SECURITY CONSIDERATIONS IN NEW REACTOR CONSTRUCTION
AND
U.S. VIEWS ON SOURCE SECURITY

Remarks by Victor M. McCree
Executive Director for Operations
U.S. Nuclear Regulatory Commission
at the
Second International Regulators Conference on Nuclear Security
May 13, 2016

Good morning. I am pleased to be here at the second International Regulators Conference on Nuclear Security to support international cooperation on this important topic. It has been a very interesting couple of days, and I hope my remarks can make a contribution to the extensive sharing of knowledge and experience that has occurred.

The bulk of my remarks will focus on security considerations in new reactor construction. I chose this topic, in part, because of my past experience overseeing new reactor construction in the United States. Prior to assuming my current position as NRC Executive Director for Operations last fall, I was the Administrator of the NRC's regional office in Atlanta, Georgia. That office is responsible for overseeing the construction of four new commercial reactor units under development at two sites in the States of Georgia and South Carolina.

My remarks today will focus on three aspects of security in new reactor construction: physical security, the safety/security interface, and cyber security. I also have noticed that my remarks precede a session on security of radioactive sources. Because there is no U.S. speaker on that panel, I thought I would conclude my remarks with some comments on source security issues and activities in the U.S.

Physical Security Challenges for New Nuclear Reactors

So, let me begin with some thoughts on approaching physical security challenges in new reactor construction. In our continually changing threat environment since the events of September 11, 2001, the security of nuclear reactors has become increasingly important, not only for operating reactors, but also for future commercial nuclear power reactors. New nuclear reactors must be adequately protected from physical security threats, even as they continue to evolve.

For currently operating reactors, the design of physical protection systems often occurred after structures were initially designed and constructed. The security approaches often relied heavily on human actions for adequate security responses to protect the nuclear power plants from the design basis threat.

Both the evolving threat and economic environments we face today make it essential that we look closely at the design of physical protection systems so that there is high assurance that they can meet the challenge of protecting a nuclear power plant against a design basis threat in a manner that is both efficient and effective.

The key to meeting the challenge of securing new nuclear reactors efficiently and effectively is early consideration of security along with safety in the design process.

The NRC now has recent experience in certifying designs and licensing new reactors that considered both safety and security early in the design process. This experience shows that efficiencies can be realized through plant configurations and engineered security systems, and that we can reduce reliance on human actions. Some examples include:

- Designing buildings with only the necessary exits and entrances, which are hardened and can be controlled remotely in a threat event.
- Configuring buildings to limit pathways available between building areas and between floors to isolate and contain the design basis threat.
- Designing buildings and configuring sites to minimize the number of security responders needed to implement a denial strategy.
- Integrating security response or fighting positions into building perimeter walls. They are protected against ballistics and blasts and are only accessible from inside the buildings. These configurations allow security responders to readily change from an external to an internal protection strategy. And,
- Including in the designs the option to use engineered remotely operated weapons systems to perform security functions necessary for implementing a combined external and internal protection strategy.

Through proactively integrating and balancing safety and security early in the design process, future reactors can realize efficiencies to protect against the changing threat environment.

The need to consider both safety and security early in the design process is not limited to new large light-water reactors. Some designers of small modular reactors have further leveraged buildings designs and site configurations with security in mind. For example:

- One designer plans to apply the concept of material access areas from non-reactor facilities to separate the compact reactor and systems from other plant areas. This configuration keeps all non-reactor systems and activities outside a protected area and restricts access to only those personnel needed for operations. And,
- A proposed standard configuration, with the end user input early in the design process, applies some of the same design features and configurations previously mentioned, and the designer expects to allow an operating license to meet the current regulatory requirements with greater efficiency and effectiveness.

We expect that future small modular reactor designers will reduce reliance on human actions through the use of engineered systems and new technologies in their designs of a physical protection system.

The NRC also has considered the need to incorporate security in advanced reactor designs. The NRC's final 2008 Policy Statement on the Regulation of Advanced Reactors included several new items to be considered during the design of such reactors; included among them is security. The Commission provided these additional expectations and guidance so that prospective applicants could use this information early in the design stage of advanced reactors to identify potential mitigative measures and/or design features that provide a more robust and effective security posture with reduced reliance on human actions.

Again, the construction of new commercial nuclear power reactors must include designs that reflect the needs of both safety and security. This will only be accomplished if the design phase also embraces security considerations early in the process.

Managing the Safety/Security Interface

Now let me talk a little more directly about the safety/security interface. This is not a new concept. At the NRC, managing the safety/security interface is a requirement that was included in the 2009 revisions to nuclear power plant security regulations and related guidance. These materials establish the principle that licensees must assess and manage the potential for adverse effects on safety and security before implementing changes to plant configurations, facility conditions, or security. While the focus traditionally has been on the safety/security interface when licensees consider modifications to current nuclear power plants, the agency's guidance on this matter is also available for consideration by entities preparing applications for new reactors that will need to address this interface during both design and construction.

The requirement is intended to ensure that plant change controls and processes embrace the need to review changes for possible effects on safety and security prior to their implementation. It increases awareness of the need to manage both safety and security requirements without one negatively affecting another. The expected outcomes are that changes do not result in unintended negative effects on engineered and administrative controls to perform their intended and required safety or security functions.

I want to describe several examples where inadequate management of safety/security interfaces caused unintended effects:

- One facility made improvements that inadvertently created openings bypassing or circumventing physical barriers relied on for security delay and access control.
- Another facility conducted maintenance on electrical power systems that inadvertently caused the loss of primary power to the plant security detection and assessment systems.

- During maintenance activities, a plant erected scaffolding and staged temporary equipment in the protected area of the plant, inadvertently blocking security lines of sight for assessment and neutralization functions.
- As part of a security upgrade, one facility locked doors and gates that could have inadvertently prevented or delayed operators from being able to access safety-related equipment and perform time-critical operator actions.
- And, finally, another facility installed fencing for security that potentially denied or delayed operator access to safety equipment in the event of an emergency.

As you can see, at currently operating facilities, some licensees established controls and processes to evaluate safety issues, but security and/or interfaces between safety and security have not always been included. These actions were taken despite some already established controls and processes at power plants, including plant operations review committees; safety review committees; engineering, design, and project management; work planning and control management; configuration management; procedure change reviews and controls; assessments and audits; corrective actions and reporting; and maintenance, testing, and surveillance management.

What that tells us is that heightened emphasis using these existing controls and processes is needed to manage the interface between safety and security; and, in doing so, ensure that the assessment and management of facility changes and activities includes security. The managing of safety/security interfaces does not require new processes, but only that those existing processes already in place account for safety and security together.

Collectively, these controls and processes must assess, identify, and resolve any potential unintended adverse effects before changes are implemented. Several good practices have been revealed from the successful integration of these controls and processes, including:

- The security organization is notified of potential changes to the characteristics of the site's physical layout (including topographical changes); configurations of facilities, structures, systems and components; the site's operational procedures; and day-to-day or planned activities.
- The security organization actively participates in change processes, reviewing proposed changes and activities to identify potential adverse impacts on the functions and performance of elements of the site's security programs. And,
- Where changes are predominantly driven by security, integration of such changes in the plant change control processes provide the opportunity for operations, safety, and emergency preparedness organizations to identify potential adverse impacts on safety and preparedness functions, prior to implementing any security changes.

Without consideration and integration of safety and security, whether it is in the design processes for a new reactor to be constructed, during construction of a new reactor, or at a currently operating reactor, unintended consequences that potentially affect the efficiency and effectiveness of the safety or security programs and actual degradation of safety and/or security conditions may occur. In short, an effective safety and security interface program is essential for safe and secure operations at both existing and new reactors in today's changing threat environment.

Cyber Security

Let me now turn to cyber security. I know NRC Commissioner William Ostendorff in his remarks the other day provided a high-level overview of the NRC's approach to cyber security controls – requiring preparation of cyber security plans, pursuing a phased approach to implementation, and the process for identifying critical digital assets. I'd like to provide some additional details on that phased approach and our other implementation activities.

Power reactor licensees are following a two-phased approach for implementation of the cyber security requirements. During the first phase, cyber security controls were implemented to protect the most significant digital components from the most significant threat vectors. This phase was completed by all licensees in December 31, 2012, and the NRC completed the first-phase inspections at all the facilities in 2015. In 2016, the NRC is following up on the identified violations and findings from the first phase inspections by reviewing licensee corrective actions.

The second phase relates to the full implementation of licensee's cyber security plans; which adds additional defense-in-depth, including the full implementation of technical controls, monitoring and detection capabilities, and incident response training and drills. Full cyber security plan implementation is currently required to be completed between 2016 and 2017. The NRC staff plans to work with industry to engage with them in preparation for full cyber security implementation through additional pilot inspections, tabletop reviews, workshops, and other activities.

The NRC also recently began to implement new cyber security event notification regulations that require, among other things, prompt notification to the NRC after discovery of a cyber attack that adversely affected or could have adversely affect safety-related or security functions. The NRC issued a companion regulatory guidance document that provides an acceptable approach for meeting these regulatory requirements and includes examples of cyber security events and the timelines required for notification. The Nuclear Energy Institute, a nuclear industry organization, also has developed a guidance document to support licensees in meeting their obligations.

With respect to reactors under construction, the NRC is actively working with those licensees to understand key design elements and their schedules for implementing the cyber security requirements. In accordance with NRC requirements, a licensee must implement its cyber security program prior to fuel delivery on site. The NRC is also in the final stages of issuing a construction cyber security inspection procedure for use by the agency during inspections at new reactor construction.

Regarding other types of NRC licensees, in 2012, the NRC staff provided a paper to the NRC Commission that outlined the status and path forward for a number of other license categories. As a result, thus far, the Commission has directed NRC staff to undertake a high-priority rulemaking to develop cyber security requirements for fuel cycle facility licensees, while the staff continues to conduct site visits, evaluations, and information gathering on other types of NRC licensees. As with power reactors, we are taking a graded approach as we look at other types of NRC license holders.

Source Security

I'd like to spend the last few minutes of my remarks on the subject of source security as conference participants transition into the next session.   The security of radioactive sources has been, and continues to be, a top priority for the NRC and other government agencies in the United States. In the U.S., 37 of the 50 States have entered into agreements with the NRC that give them the authority to license and inspect byproduct, source, or special nuclear materials used or possessed within their borders. The NRC works diligently with these partners and others to ensure that the appropriate safety and security requirements are implemented for risk-significant radioactive materials without discouraging their beneficial use.

Following the terrorist attacks of September 11, 2001, the NRC evaluated the potential vulnerabilities associated with the use and transport of risk-significant radioactive materials. At the time, the NRC issued orders to licensees to require certain protective measures. Subsequently, in 2013, the NRC issued a new regulation entitled "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material." The rule contains requirements such as:

- Access controls, including fingerprinting and background checks, for personnel with unescorted access to risk-significant radioactive materials;
- Detection, assessment, and response capabilities for unauthorized access to material or attempted removal of material;
- Transportation controls for the physical protection of radioactive materials while in transit; and
- Provisions for the protection of information that is important to the security of the material.

The NRC also regularly coordinates with the intelligence community and domestic law enforcement organizations to review and assess threat information and incorporate a graded threat concept into security programs.

To further support licensees, who have the ultimate responsibility for securing radioactive materials they possess, the NRC coordinates with other Federal agencies, such as the U.S. Department of Energy; materials licensees; and State, local and Tribal governments to build on the existing regulatory requirements through development of voluntary security enhancements and other efforts. Voluntary enhancements are complementary to, and do not replace, the licensees' obligation to meet NRC regulatory requirements. Examples of voluntary enhancements include:

- Removal of unused radioactive sources;
- Security upgrades, including in-device delay mechanisms and other hardware;

- Specialized training for local law enforcement personnel; and
- Training exercises to promote cross-communication, cooperation, and appropriate response to terrorist acts involving radioactive materials.

Moving on to the area of radioactive source control, in 2008 the NRC established the National Source Tracking System (NSTS) to track source transactions involving risk-significant radioactive sources. Now in its eighth year of operation, the NSTS has tracked over 500,000 transactions, primarily from licensees in the fields of industrial radiography, blood and research irradiators, large industrial irradiators, and source manufacturers. Approximately 1,400 licensees report information on over 75,000 sources using the system.

The NSTS has been integrated with two other licensing systems, the Web-based Licensing (WBL) system and the License Verification System (LVS), to support NRC's Radioactive Material Security Program and related radioactive materials licensing and tracking activities. Integration of the three systems significantly increases the security and accountability of these sources.

The United States has also established an interagency task force on radioactive source protection and security under the lead of the NRC to evaluate and provide recommendations to the President and Congress relating to the security of radioactive sources. Twelve federal agencies, as well as State and other Federal organizations, participate in the task force. The task force convenes routinely to assess ongoing safety and security issues, and prepares reports on the status of its activities every four years. Since 2006, the task force has issued three reports that identified recommendations for enhancing control and accountability for risk-significant radioactive sources. The enhanced interagency relationships have allowed for successful implementation of a number of activities to improve the life-cycle management of sealed sources.

Additionally, the NRC actively participates in multiple international efforts to ensure the safety and security of sources worldwide.

In summary, the NRC recognizes the direct role that radioactive source security plays in the protection of public health, safety, and the environment. Source security is a dynamic topic, given that the use of radioactive sources plays a vital role in many areas of public health and safety, including medical, industrial, academic, and research applications. As a regulatory body, the NRC has taken action to develop a comprehensive regulatory program that consists of legally binding requirements supported by descriptive guidance; electronic data tools; and routine, predictable oversight of licensee compliance and performance.

Closing

I'd like to close by circling back to the main topic of my remarks today – security considerations in new reactor construction. The security of nuclear facilities and materials licensees that the NRC regulates has been and will remain a priority. Currently, NRC-regulated nuclear facilities are considered among the most secure parts of the United States' critical infrastructure. Our aim is to continue this high level of security, while ensuring that new nuclear facilities are designed to achieve a similar goal. Early consideration of both security and safety in the design process should enable this goal to be achieved more efficiently.

It has been a pleasure participating in this important conference and an honor to speak to you today. Thank you for your attention.