Homeland Security

National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Critical Infrastructure Security and Resilience Note

NUCLEAR REACTORS, MATERIALS, AND WASTE SECTOR CYBERDEPENDENCIES

October 6, 2015, 0900 EST

PREPARED BY: PRIORITIZATION AND MODELING DIVISION

SCOPE

The Department of Homeland Security Office of Cyber and Infrastructure Analysis (DHS OCIA) produces cyberdependency papers to address emerging risks to critical infrastructure and provide increased awareness of the threats, vulnerabilities, and consequences of those risks to the Homeland. This note informs infrastructure and cybersecurity analysts about the potential consequences of cyber-related incidents in the Nuclear Reactors, Materials, and Waste Sector and its resilience to such incidents. This note also clarifies how computer systems support infrastructure operations, how cybersecurity incidents compromise these operations, and the likely functional outcome of a compromise.

For this note, infrastructure cybersecurity incidents are defined as actual and potential events that exploit cybersecurity vulnerabilities. Cyber attacks can disrupt or corrupt normal operating conditions in computer systems; networks; industrial control systems (ICS); or electronic devices that control, monitor, or support the function of infrastructure. Infrastructure is cyberdependent when it relies on computers or information technology to support its physical operations and essential functions.

This note focuses on the potential impacts of incidents on various types of Nuclear Reactors, Materials, and Waste Sector cyberdependent systems and functions. A cybersecurity incident at a Nuclear Reactors, Materials, and Waste Sector asset may have no effect on the infrastructure itself, yet still affect the Sector by the addition of new protective requirements. So many safeguards exist that cyber attacks against a nuclear power plant are not likely to succeed without the aid of authorized personnel within the restricted access areas. Analysis of complex, sophisticated, and distributed cyber attacks against multiple Nuclear Reactors, Materials, and Waste Sector assets is beyond the scope of and resources available for this note.

DHS OCIA developed this note with input from the Idaho National Laboratory and in coordination with the DHS National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection and the DHS NPPD Office of Cybersecurity and Communication Industrial Control Systems Computer Emergency Response Team (ICS–CERT); National Infrastructure Simulation and Analysis Center (NISAC); the Nuclear Regulatory Commission (NRC); and representatives of the Nuclear Reactors, Materials, and Waste Sector Coordinating Council.

KEY FINDINGS

- **Nothing suggests that a cyber attack executed through the Internet could cause a nuclear reactor to malfunction and breach containment.**
- **Nuclear power reactors have comprehensive safeguards that protect control system safety and security and prevent the misuse of portable media (e.g., Universal Serial Bus [USB] devices) and portable equipment (e.g., maintenance laptops) from circumventing these protections.**
- **The layered defense protecting critical digital assets in nuclear power plants are designed to prevent the possibility of anyone without unescorted access from initiating a cybersecurity incident affecting these systems. If preexisting undetected vulnerabilities or compromises in the digital equipment or software create a problem, alternative means are available for accomplishing safety and security functions.**
- **U.S. nuclear power reactor safety systems must have at least two independent systems to (1) keep the reactor coolant pressure boundary intact, (2) shut down and maintain the plant in a safe shutdown condition, and (3) ensure no radioactive release occurs in excess of federal limits.**
- **Multiple ways exist to read critical plant operational parameters. All operators are trained to rely on more than one indicator to make decisions in operating a plant. Even if authorized and knowledgeable individuals attempted to do harm, they would have to compromise several systems to sabotage the plant.**
- **If a single nuclear power reactor goes offline, the electric grid could manage the loss of supply in most circumstances. Under peak loads, the worst cascading effect might be rolling blackouts until the supply and demand balance.**

BACKGROUND

The Nuclear Reactors, Materials, and Waste Sector is defined by a common requirement to safely and securely manage radioactive material—from the fuel pellets powering reactors to medical isotopes to nuclear waste transportation and disposal. The key elements of the Sector are nuclear power plants; non-power nuclear reactors (used for research, testing, and training); nuclear fuel-cycle facilities; transportation, storage, and disposal of nuclear and radioactive waste; and nuclear materials used for medicine and manufacturing.

COMMERCIAL NUCLEAR POWER PLANTS

The NRC mission is to license and regulate the Nation's civilian use of nuclear by-product, source, and special nuclear materials to ensure the adequate protection of public health and safety, promote common nuclear defense and security, and protect the environment (from contamination by radioactive materials).[1,2] The NRC also regulates the management of spent fuel at operating and decommissioned power plants. The NRC requires all commercial nuclear power plants to be designed to withstand catastrophic events such as fires, tornados, floods, earthquakes, and large aircraft impacts to avoid or reduce a radiological release.[3] Emergency preparedness programs accompanied by inspections and full-scale exercises are a condition of operator licenses for all nuclear power plants in the United States.[4] Once nuclear power plants meet all of their cybersecurity requirements, this new baseline, combined with the industry's exacting standards and culture of back-up safety systems, will make it extremely difficult for an external adversary to cause a radioactive release.

[1] Source material is uranium or thorium, or any combination thereof, in any physical or chemical form, or ores that contain, by weight, one-twentieth of one percent (0.05 percent) or more of (1) uranium, (2) thorium, or (3) any combination thereof. Special nuclear material is plutonium, uranium-233, or uranium enriched in the isotopes uranium-233 or uranium-235, U.S.NRC glossary, http://www.nrc.gov/reading-rm/basic-ref/glossary , accessed May 1, 2015.

[2] The Nuclear Regulatory Commission Strategic Plan 2008–2013.

[3] 10 CFR Appendix A to Part 50–General Design Criteria for Nuclear Power Plants.

[4] http://www.nrc.gov/about-nrc/emerg-preparedness/protect-public.html, accessed July 7, 2014.

Industry culture, independent audits, and leadership of the Institute for Nuclear Power Operations keep industry focus on safety and security. Additionally, the NRC can issue the following:

- Civil penalties for violations of regulatory requirements up to $130,000 per violation, per day;
- Increased oversight billed to the power plant owner and operator; and
- Orders that modify, suspend, or revoke licenses or require specific actions by licensees or persons if they violate the regulations.[5]

The NRC currently licenses 100 operating commercial nuclear power plants. These plants produce approximately 20 percent of the electricity generated in the United States. Figure 1 illustrates the trends for different fuel sources for the production of electricity, reported in the 2015 Annual Energy Outlook. The projections are based on analyses from the Annual Energy Outlook 2014 National Energy Modeling System and show that U.S. reliance on nuclear power will remain consistent through 2040 with nuclear power generation meeting 18.56 percent of U.S. demand in 2014 and dropping gradually to 15.54 percent in 2040. The overall production of electricity by nuclear generators is expected to increase from 759 trillion kilowatt hours in 2014 to 811 trillion kilowatt hours in 2040. This decline in percent contribution reflects the anticipated growth of natural gas-fueled electricity generation, rather than a significant change for commercial nuclear power generation.[6]

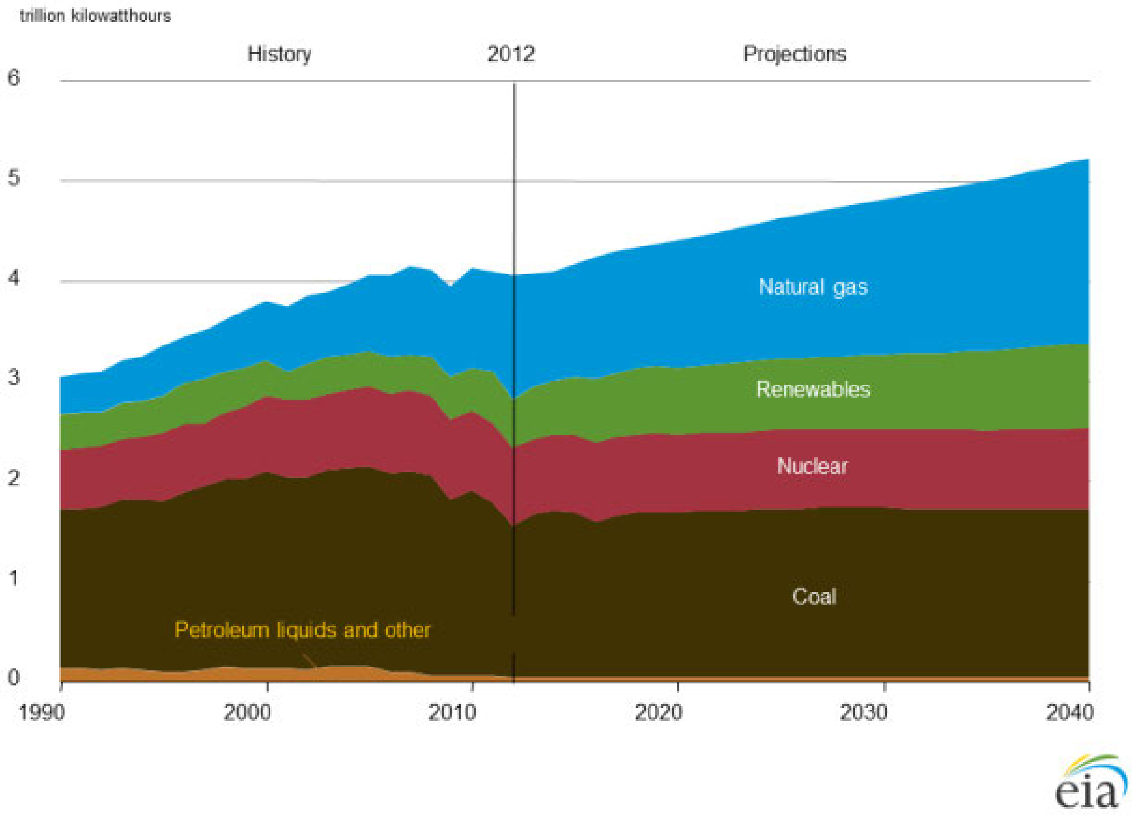

FIGURE 1—ELECTRICITY GENERATION BY FUEL ANNUAL ENERGY OUTLOOK 2014 REFERENCE CASE[7]

U.S. nuclear power plants have demonstrated design fortification and resilience against natural disasters including direct hits from Category 5 Hurricanes Andrew in 1992 and Katrina in 2005. Additionally, in 2011, the North Anna

[5] http://www.nrc.gov/about-nrc/regulatory/enforcement/program-overview.html#penalties.

[6] Energy Information Administration, 2015 Annual Energy Outlook, see downloadable data sources, http://www.eia.gov/forecasts/AEO/MT_electric.cfm accessed May 1, 2015.

[7] Energy Information Administration, 2015 Annual Energy Outlook, see downloadable data sources, http://www.eia.gov/forecasts/AEO/MT_electric.cfm accessed May 1, 2015, and EIA Reference Source: Electricity Generation by Fuel in the Reference Case 1990–2040, Projections: AEO2014 National Energy Modeling System, run REF2014.D102413A, accessible through download.

reactor successfully shut down in response to a 5.8 magnitude earthquake with an epicenter just over 12 miles away in Mineral, Virginia. The reactor restarted 3 months later following an inspection that found no functional damage.[8] Following the Fukushima Daiichi accident in 2011, the NRC established new requirements and issued orders requiring new capabilities to ensure continued reactor core cooling indefinitely, even if power is lost.[9] Thus, the U.S. nuclear power industry has a continuous risk management approach that has enabled plants to manage extreme hazards and seeks opportunities to improve based on lessons learned.

NON-POWER REACTORS

Non-power reactor uses include research, theoretical practice development, radioactive source production, and educational or medical purposes. The NRC licenses 42 non-power reactors, with 31 currently in operation. The NRC regulates all non-power reactors except those belonging to the Department of Defense (DOD) and the Department of Energy (DOE) that are responsible for regulating their own facilities, including the cybersecurity of the organizations operating the facilities. Non-power reactors use significantly less nuclear fuel in their reactors than power plant reactors, but they employ the same safety measures. Since the 1970s, non-power reactors must comply with the NRC security regulations in Section 10 of the Code of Federal Regulations Part 73 (10 CFR Part 73).

NUCLEAR FUEL CYCLE FACILITIES

Nuclear fuel cycle facilities produce non-activated nuclear fuel using multiple scientific technologies.[10] These fuel cycle facilities include six uranium fuel fabrication entities, two gaseous diffusion fuel enrichment facilities (one of which is in cold shutdown), and one uranium hexafluoride production facility, all licensed by the NRC. Nuclear fuel cycle facilities operate at lower pressure and temperature and have lower energies associated with radioactive inventory compared with commercial nuclear power plants. They use similar protections including multiple containment barriers for radioactivity, corrosion, and other problems associated with aging and toxic and radiological environments. Facilities also promote adequate long-term equipment operability and structural integrity. With the discontinuation of the Yucca Mountain waste repository in 2010, continued long-term passive and secure confinement and containment of radioactive materials (e.g., storage tanks and reservoirs) are ongoing challenges not only in nuclear fuel cycle facilities but also in commercial nuclear power reactors.

Transporting nuclear fuels has two external risks: (1) the movement of non-activated fuel to a facility for use and (2) the transfer of spent fuel as it moves from a site. The requirements for measures to reduce this vulnerability are detailed in 10 CFR 73.37 and 73.38 and include specifications for redundant communications. In addition to NRC regulation, State and other Federal authorities regulate the transport of such materials.

NRC COMPLIANCE

Licensees must demonstrate compliance with applicable NRC regulations. Currently, the cybersecurity requirements only apply to commercial nuclear power generation, not nuclear fuel cycle facilities and transporters. Research reactors must comply with cybersecurity requirements as member-participants in their established funding programs. DOE and DOD reactors must comply with the cybersecurity requirements of their respective agencies.

The NRC is the lead regulator for the nuclear industry, and the DHS Office of Infrastructure Protection is the Sector Specific Agency (SSA). The SSA leads the coordinated effort to develop improved ways to identify and manage risks. Working with the SSA allows the industry to consider an enterprise approach to risk management including risks unrelated to the regulatory framework.

[8] Nuclear Power Plants and Earthquakes, World Nuclear Association, http://www.world-nuclear.org/info/safety-and-security/safety-of-plants/nuclear-power-plants-and-earthquakes/.

[9] Government Accounting Office, Nuclear Safety, Countries' Regulatory Bodies Have Made Changes in Response to the Fukushima Daiichi Accident.

[10] Non-activated fuel is fuel for which the neutron chain reaction has not started. It is not yet radioactive.

Licensees required to follow 10 CFR Part 73 security regulations include all entities authorized by the NRC to conduct any or all of the following activities:

- Construct, operate, and decommission commercial reactors and fuel cycle facilities;
- Possess, use, process, export and import nuclear materials and waste, and handle certain aspects of their transportation; and
- Site, design, construct, operate, and close waste disposal sites.

To become licensed for any of these activities (or to amend, renew, or transfer an existing license), an entity or individual submits an application to the NRC. The NRC staff reviews the submission, using standard review plans, to ensure that the applicant's assumptions are technically correct and that the proposed activities will not adversely affect the environment.

Much of the Nuclear Reactor, Materials, and Waste Sector security efforts is similar to the security controls used for classified national security endeavors. Similarities include physical security with controlled access, air-gapped protections of sensitive computer systems, and stringent personnel security. Nuclear workers are subject to background investigations and clearance processes that feature a psychological evaluation to help exclude unreliable personnel from the most sensitive access.

Despite the significant investment in precluding untrustworthy individuals' access to sensitive areas, the processes for monitoring and removal of individuals if they become unreliable, and the significant education and training personnel are given, errors may occur. Mistakes can be made by an authorized nuclear worker triggering an emergency. Plants and processes are designed with defense-in-depth in mind and, complying with the requirements of regulation, are designed to fail safely without the need for operators to take action.[11]

CYBER-SUPPORTED PROCESSES

ICS are used within the Nuclear Reactors, Materials, and Waste Sector to control sensitive processes and physical functions, including the security of the restricted access areas. Examples of ICS include Supervisory Control and Data Acquisition systems (SCADA), Process Control Systems, and Distributed Control Systems. In commercial nuclear power plants, non-power reactors, and fuel cycle facilities, ICS may collect measurement and operational data from other parts of a plant or complex, process and display that information, then relay control commands to local or remote equipment or human-machine interfaces. ICS are in limited use in commercial nuclear power reactors and non-power reactors to operate equipment that directly controls the reactors. ICS are more widely used to control power generation equipment not associated with plant safety. Fuel cycle facilities use SCADA systems to automate uranium enrichment processes. Many ICS in commercial nuclear power plants provide control of systems that are not safety-related during normal and emergency situations. Control systems are also used in enrichment facilities operations, and may be used to monitor the state of spent fuel in storage, although this use is not universal.

Most control systems in nuclear power plants were developed before Internet connectivity and have been isolated through the use of physical air gaps or hardware-based isolation devices. Newer plant systems capable of remote or Internet-access are similarly isolated in accordance with industry consensus-approved options for responding to the regulatory requirements. That is, if access to the Internet by any plant system leads to connectivity to critical digital assets, plant operators have agreed to disable the capability to connect.[12]

The requirements for cybersecurity protection of nuclear power plants are addressed through the NRC rule 10 CFR 73.54, Protection of Digital Computer and Communication Systems and Networks. This rule focuses on the protection of digital (i.e., information technology) assets associated with safety, security, and emergency

[11] Defense-in-depth is the coordinated use of multiple security or risk management countermeasures, so that if one is not fully successful, the other layers of defense may still achieve the risk management goal.

[12] "Critical digital assets" is a nuclear-industry-accepted term for "digital computer and communications systems and networks" associated with safety, security, and emergency preparedness functions. By designating a system that monitors, operates, controls or protects the plant, or integrates any of these systems or functions as "critical digital assets," they establish that they must be isolated from the Internet.

preparedness functions, including offsite communications.[13] Presently, only licensed commercial nuclear power plants must comply with these cybersecurity regulations. The simplified cybersecurity defensive architecture illustration in Figure 2 is an example of NRC regulatory guidance.[14]

In the illustrated cybersecurity defensive architecture in Figure 2, data flow is controlled in prescribed directions. At the highest levels it is only one way in descending order, through mechanisms that enforce the security policies between each level. The distinction of the sensitivity of these levels reflects the significance of the systems that operate on them. At the lower levels, some data flow is allowed to go up from the public area of the network through the corporate area to equipment in the owner-controlled area. The approach to establishing boundary controls is not prescribed by the NRC. The data flow between levels can be accomplished through a deterministic device, such as a data diode that provides a hardware separation of the plant network or it could be accomplished through software, which uses rules to control the movement of data through firewall-like systems between the layers of the network. The nuclear power reactor industry has determined that all power reactors, both that are currently operational and those under construction are voluntarily committed to implement deterministic isolation technical measures and techniques to isolate plant safety and security systems.

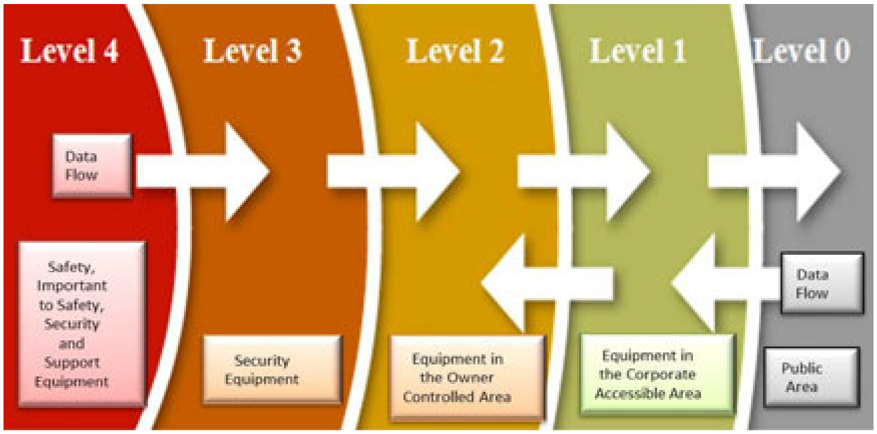
Level 4
Level 3
Level 2
Level 1
Level 0
Data Flow
Safety, Important to Safety, Security and Support Equipment
Security Equipment
Equipment in the Owner Controlled Area
Equipment in the Corporate Accessible Area
Data Flow
Public Area

FIGURE 2—EXAMPLE OF CYBERDEFENSE IN-DEPTH FOR NUCLEAR POWER PLANTS[15]

The NRC does not direct industry on how to achieve the requisite security. Operators can find the approach most suitable for their plant. Some cybersecurity experts have noted that each alternative approach to enforcing security among network security levels has its own limitations. The standard of care used in the commercial nuclear power industry is comparable to that used to protect U.S. Government classified networks. Thus, while it is not perfect, it represents the best known approach.

The nuclear industry relies on defense-in-depth. This means that in addition to the concept of cyberdefense-in-depth illustrated in Figure 2, industry standards demand employee and contractor diligence in following the site cybersecurity plan. Regulations also demand the use of rigorous approaches to personnel safety and security to help reduce insider threat. The Nuclear Physical Security Plan and Access Authorization include an Insider Mitigation Program as required by 10 CFR 73.55 and 10 CFR 73.56. In addition to the defense-in-depth approach that helps to preclude untrustworthy individuals from accessing sensitive systems either through the Internet or by becoming an insider, defense-in-depth also manifests itself in the engineering procedures which help to preclude errors from having a detrimental effect. These will be explored more fully in the section below.

NRC regulations also demand that access control systems ensure that only authorized individuals and equipment are allowed access to restricted access areas.[16] Access control portals are the locations and processes, where search equipment and personnel verify that unauthorized items do not pass into the protected area; operate

[13] The regulation requires licensees to protect digital computer and communications systems and networks from cyber attacks and NRC's Regulatory Guide 5.71 supports applicants' and licensees' efforts to meet these requirements. The guidance includes the traceability of standards organizations and agencies, such as the International Society of Automation, Institute of Electrical and Electronics Engineers, National Institute of Standards and Technology, as well as guidance from DHS.
[14] NRC Regulatory Guide 5.71, Cybersecurity Programs for Nuclear Facilities, January 2010, http://pbadupws.nrc.gov/docs/ML0903/ML090340159.pdf.
[15] Licensees are authorized to implement designs and architectures that meet the objectives of the regulation, but may differ from this example in specifics.
[16] U.S.NRC NUREG-1964, Access Control Systems.

alarmed entry control devices that prevent or delay, detect, and observe unauthorized entry; and personnel possess the capability to deny access and call for assistance, if needed. Access control lists specify who or what is allowed access to specific areas, and multiple factor authentications are required for vital areas.[17] A computerized database maintains the access list permissions approving or denying access to individuals attempting to activate an access point. Additionally, security personnel are required to perform physical tours of predetermined areas to look for any signs of tampering on critical systems or evidence of unauthorized entry. Compliance with these requirements provides a robust combination of cybersecurity and physical security controls.

POTENTIAL CONSEQUENCES OF CYBERSECURITY INCIDENTS

The protections achieved through compliance with regulations are expected to preclude any consequence from cybersecurity incidents in the Nuclear Reactors, Materials, and Waste Sector. If a cybersecurity incident should occur, the direct system and functional effects of such an incident would vary depending on the affected systems. In all cases, these incidents are expected to be recognized and addressed by back-up and mitigation procedures designed for safety and security. These back-up procedures aim for general safe operation of the plant, but serve as an additional layer of defense against harmful outcomes. If accidental introduction of malware occurs through improper procedures by well-intended personnel or through the use of compromised hardware or software, standard procedures can intervene to manage operational system failures and physical challenges, if the need arises.

In Tables 1 through 5, OCIA identified functions in the Nuclear Reactors, Materials, and Waste Sector that are commonly cyberdependent and provided examples of potential impacts of successful cybersecurity incidents affecting these systems. As a rule, the cyberdefense-in-depth precludes unauthorized access to systems if there is a possibility that manipulation of the system could be used for sabotage. Included below are records of observed incidents in which cyber attacks or information security problems appeared to affect infrastructure systems. The effect of these incidents on plant operations is explained, and in addition, descriptions of infrastructure impacts caused by events other than a cybersecurity incident are included to provide examples of infrastructure failure and outcomes comparable to what could have been caused by a successful cybersecurity incident. This is useful for understanding the many practical obstacles between an initiating problem in a nuclear power plant and a negative outcome that might affect the public.

Table 1 identifies computer systems that support access control. Licensees use layered defenses with technical sensors and security staff to monitor various spaces within their complex. In a computer-supported system, authorized access points use access-control systems to manage the validation of credentialed and approved personnel's access to sensitive spaces. Compromise of the computer systems that support these activities may prevent authorized personnel from accessing these spaces or may assist an adversary in gaining surreptitious access. Most, probably all access control systems are considered critical digital assets and are precluded from Internet access. The licensee determines which access control systems are critical digital assets, so a comprehensive statement cannot be made.

Access control management takes place for computer networks as well. The configuration of the network security architecture (see Figure 2) protects these critical digital assets from access through the Internet. These systems are on the network levels where equipment and operations important to safety and security are managed. Cybersecurity incidents here could be caused only by individuals who have unescorted access or equipment compromised before being connected to the network.

The licensee determines what access control systems are critical digital assets. If they are critical digital assets, only authorized workers would have access to the systems where they reside. This is an important feature of the current risk management.

[17] Vital areas are defined as areas in the nuclear facility around which protection will be provided to prevent or reduce the likelihood of sabotage, INFCIRC/225/Rev. 5 (IAEA Nuclear Security Series No. 13) [1].

TABLE 1—EXAMPLES OF POTENTIAL DIRECT EFFECTS IF CYBERSECURITY INCIDENTS AFFECT ACCESS CONTROL SYSTEMS

Potential Direct Effects of Cybersecurity Incidents—Access Controls				
Computer System Purpose	**Information Security Effect**	**Loss of Confidentiality**	**Loss of Integrity**	**Loss of Availability**
	Maintains access control authorization database.	A person with authorized access may gain personally identifiable information (PII) and general information about who has access.[18]	A person with authorized access may manipulate data to provide or deny access, or the access control system may malfunction.	Inability to manage access updates.
	Compares individual's credentials to lists and allows or denies access.	A person with authorized access may gain specific information of patterns of movement if logs are compromised.	A person with authorized access may manipulate data to provide or deny access, or the access control system may malfunction.	Difficulty in operating automated access control systems or triggering alarms; possible denial of all entry and exit.

Table 2 identifies computer systems that support building controls. Since the majority of nuclear power plants were built before environmental control systems became automated or any sector began using integrated control systems, there is a mixture of practices associated with the use of such controls among nuclear power plants. Those systems that have been replaced are more likely to have cyberdependent environmental controls. As new facilities are designed and built, the security issues and the potential direct effects of the failure of such systems would be considered in the design phase as a matter of routine. The nuclear industry would consider the operational experiences developed within other sectors where such innovations are more commonplace. In such a case, some of the considerations for designing with security in mind would include the potential direct effects of cybersecurity incidents that might affect the monitoring of the routine work environment. The Commercial Facilities Sector can be a good source of information, based on operational experience, for environmental controls that affect buildings within a complex that are not directly involved in the safe operation or security of a power plant.

Plant modifications must anticipate future cyber attacks by observing activities of adversaries in other sectors. Their goal is to neutralize the potential for a similar impact when the technology is introduced in the Nuclear Reactors, Materials, and Waste Sector. If a plant is being modernized or is in the design phase, the licensee must determine whether any such building control system is a critical digital asset and plan its cybersecurity accordingly.

[18] PII is personally identifiable information. Access controls sometimes require authentications at the time of establishing an account that would include PII.

TABLE 2—EXAMPLES OF POTENTIAL DIRECT EFFECTS OF CYBERSECURITY INCIDENTS IN BUILDING CONTROL SYSTEMS

Potential Direct Effects of Successful Cybersecurity Incidents—Building Controls				
	Information Security Effect	**Loss of Confidentiality**	**Loss of Integrity**	**Loss of Availability**
Computer System Purpose	Maintains programmed set points for heating, ventilation, and air conditioning (HVAC) systems.[19]	Adversary knows what the temperature settings are for various times of day.	Adversary can reprogram the settings.	Heaters or chillers may persist in whatever state they were set for, or may stop functioning; viruses may significantly slow response times.
	Maintains programmed schedule for lighting and any rules for response to sensors.	Adversary can reprogram the lighting configuration.	Adversary can deny access.	Lighting may persist in whatever state it was set for, or may turn off; viruses may significantly slow response times.

If the HVAC and water heating systems for administrative buildings were compromised, the result would be an inconvenience, an insignificant increase in operating costs, and concerns about cybersecurity. Requirements also exist to maintain effective operating conditions for computers supporting control systems. Nuclear power plants often have older engineering equipment, including control systems, and so their requirements for cooling and controlled environments exceed those of more modern equipment. In some cases, the building controls are tied into the safe operation of the plant. If the temperature goes above an acceptable threshold for safety-related operational spaces, an alarm is triggered to cue further operator actions.

If a cybersecurity incident were to disturb any automated lighting system, the plant staff would most likely override controls and restore lighting as needed. However, if a lighting control system were compromised, that would be within the scope of the NRC 10 CFR.1, “Design Basis Threat Scenario,” and plants would already consider it in their risk management and contingency plans.

Table 3 summarizes the roles of ICS in supporting the routine operations of the nuclear power plant. The defense-in-depth security afforded these critical assets precludes the possibility of anyone without insider access from being able to initiate a cybersecurity incident affecting these systems. In addition to these preventions and protections, in the event that preexisting undetected vulnerabilities or compromises in the digital equipment or software caused a problem, all digital systems important to safety have redundancy. Alternative non-digital means also exist to provide the indications or readings of critical parameters. All operators are trained to use procedures that preclude the usage of any one indication to make a decision in operating the plant. An attitude of questioning and safe, conservative decisionmaking are paramount in operating nuclear power plants. Even a knowledgeable insider would have to accomplish more than the compromise of these primary plant operations to sabotage the plant. The insider would have to sabotage other systems as well.

[19] Heating, Ventilation, and Air Conditioning; Water heaters are likely to follow similar patterns to the HVAC.

TABLE 3—EXAMPLES OF POTENTIAL DIRECT EFFECTS OF CYBER INCIDENTS IN NUCLEAR REACTOR AND POWER-GENERATION OPERATIONS

Potential Direct Effects of Successful Cybersecurity Incidents—Nuclear Reactor Operations				
	Information Security Effect	Loss of Confidentiality	Loss of Integrity	Loss of Availability
Computer System Purpose	Monitor plant operations	Adversary knows the state of the plant operations.	Adversary could present a false view of the overall plant, potentially initiating an automated shutdown.*	Inability to monitor the plant operations as a whole. Plant would likely be shut down if this is discovered. ***
	Control nuclear chain reaction	Adversary knows the state of the reactor and possibly the state of the fuel configuration.	Adversary could present a false view of the reactor, potentially initiating an automated shutdown.	Inability to manage the reaction. Plant would be brought to a safe shutdown.
	Generate steam	Adversary understands the amount of heat being drawn from the reactor and generator capacity.	Adversary can present a false view of the activity and equipment involved in removing heat from reactor to turbines.	Inability to control reactor or know the state of heat supply to the generator. Plant would be brought to a safe shutdown. **
	Convert kinetic energy to electricity	Adversary understands the electrical generation capacity and performance.	Adversary can misrepresent the electricity being produced, demanding additional operator actions to prevent errors.	Inability to safely manage contribution to the electrical grid. Plant may be disconnected from the grid manually by an authorized operator, or, if an adverse condition continued an automatic turbine or reactor trip would occur.
	Post generation cooling	Adversary understands the amount of residual heat that must be dissipated in a heat sink.	Adversary can misrepresent the residual heat and demand additional operator actions to prevent errors that harm equipment, and possible shutdown.	Cooling is necessary. Human operators would need to detect the condition and initiate responses on their own.

* On March 7, 2008, Unit 2 of the Hatch nuclear power plant near Baxley, Georgia, automatically shut down after an engineer applied a software update to a single computer on the plant's business network. The computer was used to collect diagnostic data from the process control network; the update was designed to synchronize data on both networks. When the engineer rebooted the computer, the synchronization program reset the data on the control network. The control systems interpreted the reset as a sudden drop in the reactor's water reservoirs and initiated an automatic shutdown. This innocent mistake demonstrates how malicious hackers could make simple changes to a business network that end up affecting a nuclear reactor—even if they have no intent to interfere with critical systems. It also demonstrates that plant operators in this case did not fully understand the dependencies between network devices. This would make it difficult to identify and protect all the vulnerabilities in a process control system.

** In January 2003, the Slammer worm infected computer systems at the Davis-Besse nuclear power plant, Ohio. The worm traveled from a consultant's network to the corporate network of First Energy Nuclear, the licensee for Davis-Besse, then to the process control network for the plant. The traffic generated by the worm clogged the corporate and control networks. For 4 hours and 50 minutes, plant personnel could not access the Safety Parameter Display System. Since Slammer did not affect analogue readouts, plant operators could still get reliable data.

Davis-Besse had a firewall protecting its corporate network from the wider Internet, and its configuration would have prevented a Slammer infection. However, a consultant had created a connection behind the firewall to the consultancy's office network. This allowed Slammer to bypass the firewall and infect First Energy's corporate network. From there, it faced no obstacle on its way to the plant control network. In response, First Energy set up a firewall between the corporate network and the plant control network.

The Davis-Besse incident highlighted the fact that most nuclear power plants, by retrofitting their SCADA systems for remote monitoring from their corporate network, had unknowingly connected their control networks to the Internet. At the time, the NRC did not permit remote operation of plant functions.

*** The August 19, 2006, shutdown of Unit 3 at the Browns Ferry nuclear plant near Athens, Alabama, demonstrated through an unexplained malfunction that critical reactor components could be disrupted and disabled by a cyber attack. The condensate demineralizer used a programmable logic controller; the recirculation pumps depend on variable frequency drives to modulate motor speed. Both kinds of devices have embedded microprocessors that communicated data over the Ethernet Local Area Network. However, both devices are prone to failure in high traffic environments. A device using Ethernet broadcasted data packets to every other device connected to the network.

The receiving devices examined each packet to determine which ones are addressed to them and to ignore those that are not. It appears the Browns Ferry control network produced more traffic than the programmable logic controller and variable frequency drive controllers could handle. It is also possible that the programmable logic controller malfunctioned and flooded the Ethernet with spurious traffic, disabling the variable frequency drive controllers. Tests conducted after the incident were inconclusive. Each case had an effect like a denial-of-service attack. The failure of these controllers was not the result of a cyber attack. However, it demonstrates the effect that one component can have on an entire process control system network and every device on that network.[20]

Table 4 describes the possible direct effects of cybersecurity incidents in systems that integrate data monitoring, provide alerts, and trigger automated responses. Some overlap exists between the plant operations affected by these systems and those in Table 3, which reflects the redundant back-up role for these warning and alert systems. These systems receive input from monitoring equipment and respond automatically if the input reflects a threshold requiring a programmed response. These responses may be in the form of messages, audio alerts, or some other notice of the condition. Other responses may serve as automated triggers of safety responses. In a nuclear power plant, the alarm and warning functions can be divided into those that monitor the operational environment to meet special standards and requirements beyond the demands of routine building environmental control systems, and those that monitor the state of equipment necessary for the safe and secure operations of the plant. Some of these systems would rely on hardware and software considered critical digital assets and protected from any connection to the Internet, on the highest level of security for the layered defense.

[20] Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," Strategic Insights, Spring 2011, accessed February 19, 2015.

Commercial nuclear power plants must have technical system support for the following functions. This support often involves monitoring equipment with automated alerts and operational responses:

- **Perimeter Security—**Detects intrusions into a no-man's land triggering a security force response.[21]
- **Reactor Protection—**Detects operational parameters that trigger an immediate termination of the nuclear reaction.
- **Emergency Core Cooling System—**Allows the plant to respond to a variety of unsafe conditions and adds a layer of redundancies so that the plant can be shut down even when one or more subsystems have failed. These include the following:
    - **High-Pressure Coolant Injection System—**Monitors the level of coolant in the reactor vessel and automatically injects coolant when the level drops below the established threshold.
    - **Automatic Depressurization System—**Opens to vent steam into pressure-controlled containments.
    - **Essential Service Water System—**Circulates the water that cools the plant's heat exchangers and other components before dissipating the heat into the environment.
- **Emergency Electrical System—**Includes the transitions to and from reliance on a flywheel to a diesel generator or battery.
- **Standby Gas Treatment, Ventilation, and Radiation Protection System—**Protects plant personnel and the public from radiation that could escape the primary containment system.
- **Spent Fuel Management System—**Includes water-cooled and dry storage. Spent fuel produces residual decay heat for decades after its productive life that must be removed to protect the fuel from overheating, rupturing the metal cladding on the rods, catching fire, and releasing radioactive substances into the environment.

A computer system of the type that supports the above functions may be considered a critical digital asset and given the highest level of protection and separation from outside access. It would be a mistake to construe that a direct cause and effect relationship exists between the compromised performance of any of these systems and an out-of-control reaction, releasing radioactive material, with an impact on the public or the environment. Each of these systems supports the efficient and safe execution of a function that human operators can perform on their own.

[21] Commercial nuclear power plants include a band of secured space between their outer perimeter and the space that demands protection. This slows an adversary's progress toward incursion and increases the available response time for the security force.

TABLE 4—EXAMPLES OF POTENTIAL DIRECT EFFECTS OF CYBER INCIDENTS IN SYSTEMS SUPPORTING ALERTS, WARNINGS, AND AUTOMATED RESPONSES

Potential Direct Effects of Cybersecurity Incidents—Alerts and Warning Systems, Automated Response				
	Information Security Effect	**Loss of Confidentiality**	**Loss of Integrity**	**Loss of Availability**
Computer System Purpose	Maintains normal system operating parameters.	Adversary knows what required conditions are.	Adversary can reprogram the boundary.	System will be out of service, or responses significantly delayed.
	Issues alerts or alarms when sensor readings fall outside of acceptable conditions.	Adversary knows when the measured inputs vary enough from condition boundaries to trigger an alert.	Adversary can trigger false alarms, suppress alarms, or alter the recipients of the alarms.	System will be out of service not sensing alarm conditions; system may revert to and stay in alarm status.
	Automatically triggers an operational safety response.	Adversary knows the steps and messages that trigger the operational safety response.	Adversary can alter the messages or responses that trigger operator safety response, resulting in no or delayed response.	The operational safety response system could fail to respond. Human operators would need to detect the condition and initiate responses on their own.

Fuel fabrication facilities use SCADA systems to automate the uranium enrichment processes, including the control of centrifuges and other industrial equipment. These control systems perform the same types of integrated monitoring and automated control functions seen in other industrial production processes, but with additional attention to requirements for monitoring the safety and security of the nuclear fuels themselves. Fuel fabrication is of particular note as an example in understanding the role of cyberdependencies in the nuclear industry. Iran's nuclear enrichment facility experienced such an infection in 2010 through a portable device (thumb drive) containing malware that was carried into the facility and inserted into a system. This Iranian facility had defense-in-depth cybersecurity similar to U.S. nuclear facilities, so the impacted system could be affected only through an intentional act or careless mistake.

Hardware or software may also be contaminated in the supply chain. To control such risks, nuclear plant safety components are subject to nuclear quality requirements. Safety-related components will be protected via supply chain provisions of the vendor per requirements in 10 CFR Part 21 when full compliance is achieved in 2017. Licensees look to DHS and ICS Procurement Guides as well as National Institute of Standards and Technology (NIST) for supply chain protection effectiveness for their critical digital assets.

Table 5 presents the potential infrastructure effects of cybersecurity incidents that affect the business management processes, such as payroll and supply chain management. The NRC regulates none of these systems. The internal business management systems must be isolated from digital critical assets and considered susceptible to cybersecurity risks that relate only to cybercrimes or other exposures common to major businesses, as opposed to risks of physical or operational impacts of reactors. These risks affect the electrical generation companies and employees, not the nuclear reactor operations.

Producers of electricity are also involved in selling electricity. These business management systems are typically carried out on the Internet. Any cybersecurity incidents that take place in the business systems are distinct in their potential direct effects from those that affect the security and physical operations of the nuclear power plant. The business systems are separated from the critical digital assets by the requirements of the defense-in-depth strategy. Effective cybercrimes that compromise the business activities of the electricity provider may be both possible and profitable, but they would not affect the safe and secure operation of the nuclear power plant itself.

TABLE 5—EXAMPLES OF POTENTIAL DIRECT EFFECTS OF CYBER INCIDENTS AFFECTING NUCLEAR POWER PLANT BUSINESS MANAGEMENT SYSTEMS

Potential Effects of Cybersecurity Incidents—Internal Business Management Systems				
	Information Security Effect	**Loss of Confidentiality**	**Loss of Integrity**	**Loss of Availability**
Computer System Purpose	Payroll Management	PII and financial information may be exposed, and company has compliance concerns.	Adversary can alter payroll actions, add, or subtract payees, etc.	System will be out of service. May delay pay or have a work-around.
	Inventory Management	Adversary may know the quantity of inventory in different locations.	Adversary can alter inventory data so that the firm runs out or over orders.	System will be out of service, possibly with inadequate manual inventory processes.
	Supply Chain Management	Adversary may know the inventory thresholds and status and procedures for reorder. Some customer and business proprietary data could be stolen.	Adversary can disrupt the supply chain management or cause an over-order or under order, or redirect deliveries.	System will be out-of-service and manual back-up systems are used.
	Electronic Bulletin Board Interface for Market Participation	Adversary knows the offer and potentially other proprietary or business sensitive information that leads to competitive advantage.	Adversary or competitor could alter offer details and undermine electricity producer's profitability.	Electricity provider must make offers by phone or fax.

POTENTIAL FOR CASCADING CONSEQUENCES

No evidence suggests a significant risk exists for a cybersecurity incident to trigger a series of cascading failures or dysfunctions that could result in an offsite release of radioactive materials. If such a release were to occur from any cause, plans and preparations are in place to respond.

If a nuclear power plant were to go offline abruptly for any reason, there is a risk of grid effects from the sudden loss of a large amount of electrical generating capacity. In a period of peak demand, the loss of electricity may be difficult to replace promptly with standby capacity, but grid managers have the ability to control the demand to keep the grid in balance with a loss of supply. Grid operators may drop portions of the grid to control this demand, bringing the affected areas back online as the supply becomes commensurate with demand.

If such an incident caused a non-power reactor to shut down, the impact to watch for would be on the production of medical isotopes and materials used for diagnoses and therapies. Similarly, the Chemical Sector, the Critical Manufacturing Sector, and the Food and Agriculture Sector use small amounts of radioactive materials. A temporary loss of production by one non-power reactor would not significantly affect these Sectors because of the low demand for radioactive materials and the lack of "just-in-time" delivery demands.

PATH FORWARD

Prior to the attacks on September 11, 2001, the Nuclear Reactors, Materials, and Waste Sector approached cybersecurity individually with suggested risk-based guidance from regulators. Today, the NRC's cyber security regulations apply to all commercial nuclear power plants. The nuclear power portion of the Sector is protected by the implementation of 10 CFR 73.54, consistent with the guidance offered in RG 5.71 or per NEI 08-09 Revision 6. The rule and the guidance document contain security characteristics demonstrated to be effective by such entities as the International Society of Automation, Institute of Electrical and Electronics Engineers, and DHS. NIST provided specific guidance, which was implemented by the NRC as evidenced through the content of RG 5.71.

Nuclear power plants, non-power reactors, and fuel-cycle facilities are configured with differing levels of ICS digital connectivity. The rigid physical protection in the transportation element of the Nuclear Reactors, Materials, and Waste Sector makes a successful attack in this element difficult to orchestrate. If a cyber attack were successful, the physical protections required by regulation would severely impede attempts to steal radioactive material. Physical protection in all four elements of the Nuclear Reactors, Materials, and Waste Sector includes layers of security containment that are extensive and regulated.

The common air-gapped configuration of the ICS equipment in nuclear power plants makes an attack through the Internet improbable, if not impossible. The most likely threat vectors for a cyber attack in the Nuclear Reactors, Materials, and Waste Sector include the intentional or unintentional insider using portable devices and media. Processes and procedures are management and operational controls for protection of ICS equipment; plants implement technical controls such as physical blocking of unused ports as necessary.

The importance of communication and information sharing within and between the public and private sector members of each critical infrastructure sector cannot be overstated. Executive Order 13636 emphasizes that increased protection and defense against cyber attacks is reliant upon information sharing and collaboration between all entities.[22] Cybersecurity information sharing groups include the United States Computer Emergency Readiness Team, Industrial Control Systems Computer Emergency Readiness Team (ICS-CERT), Cross-Sector Cyber Security Working Group, and the NGCC/NSCC Joint Cyber Subcouncil.[23] The sharing of threat information is supported through the DHS National Operations Center, the NRC Headquarters Operations Center, FBI Strategic Information and Operations Center, and the National Cybersecurity and Communications Integration Center.[24]

DHS coordinates a monthly unclassified threat briefing via teleconference for the Nuclear Reactors, Materials, and Waste Sector. The Sector also receives quarterly classified threat briefings. The monthly and quarterly briefings address both cyber and physical threats to the Sector.

The nuclear energy industry has been implementing and improving cyber security controls since 2002. The industry's programs are being enhanced to meet the NRC cyber security requirements.

Compliance with the strict regulatory requirements of the Nuclear Reactors, Materials, and Waste Sector makes Sector assets difficult targets for physical or cyber attack. Power reactors are implementing cybersecurity programs to meet the NRC's new requirements following an NRC-approved schedule. They have already achieved the milestone of enhancing or instituting protective measures to address the most prominent threats to the plant's most important systems.

Full implementation of cybersecurity programs in nuclear power plants is under way with target completion and inspection dates for some facilities as early as 2016.[25] These final activities include the completion of policy and procedural revisions that enhance existing capabilities, the completion of any design-related modifications necessary to implement the Cyber Security Plan, and institution of protective measures for lower consequence assets. Licensees have asked for extensions for meeting the final milestone implementation date. Construction of four new Westinghouse AP1000 nuclear power reactors (VC Summer Units 2 and 3 and Vogtle Units 3 and 4) has been approved by the NRC.[26] These new reactors will be designed with features that will make them inherently more secure and safer to meet the requirements of 10 CFR 73.54.[27]

The majority of nuclear power plants were designed and built before the cybersecurity threat materialized. The use of intelligent devices to support the operation of plants is not a substitute for, but a support to human operators. The capability to manage the operations is redundant. Trained to question inputs, operators would verify indicators before making any changes to plant operations. As control systems and devices are added to the enterprise architecture, extreme care is taken to determine the possibility of connectivity to the Internet and to

[22] Executive Order 13636-Improving Critical Infrastructure Cybersecurity (2013), p. 11739, Sec. 4.
[23] Nuclear Reactors, Materials, and Waste Sector-Specific Plan (2010), pp. 106 and 107, section 8.4.1.3.
[24] Ibid.
[25] The Nuclear Regulatory Commission Cyber Security Roadmap (2013), p. 11.
[26] Nuclear Energy Institute (2013). Five New U.S. Reactors Reach Milestones.
[27] Office of Nuclear Security and Incident Response (2011), Protecting Our Nation: A Report of the U.S. Nuclear Regulatory Commission, NUREG/BR-0314, Rev. 2.

screen for potential contamination of the supply chain. The industry has embraced conservative risk management objectives and is on the way to fulfilling them. At this time, based on what has been implemented, the overall operational and regulatory requirements of the nuclear industry substantially avoid the possibility of a cybersecurity incident having a significant effect outside of the plant. Additional programmatic elements included in the final milestone will enhance the cybersecurity program, and will make the possibility of a cybersecurity incident occurring in the isolated and protected networks of a plant extremely low.

The Office of Cyber and Infrastructure Analysis (OCIA) provides innovative analysis to support public and private-sector stakeholders' operational activities and effectiveness and impact key decisions affecting the security and resilience of the Nation's critical infrastructure. All OCIA products are visible to authorized users at HSIN-CI and Intelink. For more information, contact OCIA@hq.dhs.gov or visit http://www.dhs.gov/office-cyber-infrastructure-analysis.