

Integrated Regulatory Review Service Mission to the United States

MODULE 12: INTERFACES WITH NUCLEAR SECURITY

Overview

The responsibilities and function of the government to license and regulate the U.S. civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, promote the common defense and security, and protect the environment rest with a single agency, the U.S. Nuclear Regulatory Commission (NRC). Both safety and security share the common purpose of protecting public health and safety. In today's environment, with a greater emphasis on security-related matters, safety and security activities have become closely intertwined, and it is critical that consideration of these activities be integrated so as not to diminish or adversely impact either safety or security. While many safety and security activities complement each other, there is the potential for security measures to adversely affect plant safety, and for safety activities to adversely affect security. Recognizing this potential, the NRC has increased its attention to the interfaces between these two areas. The NRC has taken measurable steps in key areas to improve the interfaces with nuclear security, including the following:

1. developing specific regulations and guidance documents in its regulatory program
2. revising the reactor oversight framework
3. coordinating internal agency processes
4. improving liaison with local, State, and Federal law enforcement agencies
5. incorporating security-initiated activities in emergency preparedness (EP) exercises
6. revising the NRC's safety culture policy statement to include security

The following sections discuss each of these key areas.

Regulatory Program

The government shall ensure that within the governmental and legal framework adequate infrastructural arrangements are established for interfaces of safety with arrangements for nuclear security and with the State system of accounting for and control of nuclear material. (GS-R-1, Requirement 12)

The amendments to the existing security regulations in Title 10 of the *Code of Federal Regulations* (10 CFR) Part 73, "Physical Protection of Plants and Materials" (final rule issued in March 2009, with an implementation date of March 2010), added new security requirements pertaining to both current and future nuclear power plants. One of the key new features of this regulation is a regulatory requirement for a safety/security interface (10 CFR 73.58, "Safety/Security Interface Requirements for Nuclear Power Reactors"). This regulation requires licensees to (1) assess and manage the potential for adverse effects on safety and security, including the site emergency plan, before implementing changes to the plant configurations, facility conditions, or security, and (2) communicate any potential adverse interactions to appropriate licensee personnel and take compensatory and/or mitigative actions to maintain safety and security under applicable NRC regulations, requirements, and license conditions. The scope of changes to be assessed and managed by the licensee must include planned and emergent activities, such as, but not limited to, physical modifications, procedural changes,

changes to operator actions or security assignments, maintenance activities, system reconfiguration, access modification or restrictions, and changes to the security plan and its implementation.

Another new regulatory requirement appears in 10 CFR 73.55(c)(7), “Security Implementing Procedures,” of 10 CFR 73.55, “Requirements for the Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage.” This requires licensees to review and update existing procedures to reference the requirements of the interface between safety and security as outlined in 10 CFR 73.58. These facility procedures should clearly define processes to ensure that the facility perpetuates a comprehensive and effective network of communications between its operations (safety) and security staffs. Also, 10 CFR 73.55(m), “Security Program Reviews,” requires licensees to ensure that the reviews and audits of its site physical protection program include activities involving the interface between safety and security.

In December 2005, the NRC issued Information Notice¹ 2005-33, “Managing the Safety/Security Interface” (Official Use Only—Security-Related Information (OUO-SRI)), to remind licensees of the need to prevent adverse interactions between safety and security activities. The NRC staff had become aware of several cases in which actions taken by licensee operations, maintenance, or security personnel were not promptly and effectively communicated to other potentially affected licensee organizations and had the potential to result in adverse effects on plant safety or security. Information Notice 2005-33 made licensees aware of these situations and advised them to review the information for applicability to their facilities and consider actions, as appropriate, to prevent similar interactions.

As part of the reactor security rulemaking effort, the NRC developed guidance on safety/security interfaces at nuclear power plants in Regulatory Guide 5.74, “Managing the Safety/Security Interface.” The guidance states that a licensee’s management controls and processes for the interface between safety and security should ensure that the site’s security organization is notified of potential changes to (1) the characteristics of the site’s physical layout, (2) the configuration of facilities, (3) structures, systems, and components, (4) the site’s operational procedures, and (5) day-to-day or planned activities. Licensees already had controls and processes to evaluate safety issues, but interfaces with nuclear security were not always included. Integrating security into the licensee’s controls and processes for evaluating safety issues provides the security organization with the opportunity to review proposed changes and activities to identify potential adverse impacts on the functions and performance of the elements of its site physical protection program. The controls and processes also ensure that operations and emergency planning organizations are aware of proposed changes to the plant’s security program.²

¹ Generic communications include administrative letters, bulletins, circulars, information notices, regulatory information summaries, and security advisories. These provide significant recently identified information about safety, security, or environmental issues to licensees. See <http://www.nrc.gov/reading-rm/doc-collections/gen-comm/>.

² A facility’s security program consists of those measures (such as access authorization, physical barriers, and training and qualification of the security organization) in place for the protection of nuclear material or facilities against sabotage, theft, and diversion; protection of sensitive information; and accountability of nuclear materials.

Oversight

The NRC oversight program consists of its Reactor Oversight Process (ROP) and inspection activities to (1) maintain safety, (2) increase openness, (3) make NRC activities and decisions more effective, efficient, and realistic, and (4) reduce unnecessary regulatory burden. Module VII (Inspection) discusses the ROP and inspection activities. The following discussion focuses on the security-related portion of the ROP and interfaces with nuclear security. In 2000, the NRC revised the ROP, to establish a risk-informed baseline inspection program and to set documented risk-informed thresholds for licensee safety and security performance, above which increased NRC oversight would be warranted. (See Staff Requirements Memorandum on SECY-99-007, "Recommendations for Reactor Oversight Process Improvements"; SECY-99-007A, "Recommendations for Reactor Oversight Process Improvements (Followup to SECY-99-007)," and SECY-00-049, "Results of the Revised Reactor Oversight Process Pilot Program.") This initiative affirmed the NRC's commitment to better integrate security into the oversight process by enhancing safety/security interface as part of the NRC's approach to assessing licensee performance.

The regulatory framework for reactor oversight consists of three key strategic performance areas: reactor safety, radiation safety, and safeguards.³ The strategic performance areas are composed of cornerstones (initiating events, mitigating systems, barrier integrity, emergency preparedness, public radiation safety, occupational radiation safety, and security). Satisfactory licensee performance in the cornerstones provides reasonable assurance of safe and secure facility operation and the accomplishment of the NRC's safety and security missions. Like the other cornerstones, the security cornerstone contains inspection procedures and performance indicators to ensure that its objectives are being met. The NRC addresses safety/security interface issues in evaluating their implications among the cornerstones and in the crosscutting areas⁴ of human performance, safety-conscious work environment, and problem identification and resolution. Therefore, safety and security are integrated into the NRC's regulatory framework and evaluated by the agency using a common process.

With the increased attention to security following the events of September 11, 2001, the NRC recognized that the assurance of both plant security and safety requires coordination of activities. As discussed above under "Regulatory Programs," the NRC has issued regulations that require licensees to ensure that this coordination occurs. To ensure that licensees are complying with the regulations, the NRC has incorporated the evaluation of the licensee's interfaces with nuclear security into its inspection procedures. For example, to gather information about the overall security and safety activities at a nuclear power plant, resident inspectors conduct inspections on a routine basis, and regional or Headquarters inspectors perform periodic security inspections. Inspectors walk down the facility to stay current of facility status, as well as to identify unexpected safety or security conditions that may warrant additional inspection. Resident inspectors attend licensee meetings (e.g., plan of the day, shift turnover, emergent work, and corrective actions meetings) to gather information on a variety of safety and

³ The objective of the safeguards strategic performance area is to provide assurance that the licensee's security system and material control and accounting program use a defense-in-depth approach and can protect against (1) the design-basis threat of radiological sabotage from external and internal threats and (2) the theft or loss of radiological materials.

⁴ Certain aspects of licensee performance are "crosscutting" (i.e., they potentially impact more than one cornerstone). These issues generally manifest themselves as the root causes of performance problems. Adequate licensee performance in the crosscutting areas is assessed either explicitly in each cornerstone area or is inferred through cornerstone performance results from both performance indicators and inspection results.

security activities. These inspections are intended to, in part, identify safety/security interface issues, among other safety issues, that require resolution or further consideration. Inspectors are encouraged to consider and, as appropriate, question licensee staff regarding possible safety/security interface issues. Inspection Procedures 71130.04, "Equipment Performance, Testing, and Maintenance," and 71130.05, "Protective Strategy Evaluation," specifically address safety/security interface issues. The NRC will continue to leverage the elements of the ROP assessment and annual review of inspection results to ascertain how well its inspection program is evaluating licensee implementation of the new rule.

Internal Coordination

Although licensees are responsible for meeting all applicable regulations, the NRC is aware of the potential for the agency's internal activities in the security arena (e.g., licensing actions, operational or significance determination process insights, rulemaking, issuance of orders, and generic communications) to adversely impact safety, and vice versa. The NRC has several internal processes that promote interfaces with nuclear security inside the agency, as well as external processes to reach its regulated communities. These processes enhance the effectiveness of the NRC regulatory program.

The NRC has acted to ensure that its activities in one arena (safety or security) do not adversely affect the other arena. In 2004, the NRC formed a safety/security advisory panel and working group to improve the agency's integration of security requirements into the licensing process. The membership of this panel and working group included persons familiar with operations, security, and EP. Meetings were held to discuss safety issues that were identified during the review of proposed security actions taken in response to the events of September 11, 2001. As the number of NRC actions in the security arena (e.g., rulemaking, issuance of security orders) decreased, the NRC determined that it no longer needed the standing advisory panel and working group. The NRC determined that management of the safety/security interface should be incorporated into ongoing processes rather than be addressed through the committee approach.

In 2006, the NRC issued an office instruction, COM-111, "Managing the Interfaces between Safety, Security, and Emergency Preparedness," to provide staff and management in the Office of Nuclear Reactor Regulation (NRR) with guidance on, and to increase the awareness of, the need to integrate safety, security, and EP considerations into NRC activities. This instruction superseded the safety/security advisory panel and working group and required the NRR staff to be aware of the basic need to consider the relationships between programs related to plant safety, security, and EP as part of the routine decisionmaking process. The instruction provided guidance on how to resolve safety/security interface issues among NRC divisions in both NRR and the Office of Nuclear Security and Incident Response (NSIR). It also directed that an interoffice review board be convened annually to assess the NRC's management of the safety/security/EP interface. The NRC is preparing a revision to COM-111 as a joint office instruction that will apply to NRR, NSIR, and the Office of New Reactors (NRO). The revision will incorporate organizational changes within the NRC, identify points of contact within each office, and provide enhanced guidance on the handling of potential safety/security interface issues.

The NRC also took steps to promote consistent application and resolution of inspection findings. In 2003, the NRC established a panel, now called the Security Issues Forum (SIF), to ensure the consistent application and resolution of inspection findings related to compensatory measures implemented by licensees in response to NRC security orders issued after

September 11, 2001. The scope of items reviewed by this panel was later expanded to include all security-related inspection findings (i.e., not only those related to compensatory measures) to ensure full regulatory consistency for all security-related inspection findings.

The current SIF charter is to provide an environment for the discussion of security findings and other issues of common interest upon request of the membership, which consists of representatives from NSIR, NRR, Office of Enforcement, Office of the General Counsel, the Office of Nuclear Material Safety and Safeguards, Office of Federal and State Materials and Environmental Management Programs, and the regions. This broad representation across NRC offices ensures that safety, security, and EP inspection issues are identified, discussed, and resolved. In addition, outcomes of the SIF may identify generic issues that need to be addressed, as well as where changes may be needed for inspection procedures and regulatory guides.

Because the security requirements for licensees have recently changed, the potential exists for new security issues and inspection findings to arise that were not considered when the requirements were initially developed. The NRC has two complementary processes that promote consistent interpretation of the guidance relating to security regulations. The first process, the NSIR "Report on Interaction" (ROI) process, provides an avenue for regional inspectors to raise questions regarding the intent of NRC guidance on compliance with the security regulations. The ROI process documents staff positions on implementing 10 CFR Part 73. Issues reviewed through the ROI process may include those resulting in a security inspection finding (i.e., from the SIF) or issues identified in guidance documents, inspection procedures, or regulations requiring additional clarification on their intent. The second process, the "Security Frequently Asked Questions" (SFAQ) process, provides licensees with an organized forum to request NRC resolution of generic questions concerning the implementation of security requirements. The SFAQ process is intended to support the resolution of licensees' questions promptly and effectively and support the NRC's exercise of its regulatory responsibility as efficiently and directly as possible. The resolution of issues using the ROI and SFAQ processes may be incorporated into the next revision of the appropriate guidance document (e.g., a regulatory guide or the Standard Review Plan), if warranted, which helps ensure continued NRC staff awareness of the potential for safety/security interface issues. These two processes offer an additional benefit: in answering the questions from the regional inspectors or licensees, NSIR staff has the opportunity to identify potential safety/security interface issues and raise them to the responsible organizations.

The NRC emphasis on consensus through our internal processes results in the identification and resolution of potential safety/security interface issues. Experience has shown that it is rare for an issue to rise to the level of the COM-111 Interoffice Review Board for resolution because issues have been identified and resolved satisfactorily at the appropriate level through the responsible organizations. For example, NRC used internal processes to identify and resolve potential safety/security interface issues associated with digital instrumentation and control system upgrades at nuclear power plants. Licensees planned to replace outdated analog systems with more advanced digital systems that control reactor safety functions. The staff raised concerns over potential impacts on safety while ensuring and maintaining adequate cyber security. Staff members from both NRR and NSIR interacted many times to discuss and understand the possible safety and security impacts that these upgrades could have on the operation, function, and reliability of affected safety systems and the impact that an added cyber security measure could have on the operation, function, and reliability of these safety systems. The staff reached a mutually acceptable solution to ensure that cyber security measures were adequate without interfering with or hampering the performance of the required safety function.

Liaison with Local, State, and Federal Law Enforcement Agencies

NRC regulation 10 CFR 73.55(k)(9) requires that licensees, to the extent practicable, document and maintain current agreements with applicable law enforcement agencies. These agreements typically include the time it will take for law enforcement agency personnel to arrive at the site, the total number of personnel available to respond on average, communication methods, command-and-control structure, and the actions that these personnel are equipped and trained to perform. In addition, 10 CFR Part 73, Appendix C, "Nuclear Power Plant Safeguards Contingency Plans," Section II.B.3.d, "Law Enforcement Assistance," requires licensees to provide a list of available law enforcement agencies, such as local police, State police, and the Federal Bureau of Investigation, as well as a general description of the actions that each would be expected to take, the types of actions for which each is equipped and trained, a description of the conditions or events that would be met before requesting such assistance, and the predetermined site location where these responding agencies are expected to arrive and assemble. The agreements include a general discussion of working arrangements for communication between site personnel and individuals from these law enforcement agencies, communication among these agencies, and communication between law enforcement responders and other support personnel from EP organizations, fire departments, and medical facilities. The intent of this arrangement is to ensure that assistance from offsite law enforcement agencies is coordinated to the extent possible with response efforts by other agencies. These arrangements also ensure that response organizations have a clear, comprehensive, and predetermined structure and that all required actions are conducted safely, effectively, and without conflict with other responders.

Because it is not possible in advance to account for every possible scenario where offsite support may be needed, licensees preplan communication protocols to ensure that the specific details of a given event are communicated to appropriate offsite personnel who may respond. These individuals can then take appropriate actions (deployment of personnel and/or equipment) to respond effectively to the event as it happens. The licensees are required to periodically review and verify the continued capability of offsite law enforcement agencies to provide the expected response support. For example, the licensee should account for the impact that changes within the support agency's organization will have on previously discussed capabilities. These changes might include funding restrictions, the purchase of updated equipment, the discontinued use of outdated equipment, and changes in staffing levels.

Emergency Preparedness

Module 10, "Emergency Preparedness and Response," discusses EP. Offsite radiological releases from a nuclear power plant requiring emergency response actions can result from safety-initiated events (e.g., failure of structures, systems, and components) or from malicious acts (e.g., terrorist attacks that damage safety components). The following discussion focuses on security-initiated exercises termed "hostile-action-based" (HAB) drills.

After September 11, 2001, the NRC reviewed and analyzed the adequacy of its EP program and determined that the EP program was still adequate, even for an event such as an aircraft impact at a nuclear power plant. However, the NRC recognized that within the area of emergency planning and preparedness, conventional responses to an incident with a terrorist component (e.g., land, air, or waterborne attack) at a facility could be enhanced. The NRC issued Bulletin 2005-02, "Emergency Preparedness and Response Actions for Security-Based Events," dated July 18, 2005, to obtain information regarding changes licensees had made or

planned to make in their security-based EP program capabilities and to use this information to evaluate the consistency with which such changes have been implemented. The NRC used the information obtained to inform subsequent actions such as working with industry on a pilot program to conduct HAB EP drills and developing a proposed rule to require licensees to periodically conduct HAB exercises. These subsequent actions are discussed below.

Regulatory Issue Summary 2006-12, "Endorsement of Nuclear Energy Institute Guidance, 'Enhancements to Emergency Preparedness Programs for Hostile Action,'" dated July 19, 2006, endorsed a Nuclear Energy Institute (NEI) white paper that proposed a phased pilot approach to incorporate an HAB scenario during a year when the licensee does not have to demonstrate a biennial EP exercise in accordance with Appendix E, "Emergency Planning and Preparedness for Production and Utilization Facilities," to 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities." Beginning in March 2006, each licensee was to conduct an HAB drill within a 3-year period as a voluntary pilot.

As part of the pilot, the industry developed guidance for licensees to use during the voluntary pilot initiative. The NRC endorsed the industry guidance, with clarifications, in Regulatory Issue Summary 2008-08, "Endorsement of Nuclear Energy Institute Guidance Document NEI 06-04, 'Conducting a Hostile Action-Based Emergency Response Drill,'" dated March 19, 2008. Postulated HAB scenarios are initiated by hostile or terrorist actions that lead to simulated plant damage, which is a primary difference from traditional safety-initiated scenarios. These HAB scenarios require a coordinated onsite and offsite response to mitigate the event, while simultaneously addressing the security situation. HAB EP drills did not include site security or law enforcement tactical movements, but rather simulated these actions to facilitate the scenario. NEI 06-04, Revision 1, "Conducting a Hostile Action-Based Emergency Response Drill," dated October 30, 2007, provides guidance on conducting a predrill tabletop exercise. Conducting tabletop exercises is good practice for key licensee emergency response organization personnel and offsite response organizations, as it gives them opportunities to review and discuss their respective roles, priorities, and response actions during an HAB event. In particular, the tabletop exercises permit diverse organizations to gain an understanding of the others' immediate priorities and concerns during a hostile action event. NEI 06-04 provides guidance to facilitate a functional demonstration of the ability of the emergency response organization to coordinate in-plant and onsite response actions with security and offsite response organizations through the offsite incident command structure.

The NRC issued Information Notice 2009-19, "Hostile Action-Based Emergency Preparedness Drills," dated November 29, 2009, which summarizes the NRC staff's observations of pilot HAB EP drills at power reactor licensees beginning in March 2006. NRC observations were made in coordination with NEI and the Federal Emergency Management Agency, but were not part of any formal regulatory evaluation or inspection process. The NRC's review of these pilot initiative drills revealed that communications were routinely a challenge to the conduct of HAB drills. For most licensees, the need for the plant personnel to communicate and coordinate with the offsite incident command structure, whether through its own liaisons or otherwise, was a new concept. The HAB drill pilot promoted positive safety/security interfaces and enhanced communication internally at a facility, between the facility and offsite response organizations, and among offsite response organizations. This pilot study was completed at the end of calendar year 2009. The NRC is considering whether to incorporate HAB EP scenarios as an evaluated exercise under the proposed EP rule. The proposed rule was published for public comment in the *Federal Register* on May 18, 2009 (74 FR 23254), and the staff anticipates that the final rule will be published early in calendar year 2011.

Safety Culture Policy

Another example of an area where the NRC is promoting strong linkages between safety and security is in the area of organizational culture. In 1989, the NRC issued a policy statement on the conduct of operations that included safety culture considerations for nuclear power plants. In 2008, the NRC began to expand its policy on safety culture to address the unique aspects of security and to make it applicable to all licensees and certificate holders. This effort is ongoing and has included interactions and a public meeting with a wide range of stakeholders, including nuclear power plant licensees.

Most participants in the public meeting supported a joint policy statement that addressed both safety culture and security culture, rather than separate policy statements. Stakeholders generally believed that the policy statement should recognize that security culture is one of several integrated parts of a licensee's overall safety culture. In other words, there is no real distinction between cultures (e.g., there is not a stand-alone radiation safety culture, a nuclear criticality safety culture, a fire safety culture, or an environmental protection culture). Each of these programs focuses on safety for a particular discipline; the licensee safety culture integrates all of these disciplines.

The staff submitted the resulting safety culture policy statement to the Commission in May 2009. In October 2009, the Commission directed that the staff publish the policy statement in the *Federal Register* for a 90-day comment period, to continue to engage a broad range of stakeholders and to seek opportunities to harmonize terminology with existing standards and references. The NRC expects to issue a revised safety culture policy statement in 2011. This revision to the safety culture policy statement will provide another mechanism to strengthen and reinforce the safety/security interface.

Assessment Summary

Self-Assessment Results

No specific Complementary Self-Assessment questions are related to interfaces with nuclear security. However, the staff has conducted an assessment of the NRC's current programs relative to IAEA draft GSR-1, "Governmental, Legal and Regulatory Framework for Safety," Requirement 12, which addresses interfaces with nuclear security. Requirement 12, "interfaces of safety with nuclear security and with the State system of accounting for and control of nuclear material," states, "The government shall ensure that within the governmental and legal framework adequate infrastructural arrangements are established for interfaces of safety with arrangements for nuclear security and with the State system of accounting for and control of nuclear material." This self-assessment is limited to interfaces with nuclear security.

Requirement 12 specifies four responsibilities within the governmental and legal framework. The NRC meets each of these responsibilities as described below; additional supporting detail may be found in the Executive Summary.

1. Assessment of the Configuration of Facilities and Activities for the Optimization of Safety with Factors Relating to Nuclear Security

The NRC's regulatory program specifically addresses assessment of the configuration of facilities and activities for the optimization of safety with factors relating to nuclear security. NRC regulations in 10 CFR 73.58 require licensees to ensure that adequate

programs for assessing, managing, and coordinating proposed changes and activities (including assessment of the configuration of facilities) are established such that adverse interfaces between safety and security are identified and appropriate compensatory or mitigative actions are taken to maintain both safety and security. Compliance with the regulations is determined through inspections and the ROP.

2. Oversight and Enforcement To Maintain Arrangements for Safety and Nuclear Security

The NRC's regulatory framework includes oversight and inspection programs to maintain arrangements for safety and nuclear security. Module VII discusses the NRC's oversight and inspection programs in detail.

3. Liaison with Law Enforcement

The NRC's regulatory program specifically addresses liaison with law enforcement. NRC regulations in 10 CFR 73.55(k)(9) require licensees, to the extent practicable, to document and maintain current agreements with applicable law enforcement agencies. Liaison efforts with law enforcement are exercised as part of the HAB drills and security performance drills. Compliance with the regulations is determined through inspections and the ROP.

4. Integration of Emergency Response Arrangements for Safety-Related and Nuclear Security-Related Incidents

The NRC requires licensees to consider safety and security implications of all aspects of nuclear power plant operation, including emergency planning and response. Recent emergency exercises have included security-related scenarios (HAB drills). The NRC has further integrated safety and security into its emergency response arrangements in the proposed EP rule.

Conclusion

Consideration of the safety/security interface has been implemented into all key aspects of the NRC's nuclear power plant regulatory framework. The NRC has taken measurable steps in its regulatory processes to improve the interfaces with nuclear security including the following:

1. developing specific regulations and guidance documents in its regulatory program
2. revising the reactor oversight framework
3. coordinating internal agency processes
4. improving liaison with local, State, and Federal law enforcement agencies
5. incorporating security-initiated activities in EP exercises
6. revising the NRC's safety culture policy statement to include security concerns

Areas for Improvement

The Module 12 Executive Summary provides an overview of the NRC's processes for managing the safety/security interface. These processes, when taken together, provide a comprehensive approach to managing the safety/security interface and issues that arise within it.

In reviewing its internal safety/security coordination activities, the NRC determined that the guidance in COM-111 needs to be enhanced. For instance, some of the actions in the office

instruction will need to be reevaluated to ensure they remain practical and effective, including annual meetings of the interoffice review board. The NRC organization, management, and personnel have changed since the initial issuance of COM-111. Other internal procedures need review to address whether they need to include safety/security interface actions. Upon update of COM-111, the NRC staff needs further orientation as to its responsibilities to identify and communicate to affected organizations the potential safety/security interface issues, as described in COM-111.