Ensuring Nuclear Security in a Dynamic Threat Environment
by Michael Weber
(Summarized by James Lemley)

The second Closing Plenary speaker was Michael Weber who is deputy director of the new Office of Nuclear Security and Incident Response (NSIR) in the U.S. Nuclear Regulatory Commission (NRC). NSIR was created in April 2002 by consolidating security elements from throughout the agency. In this capacity Mr. Weber helps manage the development of policy and oversees safeguards, security, threat assessment, and incident response associated with civilian use of nuclear materials in the U.S. Immediately prior to his current position, Mr. Weber was the director, Division of Fuel Cycle Safety and Safeguards in NRC's Office of Nuclear Material Safety and Safeguards (NMSS). He is a geosciences graduate of the Pennsylvania State University and a graduate of the Office of Personnel Management's Interagency Executive Potential Program. The title of Mr. Weber's talk was "Ensuring Nuclear Security in a Dynamic Threat Environment."

Introduction to NSIR
In response to the terrorist attacks of September 11, the NRC recognized that greater effectiveness and efficiency could be achieved by combining safeguards and security with incident response. The responsibilities of the new Office of Nuclear Safety and Incident Response (NSIR) include oversight of material control and accountability, international safeguards, physical protection, threat assessment, information security, and incident response. The offices of Nuclear Material Safety and Safeguards (NMSS) and Nuclear Reactor Regulation (NRR) retain responsibilities for licensing. NSIR partners with these offices and the regions to ensure sufficient oversight of security, safeguards, and incident response activities. NSIR is working hard to enhance communications internally and with the regional offices as well as externally with Congress, the Office of Homeland Security, other federal agencies, States, licensees, and other stakeholders.

New Threat Environment
NRC has been keenly coordinating with the intelligence community and law enforcement agencies since well before the terrorist attacks last September. In the late 1970s, NRC established its Design Basis Threats (DBT) for radiological sabotage and for theft and diversion. About every six months the staff completes a systematic review of significant terrorist, criminal, and civil unrest incidents. The purpose of these reviews is to assess the overall threat environment, as well as to identify any necessary changes to the DBTs and highlight for the Commission any emerging trends in targets, tactics, weapons, or other threat attributes.

Mr. Weber noted that, despite all the rhetoric in the press, there have been no specific credible threats against nuclear facilities or activities since September 11.There have been suspicious incidents but no operational planning or attacks.

In 1994, for example, following the first bombing of the World Trade Center (WTC), NRC added vehicle bombs to the DBT for radiological sabotage. Critics of NRC pointed

out that this decision was obvious but belated since vehicle bombings had occurred overseas much earlier. The U.S. is often accused of fighting the "last war." Mr. Weber observed that staying ahead of terrorists, criminals, disgruntled citizens, and extremists is consuming the professional attention of many INMM members and a growing portion of our intelligence and law enforcement agencies. The threat environment is very uncertain, and this complicates planning.

While America has other enemies, al Qaeda continues to present a clear and present danger. NRC has been working closely with the intelligence community and law enforcement agencies in assessing al Qaeda - its tactics, training, targets, and capabilities. Assessments of al Qaeda and other enemies provide insight into what may be next. Open sources have widely reported al Qaeda interest in nuclear targets. Noting the great irony, Mr. Weber claimed that apprehension by the public and the media about nuclear and radiological terrorism may have the unanticipated effect of reinforcing terrorist interest in nuclear targets. He pointed out that radiological dispersal devices, for example as reported in connection with the detainment of Jose Padilla (Abdullah al-Mujahir), would not achieve the terrorist objective of widespread devastation and casualties but could be successful in disrupting society, causing public concern, and imposing economic impacts.

In a comprehensive security and safeguards review launched by Chairman Meserve, NRC is scrutinizing these insights and deliberating on the best approaches for revisions to the DBTs. Revisions to the DBTs and the changing threat environment provide new impetus for consideration of changes to existing security and safeguards programs.

Security Measures

Immediately after the attacks, NRC issued a series of threat advisories to certain licensees advising them to upgrade security measures because of the great uncertainty that existed in mid-September. In developing these advisories, NRC staff also examined what other vulnerabilities could exist at licensed nuclear facilities, particularly if adversaries used weapons and tactics that went beyond those postulated in the DBTs. After all, NRC's DBTs did not anticipate the use of civilian airliners as missiles. From first-order vulnerability analyses, NRC formulated a string of measures that could be readily implemented to enhance security, if they were feasible and compatible with safety, and communicated them to licensees in early October 2001. Although the exact measures are protected safeguards information, they included actions such as increasing standoff distances to access portals, restricting access, and revising emergency procedures in response to terrorist attacks. NRC audited licensee consideration and implementation of these measures during the remainder of calendar 2001.

Shortly thereafter, NRC identified additional interim compensatory measures (ICM) that could further enhance security at a wide range of nuclear facilities and imposed enforceable requirements at some facilities, such as power reactors, decommissioned reactors, and the gaseous diffusion plants. Enhancements included increased patrols, augmented security-force capabilities, additional physical barriers, vehicle access checks at greater standoff distances, more restrictive site access controls, and enhanced coordination with local law enforcement agencies.

Additional ICMs being considered are tailored to each class of licensee and to entities that use, transport, and store significant quantities of radioactive materials. With ICMs in place, NRC is proceeding with a more deliberate and comprehensive review, including revisions to the DBTs and threat characteristics, vulnerability analyses, and regulatory improvements. The continuing vulnerability assessments will provide a more systematic and risk-informed basis for identifying and justifying regulatory improvements to the safeguards and security program over the next several months to years.

Challenges Ahead
In planning a way forward, Mr. Weber identified a series of fundamental issues that would affect security decisions by NRC and nuclear security and homeland security more broadly.

Risk avoidance vs. risk mitigation: As an independent public-service agency NRC serves the public by responding to their elected representatives in Congress. Does the public want to eliminate security risks altogether or, alternatively, to reduce them sufficiently that they do not warrant additional attention, cause undue alarm, or infringe on our civil liberties? Mr. Weber reported that NRC generally perceives public will to be the latter, as framed under the Atomic Energy Act, which specifies "adequate protection" not "absolute," and as displayed more recently in the resumption of normal business following September 11.

Federal, state and local roles: Licensee reliance on federal, state and local agencies to supplement and augment licensee security forces was never more evident than in the days and weeks following September 11. If public-sector agencies are to have ongoing roles in post-9/11 security, the operationally effective allocation and coordination of responsibilities among federal, state, and local agencies will be a significant challenge.

Distinguishing public and private responsibilities: The NRC has required licensees to provide the security forces necessary to ensure sufficient protection of the public, and in most cases this meant extensive reliance on the private sector. NRC-licensed power reactors are among the most protected of private sector facilities in the U.S. However, NRC's existing regulatory framework makes it clear that licensees cannot be held accountable for designing nuclear facilities to protect against enemies of the United States (10 CFR 50.13). So where is the threshold for public-sector responsibility? Is such a threshold pragmatic or would it be more constructive to look at security as a seamless continuum ranging from private sector for handling the smallest incidents up to U.S. military defense for threats from foreign nations? Even under shared public and private responsibility a number of practical questions will have to be addressed. How long should private-sector guards be held responsible for defending the facilities until offsite public help arrives? Are plans for offsite assistance well designed and adequately exercised? What are the obligations of private-sector guards once the "cavalry" arrives from offsite?

The nuclear industry compared to other infrastructure assets: Mr. Weber raised a fundamental question of whether the nuclear industry is sufficiently different that it

warrants special consideration in examining the adequacy of homeland security or whether nuclear security should be subsumed in broader efforts to protect the infrastructure in general. More specifically, are the potential threats, consequences, vulnerabilities, and risks so different from other parts of the infrastructure that nuclear warrants separate and distinct consideration? Will the public ultimately support homeland security initiatives intended to provide a coherent and harmonized approach, despite perceptions that nuclear facilities pose higher risks and consequences? What should be the measures for evaluating the risks associated with sabotage or with theft or diversion and how would they apply across the infrastructure? If different criteria and metrics are used, how can decision makers best evaluate the relative risks associated with nuclear facilities and materials, versus other components of the critical infrastructure?

Openness vs. information security: If the public continues to expect the NRC to conduct business in an open, forthcoming, and meaningful process, how can NRC most effectively balance this expectation with the need to enhance security through restricting access to information? Is there a legitimate role for public stakeholders to engage NRC staff in discussion of security measures? How can these stake holders be engaged effectively in the peer review process? If NRC continues to conduct its business in an open environment, how can NRC ensure that sensitive information released to the public does not find its way to terrorists, criminals, or other adversaries who might exploit it nefariously?

Conclusions

NRC has continued to ensure security in an uncertain threat environment through advisories and interim security measures. NRC licensees remain at a high security level and are on the lookout for suspicious or threatening activities. Although there have been no specific, credible threats against licensed activities or facilities, private security forces remain vigilant against sabotage or theft. NRC continues a high level of engagement with the Office of Homeland Security, other federal and state agencies, and other entities involved in antiterrorism activities. These measures afford NRC the time to proceed thoughtfully and deliberately with revisions to NRC's DBTs and threat characteristics. Further enhancements in security are being planned from ongoing threat revisions, vulnerability analyses, and regulatory improvements. To make progress in ensuring security in an uncertain threat environment, NRC will have to resolve vexing issues and provide scrutability and predictability in its regulatory decisions, while preserving flexibility and efficiency to accommodate future changes.