U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NRC NEWS
Office of Public Affairs, Headquarters
Washington, DC. 20555-0001
www.nrc.gov ■ opa.resource@nrc.gov

No.: S-16-014 December 9, 2016
Contact: Office of Public Affairs, 301-415-8200

International Conference on Nuclear Security: Commitments and Actions
December 9, 2016
Vienna, Austria
Remarks as Prepared

"U.S. NRC Perspectives on the Security of Nuclear Installations and Radiological Materials"

Thank you for asking me to speak today as part of this important ministerial conference on security. I'm pleased to be among my international colleagues and have enjoyed the productive interactions both within the formal sessions and in the hallways, over coffee and during other opportunities for informal conversation.

It is true that the security of nuclear installations and radiological sources is no small matter for the U.S. Nuclear Regulatory Commission or for any nuclear regulator around the world. Some 15 years after the events of September 11, 2001, regulators remain in a defensive mode ensuring protection of nuclear installations from threats both internal and external, improving nonproliferation efforts, and working well together as we address concerns both specific to our countries and pervasive around the world.

There remain many challenges. The terrorist threat from groups such as ISIS, insider threats, increasingly sophisticated cybercrime, and the possibility of new and advanced reactors with unique security features are much more than mere headlines in the media. They are what we as regulators now must consider day in and day out when crafting our defensive strategies.

Let me briefly touch on a few topics on which, I believe, we must remain focused.

First, let me state the obvious ─ physical security of our nuclear installations can never be taken for granted. In the United States, guns, guards, gates along with solid planning, access authorization and behavioral observation policies, and highly realistic mock adversary experiences, are bedrock principles. Such measures for prevention and protection are rooted in the principles of defense in depth.

While not all security regimes follow the U.S. model, security practice around the world is and must continue to be a potent mixture of hardware, procedures, facility design, physical barriers or other technical means, guards and response forces, and a trusted, reliable and properly vetted workforce. Our respective countries count on us to put regulations and oversight in place that makes physical security of nuclear infrastructure beyond reproach.

Evaluation of the threat and assessment of the risk is an ongoing process. In the United States, the Design Basis Threat – the DBT – takes into account the changing threat landscape and is subject to constant re-evaluation. DBTs as a concept are embraced by the IAEA. They are generally derived from a number of important themes: the potential adversary, including motivation and capability, the consequences of the malicious act, the design and implementation of physical protection, the type of facility being protected, and perhaps the culture and tradition of the state in which the installation resides.

In the United States, the foundation of the security framework for a nuclear power installation is the DBT. The DBT itself, which is reflected in the NRC's publicly available regulations, is a performance-based standard that outlines the general adversary characteristics licensees must defend against. Licensees use the DBT to design their protective strategies, but the NRC does not dictate precisely the details of those strategies. It is also important to note that, since U.S. installations are guarded by private security forces, the NRC has accounted for this by defining the DBT as the largest adversary against which private security forces can reasonably be expected to defend.

The ability of our licensees to defend against the DBT is periodically tested during rigorous force-on-force security inspections conducted by the NRC at nuclear power facilities. These simulated combat engagements were significantly enhanced after September 11, with stronger mock adversary forces, added realism and increased frequency.

The NRC inspection team monitors all aspects of the four-week-long inspection and any potentially significant findings identified are promptly reviewed, addressed and corrected before the NRC inspectors leave the facility no matter what time of the day or night.

While the visuals of a mock adversary force attacking an installation are dramatic, perhaps the more important element of these inspections is the planning that goes into them. The process of planning and thinking in anticipation of the inspection is as important as what happens that night. As President Dwight D. Eisenhower once said: "I have always found that plans are useless, but planning is indispensable."

The NRC incorporates lessons learned from past force-on-force inspections when making enhancements to procedures and inspector training programs. As the threats change, as the program evolves, and as inspectors learn from the exercises before, this program only grows in sophistication, and benefits the entire industry and regulators around the world.

Much less visible to the public, but no less important, is the challenge of cyber security. The NRC has sought to be forward-thinking in developing cyber security requirements for nuclear power installations. The cyber threat is always evolving, and so must be our readiness to defend against it.

The NRC originally imposed cyber security requirements on nuclear power installations in Orders issued after the September 11, 2001, terrorist attacks. Drawing on our experience with those early measures, we formalized more comprehensive regulations in 2009. Our "cyber security roadmap" spells out how nuclear plant licensees have been implementing our 2009 cyber regulations, as well as our approach to assessing cyber needs of other classes of licensees.

Using an approach that prioritized the protection of the most safety significant digital equipment, nuclear plants are meeting these requirements in two phases.

During Phase 1, they implemented controls to protect their most significant digital assets from the most prevalent cyber attack vectors. This phase was completed in December 2012, and our inspections of Phase 1 actions were completed in 2015.

During Phase 2, which will be completed by 2017, licensees will complete full implementation of their cyber security programs. They will add additional technical cyber controls, cyber security awareness training for employees, incident response testing and drills, configuration management controls, and supply chain protection.

Like other NRC programs, cyber security involves "defense in depth." Crucial safety- or security-related systems (both digital and analog) are isolated from the Internet, giving them strong protection. Such "air gaps" are important, but not sufficient. Licensees must also address wireless threats, portable media such as discs or thumb drives, and other avenues of attack.

Physical security and access controls, including guarding against an insider threat to the plant, also add to cyber security, as do cyber intrusion detection and response capability.

Cyber security has become an intrinsic part of the safety culture both within the NRC and within the nuclear industry. Every employee must be clear that the part they play in cyber defense is both real and important. We emphasize constant training and vigilance, and awareness and warning related to evolving threats.

Let me turn from the technological challenge of cyber security to the physical challenge of protecting Category 1 and Category 2 radioactive material. After the terrorist attacks of 2001, the NRC determined there was a need for heightened focus on ensuring the prevention of intentional unauthorized access to radioactive materials to carry out potential malicious acts. As a result, the NRC imposed certain additional security controls to supplement the existing regulatory requirements.

The additional security requirements were consistent with the International Atomic Energy Agency's (IAEA) Code of Conduct on the Safety and Security of Radioactive Sources thresholds for Category 1 and Category 2 materials. Because the majority of the materials licenses in the United States are regulated by the individual states through the NRC's Agreement State program, those states subsequently issued their own legally-binding requirements compatible with the NRC's.

As the NRC and Agreement States made efforts toward the implementation of these requirements, NRC also began the process of developing a generically applicable security framework in its regulations. A final rule known as "Part 37" was published on March 19, 2013, and implementation of the rule by both the NRC and the Agreement States was completed in March 2016.

The NRC will be submitting a report to the U.S. Congress this month on the results of a comprehensive review we conducted of these regulations. The report, in sum, concludes that the NRC continues to believe that this existing regulatory framework provides an appropriately robust infrastructure to ensure the security of radiological sources commensurate with their risk. However, our

own review did conclude there are a few areas in which revisions to the rule, development or revision of guidance, or enhanced communication with licensees is warranted.

The ongoing review of security threats and security measures are they sufficient, are they current, are they meaningful is important to all nuclear regulators around the world. The threats are not ending and they are not static, and neither can we drop our guard nor believe our efforts have reached their conclusion. At the same time, this ongoing review must also determine if we are being realistic in our measures or have gone too far or done too much inconsistent with the posed risk.

Now, let us look to the future for a moment. We have all heard the potential for future deployment of small modular reactors using non-light water technology. These potential new technologies may bring both benefits to security regimes, and challenges to existing regulations and processes. It's possible such designs of smaller profile may prove to be self protecting or more inherently secure.

As appropriate, the NRC is reviewing the security approaches best suited to advanced reactors, should such technology be realized. The Commission's Policy Statement on the Regulation of Advanced Reactors states that the design of advanced reactors should include considerations for safety and security requirements together in the design process.

But this confluence of safety and security the safety/security interface is not a concept reserved for new reactor designs and new approaches.

At the NRC, managing the safety/security interface is a requirement formally incorporated in our 2009 revisions to nuclear power plant security regulations and related guidance. These revisions established the principle that licensees must anticipate the possible negative consequences that could result from implementing changes to plant configurations, facility conditions, or security.

Clearly stated: Plants must manage both safety and security requirements without one negatively affecting another.

How might those negative consequences occur? Let me give you three examples:

- In one situation, a 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, yet another plant erected scaffolding and staged temporary equipment that inadvertently blocked security lines of sight.

As you can see from these albeit small examples, the importance of the interaction and the interface between safety and security activities cannot be downplayed. Safeguarding our sites requires emphasis on, and the interaction, of both. We must avoid any unintended consequences of security measures on safety and vice versa.

One may also look at the safety security interface paradigm as a way to ensure that the security risks associated with nuclear installations and materials are appropriately balanced against the need the ensure their safety.

Requiring security measures with a "zero risk" approach without consideration for the impact on the safety of the installation those security measures might have is potentially fraught with danger. For instance, constructing impenetrable barriers to protect safety equipment from malevolent attacks might perversely have the effect of preventing operators from accessing the equipment in the event of an emergency. This is obviously not a result any of us would intend or desire. Therefore, we must always be diligent and not myopic in ensuring an appropriate balance in the risks between safety and security.

As many of you know, the NRC hosted the first International Nuclear Regulators' Conference on Nuclear Security in 2012 and our colleagues at Consejo de Seguridad Nuclear in Spain hosted the second in May of this year. These meetings have proven to be highly successful and I am pleased that they will continue. I'd like to note my appreciation for the generosity and leadership shown by the Moroccan Agency of Nuclear and Radiological Safety and Security for agreeing to host the third such conference.

I have no doubt that Dr. Khammar Mrabit, the agency's Director General, and his staff will do an outstanding job planning for the next iteration of this conference. You can expect the NRC's full support and I encourage your participation.

I also want to highlight my appreciation for the work done by IAEA to help bring together the international community to share experiences and best practices on the many topics we're discussing this week.

The NRC is a strong proponent of the work of the Nuclear Security Guidance Committee and we appreciate the efforts to complete the Nuclear Security Series documents. The work is not easy but the results are important to the international community, and they contribute to a strengthening of the nuclear security regime worldwide.

As I said at the start of my remarks today, we share a common goal of safeguarding our nuclear installations and nuclear materials against those who wish us harm. We must continue to maintain our motivation in this area and our high performance even in the absence of realized threats.

Thank you again for allowing me an opportunity to speak.