NRC NEWS

U.S. NUCLEAR REGULATORY COMMISSION

Office of Public Affairs Telephone: 301/415-8200
Washington, D.C. 20555-0001
E-mail: opa.resource@nrc.gov Site: www.nrc.gov
Blog: http://public-blog.nrc-gateway.gov

No. S-12-07

Nuclear Security in the New Threat Environment

Prepared Remarks for
The Honorable Gregory B. Jaczko
Chairman
U.S. Nuclear Regulatory Commission
at
GovSec Conference
Washington, DC
April 4, 2012

Thank you and good morning! I am glad to be here at the Government Security Conference and to have the opportunity to speak with you for the first time. Given the wide range of security professionals in the audience today, I am sure some of you have dealt with the Nuclear Regulatory Commission in one way or another.

For those of you who may not be familiar with the NRC, let me give you a brief introduction on who we are. The agency was formed in 1975, and is primarily responsible for the regulation of nuclear power reactors and nuclear materials. Our sole mission is to protect public health and safety, security, and the environment in matters involving the peaceful uses of nuclear materials.

The breadth of our licensees varies greatly. We regulate 104 nuclear power reactors across the country and recently licensed four more to begin construction. We also regulate 31 research and test reactors across the country, including three in the Washington suburbs. We regulate almost 3,000 nuclear materials licensees across the United States. Another 19,000 nuclear material users are regulated by 37 states under agreements with the agency. These materials licensees vary from very small companies that use portable gauges containing a radioactive source, up to the largest hospitals that use radioactive materials in cancer treatments and diagnostic procedures like heart scans.

Across the United States, approximately 50 large commercial irradiators are also in use, some regulated by the NRC and others by Agreement States. We also regulate more than a dozen facilities, either operating or under construction, that enrich uranium or fabricate nuclear fuel.

The NRC is principally thought of as a safety regulator of nuclear power plants and nuclear materials. But the agency also has an equally critical mandate to ensure the secure use of the nuclear materials it licenses. And while the events of September 11 may not seem that long ago for many of you, they are becoming more distant to many in our agency and with the licensees we regulate. It is important that we continue to remember what happened on September 11, and remain vigilant in ensuring the security of nuclear materials going forward.

Just as the NRC is proactive in regulating safety, it also seeks to be equally proactive in the security arena. But in this arena, the world is a much different place in 2012 than it was when the NRC was formed. We adapted to these changes by acquiring the skills and resources necessary to understand this ever-changing security environment, and to establish requirements that enable our licensees to defend against modern security threats. We also developed a new organization in our agency to deal with all these security challenges.

Since 9/11, the policy changes and increased coordination have contributed significantly to today's enhanced security framework. Those changes would not have been possible without the commitment by the NRC to stay on top of the dynamic threat environment, and to implement the necessary regulatory programs in response. We have made considerable progress towards greater security, but it remains critical that both the NRC and its licensees not become complacent, and that we maintain a proactive approach in the future. With that in mind, I want to discuss a number of important initiatives that reflect our continuing focus on guarding against security threats, and the NRC's commitment to maintain that strong focus in the future.

The attacks on September 11, 2001, prompted extensive changes to our security requirements. While the NRC had numerous security regulations in place, most dating back to the late 1970s, many additions were made to site security at nuclear facilities to deal with the significant change in the threat environment.

The cornerstone of our physical security program for power reactors and some fuel cycle licensees has become our force-on-force exercises. To ensure licensees remain ever diligent, we conduct these exercises every three years at licensee facilities. In these exercises, we employ experts in assault tactics to ultimately oversee the program. They test a licensee security force's actual response to a simulated assault using a select team of trained individuals. Many of these people on the mock assault teams come from law enforcement or military backgrounds, and are very highly trained individuals. It is also adjusted with time as new lessons are learned from prior exercises.

One of the ways we judge the performance of our licensees is to establish what we call a security design basis threat. The design basis threat references and identifies the basic threat that each nuclear power plant has to protect against. That threat is something that has evolved over time to address new intelligence information and other sources of information to ensure that our licensees are well prepared to deal with any assault on its security.

One of the biggest changes in this design basis threat has been in the area of cyber security. In one of the early regulatory orders issued after 9/11, the NRC added a cyber attack as one of the adversary threat types included in our security design basis threat. Malicious cyber

activity has proliferated in the past decade, making it a clear and credible threat. And it has caused a significant shift for an agency traditionally focused on physical security, and on the safety of reactors and other facilities built in a far less automated age. It has become clear how safety and security are intertwined when we look at issues involving the reliability and vulnerability of the offsite electrical grid, as well as digital safety systems, to a cyber attack.

Three years ago, the Commission issued a final rule for the protection of digital computer and communication systems and networks. This new rule requires nuclear power plants to provide high assurance that digital equipment associated with safety, security, and emergency preparedness functions is protected against cyber attacks. To do so, our licensees prepared plans showing how they identified critical digital assets and describing their protective strategy now and going forward. These were bold, proactive moves made by the agency to address the possibility of a new threat to our licensees. At this point, I believe we are in a good position to deal with the cyber threat faced today.

Our licensees have submitted, and we have approved, plans for how they are dealing with cyber security threats, and the NRC will begin inspections in this critical area next year. Since all of our current operating reactor licensees were designed in the 1960s and 1970s, employing the control technology of that time, most of their technology is not digitally-based. The cyber threat at these facilities is very different from new nuclear reactors, which use digital technology extensively. While many of these licensees have replaced some control technology in systems not critical to the safe shutdown of the nuclear reactor, we must ensure our licensees do not become complacent and assume their facilities have little vulnerability to an attack based on their limited use of digital technology. These same operating reactors have long since installed modern communication and security systems, which are critical to plant safety and security. For new reactors pursuing a license or currently beginning construction, protections against cyber attacks were included in the design and in our license review process.

But as we also know, nuclear reactors are not the only facilities of concern for a cyber attack. Several years ago, cyber weapons against critical infrastructure were considered a future threat, and were estimated to be perhaps a decade away. Then in 2010, the Stuxnet computer malware was discovered. In the case of a cyber weapon such as Stuxnet, this event serves as a proof of concept – or a template – for future attacks. And we have already seen some proliferation of Stuxnet-like programs since that time. In the future, security threats may not involve just a direct attack using guns and vehicle bombs, but also indirect attacks involving malicious computer programs.

Since the threat timeline is moving faster all the time, we have to ensure that we never become complacent – we must always be forward-looking. Currently the NRC has a cyber assessment team staffed by experts in cyber security, digital instrumentation and control, and other disciplines. They promptly address and evaluate cyber security issues that could impact licensee digital computer and communication systems and networks, and promptly provide recommendations to NRC management. In accordance with the National Cyber Security Incident Response Plan, this team regularly coordinates and communicates with other federal computer emergency response teams.

Finally, as in any regulatory agency, implementing regulatory changes takes time. We must continue to look for new ways to develop agency requirements more promptly when necessary. In the cyber security area, the threat is constantly changing, so we can never become complacent.

The NRC must also protect our own valuable computer programs, which contain a wealth of information, but are often under attack from malware and other external probes. The agency has comprehensive security controls in place in accordance with the Federal Information Security Management Act, and periodically trains all its employees on computer security and cyber threats. But all it takes is one employee to inadvertently click on an email, releasing some malicious code into our computer system that could circumvent our engineered security controls. Therefore, like our licensees, we must be diligent in protecting our digital assets.

The security of radioactive sources is also a significant concern. Our requirements in this area come in two forms – physical protections, and material control and accounting. Just last month, the Commission approved a final rule on the security requirements for licensees possessing the most risk-significant sources of radioactive material, although most of these security requirements have been in place for years under orders issued by the agency after 9/11.

As these sources are scattered around thousands of locations across the United States, they can be quite challenging to regulate from a security standpoint. They also are managed by licensees of widely varying capabilities and complexities, from large corporations and hospitals to small, family-run businesses. In general, we are concerned that there could be some way for an adversary to accumulate a significant amount of radioactive material from multiple licensees, then create and set off a radiological dispersal device.

The immediate health effects from setting off such a device would be limited to those individuals near the blast. In general, we don't expect that such a device would pose an immediate health impact to individuals from the resulting radiological exposure. However, the resulting radioactive contamination might force the evacuation of the immediate area, as well as areas downwind, and require a long, expensive cleanup effort to make the area safe again. Our security regulations, as well as our safety regulations, are focused on limiting the potential impact of the radiological exposure to the public following either a nuclear accident or a security event, but not the cost of such a cleanup effort.

To enhance nuclear materials source security, the NRC launched a National Source Tracking System several years ago. This inventory control program is a secure, national registry that tracks radioactive sources licensed by the NRC and the States from the time they are manufactured or imported through the time of their disposal, decay, or export. These sources are also categorized by their relative risk significance, with higher levels of physical security required for more risk-significant sources. By accounting for the tens of thousands of risk-significant sources, this tracking system enhances our ability to detect and act upon inventory anomalies, respond to emergencies, and verify the legitimate use and transfer of sources. More often, the agency has used this tracking system to help us locate, and later ensure the safety of, sources in the pathways of natural events, such as the recent tornados in Texas or hurricanes along the Gulf states and the East Coast.

Complimenting this tracking system, the agency also has in place verification measures to ensure nuclear materials and sources are initially provided only to trustworthy individuals. These measures are intended to ensure these materials are not used for malevolent purposes. The agency also has well underway a web-based licensing system for nuclear materials licensees that will provide a comprehensive, secure source of information on each licensee in the country to the NRC and our 37 Agreement States. In the aggregate, all of these measures serve to significantly strengthen the security of the nuclear material we license.

The 10 years since the events of 9/11 have been a period of relative calm regarding domestic terrorism. But, this calm must not allow complacency to set in going forward. Rather, we need to constantly keep analyzing the security threat environment and react promptly. I can assure you that at the NRC, our dedicated staff will remain vigilant about the security threats facing our licensees and will promptly react.

While we are doing many good things in the security area, we cannot do them successfully without the tremendous support we receive from many of you. The NRC is not an intelligence agency, and the timely sharing of accurate information by other federal agencies is critical to helping us plan for, prevent, or mitigate a potential terrorist attack. NRC security analysts work with intelligence and law enforcement agencies, to strengthen communication and support the integrated assessment of security-related information.

The NRC also coordinates with many other federal organizations to make sure its licensees have up-to-date information and adequate security protections in place. This is critical - all levels of federal, state and local government must work together effectively if the security measures we require of our licensees are to be successful when—and if—they are challenged.

This information would also be of no benefit if it were not shared with our licensees promptly and effectively. The NRC is constantly assessing threat information and disseminating information to our licensees promptly through formal threat advisories or secure calls with individual licensees. Assessing and providing developing security information is a 24/7 activity for the NRC, but it ensures our licensees are given advanced warning of developing security threats and can remain alert and ready.

In conclusion, the security threats facing our nation and our licensees have greatly changed over time. The NRC's security regulations have done the same. The challenge going forward is to avoid becoming complacent as the events of 9/11 recede in time. We must continue to implement changes proactively in an environment where the security threat is changing more rapidly, particularly in the area of cyber security. At the NRC, our employees will continue working hard to track changes in the threat situation, propose ways to strengthen our regulations to meet new security challenges, and ensure our licensees implement those changes in a timely and effective manner. I am very proud of the dedication and professionalism of our staff, and equally proud that the NRC has continued to rank as one of the Best Places to Work in the Federal Government.

As we look to the future, we need your help in assessing security threats and adjusting to new realities. We greatly appreciate all of the advice and support provided to us by the intelligence community and other elements of the federal family. We look forward to working with you in the future to ensure the continued safety and security of nuclear materials in this country.

###