this IN provides additional effective practices related to cyber security issues licensees may use as applicable.

Previously, the NRC staff provided additional details and examples of applicable effective practices in guidance developed by the Office of Nuclear Reactor Regulation for nonpower reactors, "Cyber Security: Effective Practices for the Establishment and Maintenance of Adequate Cyber Security at Non-Power (Research and Test) Reactor Facilities," dated January 8, 2016 (ADAMS Accession No. ML15252A236 (package)).

In addition, the U.S. Food and Drug Administration (FDA) regulates the manufacturers of medical devices. Additional information on the FDA's activities, role, and expectations for continued cyber security of medical devices can be found at https://www.fda.gov/downloads/medicaldevices/digitalhealth/ucm544684.pdf.

The National Institute of Standards and Technology Special Publication 800 Series is a set of documents that provides U.S. Federal Government computer security policies, procedures, and guidelines. These publications, available at https://csrc.nist.gov/publications/sp800, may be useful to licensees by providing guidelines for workable and cost-effective methods for optimizing the security of information technology (IT) systems and networks in a proactive manner. The publications cover all procedures and criteria recommended by the National

[1] Risk-significant quantities of radioactive material are defined as those that meet the thresholds for Category 1 and Category 2 as included in Appendix A, "Category 1 and Category 2 Radioactive Materials," of Title 10 of the *Code of Federal Regulations* (CFR) Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material."

Institute of Standards and Technology for assessing and documenting threats and vulnerabilities and for implementing security measures to minimize the risk of adverse events.

CONTACT

This IN requires no specific action or written response. Please direct any questions about this matter to the technical contacts listed below.

/RA/

Christopher G. Miller, Director
Division of Inspection
and Regional Support
Office of Nuclear Reactor Regulation

/RA/

Andrea L. Kock, Director
Division of Materials Safety, Security, State,
and Tribal Programs
Office of Nuclear Material Safety
and Safeguards

Technical Contacts: Kim Lukes, NMSS
(301) 415-6701
E-mail: Kim.Lukes@nrc.gov

Paul Goldberg, NMSS
(301) 415-7842
E-mail: Paul.Goldberg@nrc.gov

Note: NRC generic communications may be found on the NRC public Web site, http://www.nrc.gov, under NRC Library/Document Collections.

NRC INFORMATION NOTICE 2019-04: EFFECTIVE CYBER SECURITY PRACTICES TO PROTECT DIGITAL ASSETS OF BYPRODUCT MATERIALS LICENSEES

ADAMS Accession No.: ML18044A350 **CAC/EPID: A11017/L-2019-GEN-0000** *** - via email**

OFFICE	NMSS/SMPB/TR	NMSS/SMPB/TR	QTE	NMSS/SMPB/BC	NMSS/ASPB/BC
NAME	PGoldberg	KLukes	JDougherty*	ZCruzPerez*	PMichalak*
DATE	03/19/19	03/19/19	03/28/19	05/22/19	05/29/19
OFFICE	NRR/DIRS/IRGB/PM	NRR/DIRS/IRGB/OLA	NRR/DIRS/IRGB/ BC	NMSS/MSST/D	NRR/DIRS/D
NAME	TGovan*	IBetts*	TInverso*	AKock	CMiller
DATE	06/03/19	06/06/19	06/11/19	08/13/19	08/14/19

Official Record Copy

EFFECTIVE CYBER SECURITY PRACTICES TO PROTECT DIGITAL ASSETS OF BYPRODUCT MATERIALS LICENSEES

EFFECTIVE PRACTICES

Personnel

Define Roles and Responsibilities

Effective practices include instituting role-based access controls to network resources based on personnel job functions. Limiting permissions through access controls can reduce the risk of compromise to systems and facilitate better tracking of network intrusions and suspicious activities. In addition, restricting the number of personnel granted administrative (i.e., "super user" or "root") rights or accounts on each digital asset and ensuring that all such personnel have the applicable training and experience in administrative functions for those digital assets is an effective practice.

Implement Staff Cyber Security Training

One of the best means of preventing cyberattacks is to educate personnel who perform administrative functions or use digital assets about the mechanisms by which cyberattacks may be carried out and strategies to protect them. Effective initial and periodic cyber security training may include information on social engineering methods that malicious actors might use to attempt to entice employees into providing sensitive personal or corporate information through phishing, phone calls, or other types of personal interactions; smart browsing practices such as awareness of malware, updating systems, and installing patches; password policies; use of portable electronic media and devices; use of wireless communications; appropriate incident response and reporting; and awareness of relevant information technology (IT) policies and procedures related to the employees' job activities.

Physical Protection

Physical Security

Part of the effort to protect digital assets against cyberattacks involves ensuring that physical security is in place. Devices containing risk-significant radioactive materials that have digital components to their operations, such as panoramic irradiators and stereotactic radiosurgery devices, are typically located within security zones that are already subject to Title 10 of the *Code of Federal Regulations* (CFR) Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material." Effective practices include physical security measures such as using locked rooms and enclosures for other types of digital assets, such as computers that house sensitive security-related information.

Some facilities use radiofrequency identification (RFID) personnel badges as part of their access control systems. Licensees could consider whether their facilities could be susceptible to badge-cloning attempts. Multifactor authentication measures, such as using a unique passcode or biometric in association with use of the badge, can augment the secure use of RFID badges. In addition, a cover or carrier used to shield an RFID personnel badge can prevent badge-cloning attempts.

Beyond physical controls for protecting digital assets, other types of controls, which may be technical (e.g., firewalls, account passwords, antivirus software) or administrative (e.g., policies, procedures, guidelines, training), can reduce the pathways available for a cyberattack.

Security Information Technology Infrastructure

Maintain an Accurate Inventory of Digital Assets and Eliminate Exposure to External Networks

Maintaining an inventory of the facility's digital assets and specifying which, if any, of those devices are connected to other business networks or the Internet is considered an effective practice for determining where pathways may exist for cyber threat access. Such an assessment could be done by mapping out all interconnectivities and dependencies, including perimeters and connections to other systems. Removing any unnecessary software or services could eliminate any unnecessary routes for possible cyberattacks.

Implement Local Networks or Network Segmentation and Apply Firewalls

Keeping digital assets isolated from one another (no communications connectivity, or creation of an "isolated" local area network (LAN)), when possible, is an effective practice. For example, licensees could maintain boundaries to isolate digital components related to operations (e.g., panoramic irradiators and gamma stereotactic radiosurgery units) from the digital components of the physical security systems (e.g., the intrusion detection devices/systems). This concept also applies in large radioactive material licensee settings (e.g., hospitals and college campuses) where there is mass interconnectivity of LANs.

As another practice, network segmentation, divides a computer network into subnetworks or network segments, and it entails classifying and categorizing IT assets, data, and personnel into specific groups and then restricting access to these groups. Through network segmentation, a compromise of one device or sector cannot translate into the exploitation of an entire system.

Access to network areas can be restricted by isolating them entirely from each other or by implementing firewalls or similar security features. A firewall is a software program or hardware device that filters the inbound and outbound traffic between different parts of a network or between a network and the Internet. Firewalls can be used to block malware delivery and attempts at the remote exploitation of various systems and to provide notification of all such attempts.

Disabling wireless interfaces when they are not needed and avoiding the use of wireless communications for certain functions is an effective practice. In an automated system, avoiding the use of wireless communications for any signal or control that is essential for a safety function is an effective practice. When communicating between remote sites (i.e., sites that are not part of the internal data communications), the licensee could consider encrypting data communications, as appropriate and commensurate with the sensitivity of the data being transmitted.

Use Secure Remote Access Methods

If remote access is necessary, a higher level of security can be achieved through a secure access method, such as use of a virtual private network (VPN). A VPN is an encrypted data channel for securely sending and receiving data through public IT infrastructure, like the Internet. This remote access can be further hardened by reducing the number of Internet Protocol (IP) addresses that can access it (i.e., by limiting access to only a specific set of IP addresses through a firewall). A VPN is only as secure as the devices connected to it. For example, a laptop infected with malware can introduce vulnerabilities into the network, which can lead to additional infections and negate the security of the VPN.

Another practice is to disconnect and remove telephone modems and phone lines used for temporary remote access when they are not in use.

Implement Measures for Network Port Access

All open network ports on switches, routers, and firewalls could be access points that enable cyber criminals to gain physical access to licensee networks and computer systems. Licensees may consider disabling all open and unused network ports. Disabling any ports that will not be used for an extended period (e.g., when an employee goes on extended leave) is an effective practice.

Cyber Security Policies

Use Strong Passwords, Change Default Passwords, and Consider Other Access Controls

Strong passwords and the use of different passwords for different accounts can keep systems and information secure. Password policies that define how complex passwords need to be generated and how often or under what condition they need to be changed are good preventive measures. The following techniques are useful in creating unique passwords: (1) avoid using passwords that are based on personal information that can be easily guessed, (2) use a combination of capital and lowercase letters, numbers, and special characters, and (3) develop mnemonics such as passphrases for remembering complex passwords. In addition, using password managers and implementing policies of not reusing passwords across accounts are effective practices, as well as changing all default passwords upon installation of new software and using account lockout controls that activate when too many incorrect passwords have been entered. Multifactor authentication, under which users must verify their identities whenever they attempt to sign in, is an effective practice.

Providing temporary accounts for vendor or contractor support and updating password and user account policies to identify events that would trigger a need to remove an account are effective practices.

Maintain Awareness of Vulnerabilities and Implement Necessary Patches and Updates

Installing patches is an effective practice. Whenever a new flaw is discovered, the typical protocol is to alert the software developer immediately so that it can issue a patch. Automatic updating of software and handheld devices provides the simplest means of protecting against cyber vulnerabilities. Limiting upgrades such that only authorized administrators complete the upgrades and that patches and firmware are obtained only from authorized and reputable vendors can prevent hackers from using flaws to their advantage. Maintaining a list of security

patches and software updates can help ensure that systems are up to date as cyber threats and vulnerabilities are identified.

Develop and Enforce Policies on Mobile Devices

Establishing reasonable limitations for employees and contractors on the use of mobile devices (e.g., laptops, tablets, and smartphones) in the conduct of business in the office or at an offsite workplace is an effective practice.

Enhancing the security of mobile devices by configuring them with a password feature that only enables access upon entry of a specific password and locks the device after repeated incorrect password entry attempts is an effective practice. The regulations in 10 CFR Part 37 do not prohibit the storage of sensitive, security-related information on mobile devices. Encryption, remote wipe capability (which allows licensees or device providers to remotely delete all data on the devices if they are lost or stolen), and routine antivirus software use and update are additional effective practices for mobile devices, as well as securely deleting all stored information on devices before discarding them.

Enabling full-disk or folder encryption (i.e., the encryption of all files in a directory and its subdirectories) can protect the sensitive or security-related information in a laptop or mobile device, even if the hard drive is removed and reinstalled in a different system. Most modern operating systems (such as Microsoft Windows) have built-in encrypted file system functionality.

It is an effective practice to avoid joining unknown Wi-Fi networks or using public Wi-Fi hotspots, as adversaries could create fake Wi-Fi hotspots designed to attack mobile devices and may patrol public Wi-Fi networks for unsecured devices. In addition, limiting the use of the hot-spot functionality on cell phones is effective practice because they can be used as an entry point for tampering.

Develop and Enforce Policies on Electronic Media and Device Handling

Electronic media can be either active (i.e., items can be edited, such as hard drives, secure digital memory cards, subscriber identity module cards, and USB memory sticks) or passive (i.e., the item simply provides a container for electronic information storage and cannot be edited, such as compact disks, digital versatile disks, and magnetic tapes). Regardless of the type, protection of electronic media is an effective practice.

Labeling and controlling all electronic media and devices according to the highest sensitivity of information being stored on the media and devices is an effective practice. Tracking these media and devices and documenting the individuals that have access to them is effective at preventing cyber attacks.

Whether active or passive media are used to transfer information to a system, the content of the data container on the media can be a vehicle for viruses, malware, or other malicious code. When loading or copying information onto a digital asset, an antivirus scan can be conducted on the media used for the transfer.

Purging of all residual data on components that are no longer needed is an effective practice.

Implement Measures for Detecting Compromises and Develop a Cyber Security Incident Response Plan

Implementing measures such as intrusion detection systems (IDSs) and intrusion prevention systems (IPSs),[2] antivirus software, and logs can help to detect compromises in their earliest stages. Most IDSs and IPSs use signatures to detect port scans, malware, and other abnormal network communications.

Cyber security incident response plans can limit damage and reduce recovery time and costs in the event of a cyber security incident. Plans may include measures for reacting to malware and being prepared to operate manually, if needed.

Develop and Enforce Policies on Maintenance and Testing

Cyber security testing—particularly before deploying new components—can verify that applicable software, systems, and devices do not contain any known, exploitable cyber security vulnerabilities and that they perform all the specified functions. The functionality of digital and software-based systems and assets after performing maintenance can be verified. Testing, updating, and patching digital and software-based systems and assets on a routine basis will make the compromise of systems and devices more difficult.

If the maintenance and support of digital assets is outsourced to vendors, it is an effective practice to establish a means of confirming that the remote support from vendors or IT organizations is secure and that vendor support personnel can handle cyber security-related issues.

[2] An IDS is a device or software application that monitors a network or systems for malicious activity or policy violations. An IPS is a network security and threat prevention technology that examines network traffic flows to detect and prevent the exploitation of vulnerabilities.