AUDIT REPORT

Audit of NRC's Force-on-Force
Inspection Program

OIG-09-A-12 July 30, 2009

All publicly available OIG reports (including this report) are accessible through NRC's Web site at:
http:/www.nrc.gov/reading-rm/doc-collections/insp-gen/

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF THE
INSPECTOR GENERAL

July 30, 2009

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

FROM: Stephen D. Dingbaum **/RA/**
Assistant Inspector General for Audits

SUBJECT: AUDIT OF NRC'S FORCE-ON-FORCE INSPECTION PROGRAM (OIG-09-A-12)

Attached is the Office of the Inspector General's (OIG) audit report titled, *Audit of NRC's Force-on-Force Inspection Program.*

The report presents the results of the subject audit. Agency comments provided during and subsequent to a July 21, 2009, exit conference have been incorporated, as appropriate, into this report.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this memorandum. Actions taken or planned are subject to OIG followup as stated in Management Directive 6.1.

We appreciate the cooperation extended to us by members of your staff during the audit. If you have any questions or comments about our report, please contact me at 415-5915 or Beth Serepca, Team Leader, at 415-5911.

Attachment: As stated

Electronic Distribution

Edward M. Hackett, Executive Director, Advisory Committee on Reactor Safeguards
E. Roy Hawkens, Chief Administrative Judge, Atomic Safety and Licensing Board Panel
Stephen G. Burns, General Counsel
Brooke D. Poole, Jr., Director, Office of Commission Appellate Adjudication
Jim E. Dyer, Chief Financial Officer
Margaret M. Doane, Director, Office of International Programs
Rebecca L. Schmidt, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
R. William Borchardt, Executive Director for Operations
Bruce S. Mallett, Deputy Executive Director for Reactor and Preparedness Programs, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Waste, Research, State, Tribal, and Compliance Programs, OEDO
Darren B. Ash, Deputy Executive Director for Corporate Management and Chief Information Officer, OEDO
Vonna L. Ordaz, Assistant for Operations, OEDO
Kathryn O. Greene, Director, Office of Administration
Cynthia A. Carpenter, Director, Office of Enforcement
Charles L. Miller, Director, Office of Federal and State Materials and Environmental Management Programs
Guy P. Caputo, Director, Office of Investigations
Thomas M. Boyce, Director, Office of Information Services
James F. McDermott, Director, Office of Human Resources
Michael R. Johnson, Director, Office of New Reactors
Michael F. Weber, Director, Office of Nuclear Material Safety and Safeguards
Eric J. Leeds, Director, Office of Nuclear Reactor Regulation
Brian W. Sheron, Director, Office of Nuclear Regulatory Research
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
Luis A. Reyes, Regional Administrator, Region II
Mark A. Satorius, Region III
Elmo E. Collins, Jr., Regional Administrator, Region IV

EXECUTIVE SUMMARY

BACKGROUND

The Nuclear Regulatory Commission (NRC) conducts Force-on-Force inspections at each of the Nation's nuclear power plants on at least a triennial basis in accordance with the 2005 Energy Policy Act.[1] A Force-on-Force inspection is a performance-based inspection designed to assess the ability of licensees' security organizations to protect their facilities against sabotage.[2] Any potentially significant deficiencies identified during these inspections are to be promptly corrected by the licensee.

The Office of Nuclear Security and Incident Response (NSIR) manages the Force-on-Force inspection program. Force-on-Force inspections are part of NRC's baseline physical protection inspection program, and are the only baseline inspections managed at the headquarters level.[3] Teams of headquarters-based inspectors and security risk analysts conduct inspections with support from physical security inspectors based in NRC's four regional offices. These regional inspectors provide site-specific knowledge and represent their respective offices while on site with headquarters staff and licensee employees. U.S. military personnel serve as technical advisors to the NRC teams and assist with some inspection tasks.

The Force-on-Force program budget for Fiscal Year (FY) 2009 is approximately $3.5 million, and composes about 6 percent of NSIR's FY 2009 budget. Of the 251 Full Time Equivalents (FTE) allocated to NSIR in FY 2009, 14.8 FTE (6 percent) are assigned to the Force-on-Force program. NRC began the second triennial Force-on-Force inspection cycle in January 2008. NRC plans to conduct 25 Force-on-Force inspections during FY 2009.

PURPOSE

The objective of this audit was to evaluate NRC's Force-on-Force inspection program to determine if design and implementation of the program are thorough, consistent, and in accordance with NRC

[1] Pub L. No. 109-58, "The 2005 Energy Policy Act," §651, August 8, 2005.

[2] NRC also conducts Force-on-Force inspections at other facilities that handle special nuclear materials, such as nuclear fuel cycle facilities. However, this audit focused on inspections at nuclear power plants.

[3] Inspection Procedure (IP) 71130, "Baseline Physical Protection Program."

standards. The audit focused on the program's development from the first triennial inspection cycle through the current second triennial inspection cycle.

RESULTS IN BRIEF

NRC conducts Force-on-Force inspections to evaluate licensees' ability to protect nuclear power plants against Design Basis Threat type adversaries. NRC meets its 2005 Energy Policy Act requirement to conduct Force-on-Force inspections on a triennial basis, and the program has adequate management controls to ensure that inspections are thorough and comply with NRC standards. In particular, the Office of the Inspector General found:

- NSIR management assessed the Force-on-Force program early in the second inspection cycle, and subsequently undertook organizational and procedural changes to improve internal controls and program performance.

- NSIR and regional staff differ over interpretation of some NRC guidance and approaches to conducting Force-on-Force inspections.

By taking steps to reach agreement between headquarters and regional staff regarding Force-on-Force inspection program guidance, objectives, and best practices, NRC can better ensure its credibility with licensees and foster positive working relationships among staff involved in the Force-on-Force inspection program.

RECOMMENDATIONS

All recommendations for this report appear at the end of Finding B.

AGENCY COMMENTS

At a July 21, 2009, exit conference, NRC senior managers agreed with the report contents and provided editorial suggestions. This final report incorporates revisions made, where appropriate, as a result of the agency's suggestions.

ABBREVIATIONS AND ACRONYMS

CAF	Composite Adversary Force
CFR	Code of Federal Regulations
DBT	Design Basis Threat
FTE	Full-Time Equivalent
FY	Fiscal Year
IDS	Intrusion Detection System
NRC	Nuclear Regulatory Commission
NSIR	Office of Nuclear Security and Incident Response

[Page intentionally left blank.]

TABLE OF CONTENTS

EXECUTIVE SUMMARY i

ABBREVIATIONS AND ACRONYMS iii

I. BACKGROUND 1

II. PURPOSE 4

III. FINDINGS 5

A. NSIR Management Has Assessed the Force-on-Force Program and Instituted Changes to Enhance its Performance 5

B. Headquarters and Regional Staff Differ Over Guidance and Approaches to Force-on-Force Inspections 8

IV. AGENCY COMMENTS 12

APPENDICES

A. TITLE 10, CODE OF FEDERAL REGULATIONS, SECTION 73.1a AND b 13

B. SCOPE AND METHODOLOGY 17

[Page intentionally left blank.]

I. BACKGROUND

The Nuclear Regulatory Commission (NRC) conducts Force-on-Force inspections at each of the Nation's nuclear power plants on at least a triennial basis in accordance with the 2005 Energy Policy Act.[4] A Force-on-Force inspection is a performance-based inspection designed to assess the ability of licensees' security organizations to protect their facilities against sabotage.[5] Any potentially significant deficiencies identified during these inspections are to be promptly corrected by the licensee.

The Office of Nuclear Security and Incident Response (NSIR) manages the Force-on-Force inspection program. Force-on-Force inspections are part of NRC's baseline physical protection inspection program, and are the only baseline inspections managed at the headquarters level.[6] Teams of headquarters-based inspectors and security risk analysts conduct inspections with support from physical security inspectors based in NRC's four regional offices. These regional inspectors provide site-specific knowledge and represent their respective offices while on site with headquarters staff and licensee employees. U.S. military personnel serve as technical advisors to the NRC teams and assist with some inspection tasks.

NRC conducts each Force-on-Force inspection in three phases. The first phase, target set[7] review, is performed by headquarters-based security risk analysts and generally occurs at least several weeks before onsite inspection work begins. Security risk analysts review plant operating procedures and documentation of plant operating systems in coordination with licensee security and engineering personnel. Following their evaluation, security risk analysts create a list of potential target sets to be used in planning the exercise portion of the inspection.

[4] Pub L. No. 109-58, "The 2005 Energy Policy Act," §651, August 8, 2005.

[5] NRC also conducts Force-on-Force inspections at other facilities that handle special nuclear materials, such as nuclear fuel cycle facilities. However, this audit focused on inspections at nuclear power plants.

[6] Inspection Procedure (IP) 71130, "Baseline Physical Protection Program."

[7] A target set is a combination of equipment, which, if damaged or disabled, would likely result in significant reactor core damage. Target sets also include plant operator actions intended to prevent or mitigate damage to this equipment.

During the second phase, pre-exercise planning week, NRC inspection teams composed of headquarters and regional staff conduct onsite planning and inspection work in preparation for Force-on-Force exercises. For example, the inspection teams conduct tabletop drills with licensee personnel to evaluate plant security plans against a series of possible attack scenarios. In addition to tabletop drills, the NRC inspection teams physically test plant intrusion detection systems,[8] and observe a sample of plant security personnel perform tactical demonstrations.

The exercise week is the last portion of the inspection. During this week, a composite adversary force (CAF) playing the role of a mock adversary group simulates attacks against the power plant.[9] The CAF is trained and equipped to approximate the capabilities of a design basis threat (DBT) adversary. The DBT reflects NRC's intelligence analysis of the type, composition, and capabilities of potential adversaries.[10] The CAF attempts to simulate destroying enough plant equipment to damage the power reactor's core or spent fuel pool, thereby triggering a release of radiation into the environment. The licensee's security personnel seek to interdict the CAF and prevent damage to plant equipment.

NRC gives plant operators 8 to12 weeks advance notice of Force-on-Force inspections for safety and logistical purposes. Plant staff must coordinate the efforts of two sets of security officers: one for maintaining site security during exercises, and another for participating in the exercises. In addition, plant staff must assemble and train a group of individuals, typically plant employees, to control and monitor exercises.

[8] NRC regulations require detection of penetration or attempted penetration of a power plant's protected area to ensure that the plant's security organization can adequately respond. A perimeter intrusion detection system generally consists of one or more sensors, electronic processing equipment, a power supply, signal transmission media, an alarm monitor with display, and a means for maintaining and providing an alarm history. See NRC Regulatory Guide 5.44, pp.1-2.

[9] The CAF is composed of security officers from various nuclear power plants, and is managed by a private company that provides security services for a number of U.S. nuclear power plants. Although NRC does not oversee CAF teams, NRC inspectors monitor CAF performance with assistance from U.S. military personnel assigned to inspection teams. NRC requires a separation of functions between the CAF and licensee security forces to ensure an independent, reliable, and credible mock adversary force.

[10] DBT details are classified; however, Title 10 Section 73.1 of the Code of Federal Regulations (CFR) prescribes general DBT adversary characteristics. See Appendix A for 10 CFR 73.1 a (Purpose) and b (Scope).

Licensee security personnel preparing for a Force-on-Force exercise.
Source: NRC

The Force-on-Force program budget for Fiscal Year (FY) 2009 is approximately $3.5 million, and composes about 7 percent of NSIR's FY 2009 budget. Of the 251 Full Time Equivalents (FTE) allocated to NSIR in FY 2009, 14.8 FTE (6 percent) are assigned to the Force-on-Force program. Table 1 shows program budget and FTE data for FY 2005 through FY 2009.

Table 1: Force-on-Force Program Annual Budgets and FTE

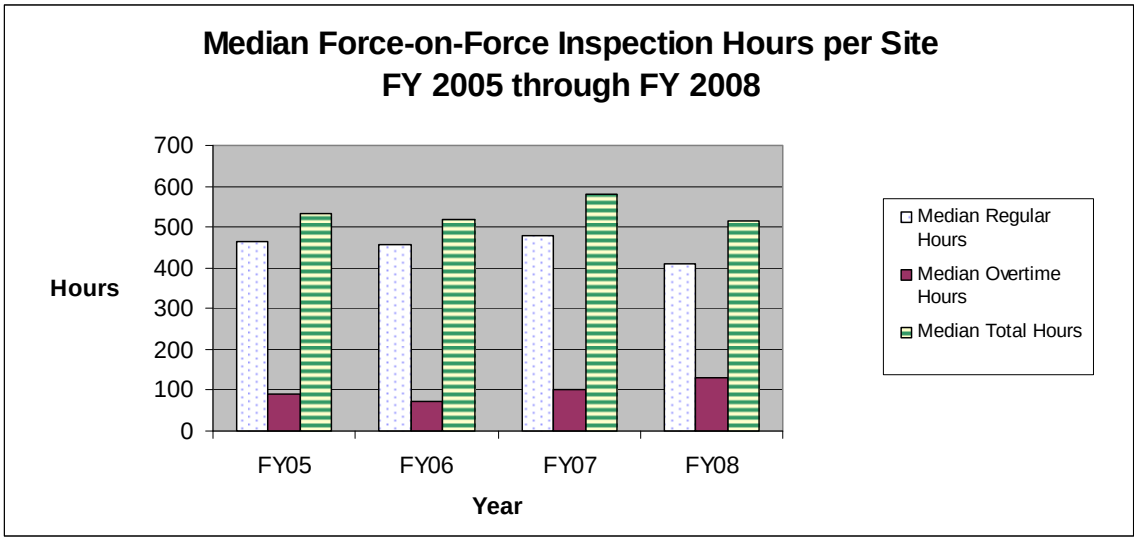
	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009
Budget	$1,878,397	$1,911,088	$1,395,392	$2,049,530	$3,500,000[11]
FTE	9.3	14.6	17.2	15.4	14.8

Source: OIG analysis of NSIR data.

NRC began the second triennial Force-on-Force inspection cycle in January 2008. NRC plans to conduct 25 Force-on-Force inspections during FY 2009. Auditor analysis of historical data found that inspector workload varies from site to site, depending on variables such as the amount of followup needed after each site's inspection. Graph 1 shows median annual inspection hours per site from FY 2005 through FY 2008.

[11] The program budget increase in FY 2009 reflects costs of upgrading Multiple Integrated Laser Engagement System equipment used to simulate gunfire in Force-on-Force exercises, as well as the purchase of a new truck and trailer to transport this equipment.

Graph 1: Median Annual Force-on-Force Inspection Hours Per Site



Source: OIG analysis of NSIR data.

II. PURPOSE

The objective of this audit was to evaluate NRC's Force-on-Force inspection program to determine if design and implementation of the program are thorough, consistent, and in accordance with NRC standards. The audit focused on the program's development from the first triennial inspection cycle through the current second triennial inspection cycle.

III. FINDINGS

NRC conducts Force-on-Force inspections to evaluate licensees' ability to protect nuclear power plants against DBT-type adversaries. NRC meets its 2005 Energy Policy Act requirement to conduct Force-on-Force inspections on a triennial basis, and the program has adequate management controls to ensure that inspections are thorough and comply with NRC standards. In particular, the Office of the Inspector General found:

- NSIR management assessed the Force-on-Force program early in the second inspection cycle, and subsequently undertook organizational and procedural changes to improve internal controls and program performance.

- NSIR and regional staff differ over interpretation of some NRC guidance and approaches to conducting Force-on-Force inspections.

By taking steps to reach agreement between headquarters and regional staff regarding Force-on-Force inspection program guidance, objectives, and best practices, NRC can better ensure its credibility with licensees and foster positive working relationships among staff involved in the Force-on-Force inspection program.

A. NSIR Management Has Assessed the Force-on-Force Program and Instituted Changes To Enhance Its Performance

As a best practice, management should periodically assess programs and apply the results to improve program performance. In response to industry concerns regarding the consistency of inspections, NSIR staff assessed the Force-on-Force program in summer 2008. Following this assessment, NSIR management implemented several organizational and procedural changes designed to improve program performance. Some of these changes were instituted through revision of the Force-on-Force inspection procedure.[12]

[12] The current version of IP 71130.03 took effect in February 2009.

Branch Reorganization

NSIR management created the Security Training and Support Branch to manage inspection scheduling, development of new guidance, staff training, and other support tasks. These tasks were previously performed by the Security Performance Evaluation Branch, which also runs Force-on-Force inspections. The new organization enables the Security Performance Evaluation Branch to focus on inspections, and divides management duties between the respective branch chiefs.

Standardization of Training Requirements

Headquarters-based Force-on-Force inspectors are now required to satisfy full qualification standards prescribed in Inspection Manual Chapter 1245. This aligns the program with qualification standards for regional-based physical security inspectors. Previously, Force-on-Force inspectors were not subject to Inspection Manual Chapter 1245 standards and thus were not required to undergo training and demonstrate proficiency in basic inspection skills.

Increased Recruitment and Training of Force-on-Force Personnel

NSIR management has increased recruiting and training of security risk analysts and Force-on-Force inspectors to add rotational depth and distribute workload more evenly among staff. These efforts respond to workload and inspection schedule pressures, as well as reportedly high staff turnover problems during the first inspection cycle. Though Force-on-Force team members rated morale as high, several acknowledged that the frequent travel and long work days required for inspections are significant sources of stress.

Revised Target Set Review Procedures and Standards

NSIR management introduced new target set review procedures and adopted new standards for the types of actions plant operators could take to protect critical plant equipment. Previously, NSIR security risk analysts conducted site visits during the pre-exercise planning week, which limited target set review time and increased the chance of unresolved issues impacting subsequent exercises. Security risk analysts now review target set information and visit licensees' sites before Force-on-Force inspections begin. In addition, the new inspection procedure enhances criteria that

licensees must meet to receive credit for actions that plant operators would take during a contingency, such as a terrorist attack, to protect target set equipment. Specifically, licensees must demonstrate that their operators are properly trained and equipped, and are physically capable of performing planned protective actions while their plant is under attack.[13]

Escalation Process

The revised inspection procedure provides licensees a formal escalation process for resolving disputes with NRC about inspection planning and conduct. The process is designed to resolve disputes at the lowest NSIR management level necessary, and progressively elevate matters as higher management involvement is warranted. This enables Force-on-Force inspection team leaders to focus on inspection tasks while NSIR managers work directly with licensee managers to address their concerns, thereby reducing the impact of disputes on inspection schedules.

Exercise Lessons Learned

The revised inspection procedure establishes a formal process for capturing lessons learned and applying them to program guidance. According to NSIR staff, this previously occurred informally as staff shared observations about inspections verbally among themselves. The new procedure includes a template to be used in documenting lessons learned during inspections. Moreover, this new guidance requires managers to document cases in which lessons learned could serve as the basis for revising program guidance.

Because these organizational and procedural changes have only recently been implemented, it is too early for OIG to evaluate the effectiveness of each change in meeting its intended goals. However, based on feedback received from industry and NRC staff, OIG believes these changes have the potential to enhance the efficiency, transparency, and rigor of the Force-on-Force inspection program.

[13] For instance, licensees cannot claim credit if high radiation or other environmental hazards would prevent operators from carrying out protective actions. Additionally, plant operators must be capable of accessing target set equipment without risking their own safety by confronting adversaries or passing through areas controlled by adversaries.

B. Headquarters and Regional Staff Differ Over Guidance and Approaches to Force-on-Force Inspections

Improved coordination of headquarters and regional inspection activities would result from a shared understanding of policies and procedures, and open communication among staff. Headquarters and regional staff differ over interpretation of some inspection guidance, and over approaches to conducting Force-on-Force inspections. This has occurred in part because the program has undergone substantial changes in a short period of time, but procedural changes have not been effectively communicated to regional staff in a systematic fashion. Additionally, differences among headquarters and regional staff with respect to professional backgrounds and skillsets are an additional factor. These issues have not compromised Force-on-Force inspections; however, disagreements between headquarters and regional staff regarding procedures and policy can undermine NRC's credibility with licensees and degrade staff morale.

Coordination of Headquarters and Regional Efforts Benefits From Shared Understanding of Policies and Procedures

Improved coordination of headquarters and regional inspection activities would result from a shared understanding of policies and procedures, and open communication among staff. Internal control principles applicable to NRC recommend that agency managers communicate openly about policies and procedures, both internally with their staff and externally with licensees. In addition, agency managers should be conscious of issues affecting their agency's internal control environment, including:

- Organizational structure and delegation of authority.
- Human capital policies and practices.
- Employee morale, competence, and discipline.

Headquarters and Regional Staff Differ Over Inspection Guidance and Approaches

Headquarters and regional staff differ over interpretation of some inspection guidance, and over approaches to conducting Force-on-Force inspections. First, auditors found disagreements among some staff regarding NRC's process for determining ownership of findings resulting from Force-on-Force inspections. Specifically, staff said NRC lacked clear direction regarding the scope of headquarters and regional responsibilities for developing and following up on findings. In addition, some regional staff expressed

concern that headquarters was assuming more responsibility for non-Force-on-Force baseline security issues, which have traditionally been the responsibility of NRC's regional offices. This issue was eventually resolved during a May 2009 counterpart meeting involving headquarters and regional staff, and NSIR management agreed to clarify the inspection guidance.

Second, headquarters and some regional staff differ in their interpretations about procedural standards for Intrusion Detection System (IDS) testing. These standards determine how Force-on-Force teams "challenge test" licensees' systems during the pre-exercise planning week. Challenge testing entails broader goals and fewer constraints than operational tests performed by licensees; thus, interpretation of NRC's standards affects staff and licensee perceptions about whether Force-on-Force teams conduct challenge testing with an appropriate level of rigor.[14]

Headquarters and some regional staff expressed differing views about headquarters teams' approaches to conducting Force-on-Force inspections. The majority of regional staff interviewed characterized these inspections as excessively adversarial, and attributed this to what they perceive as an overly aggressive mentality among headquarters staff and the CAF. Further, a few regional staff believed Force-on-Force exercise scenarios developed by the headquarters based teams exaggerate real-world threats to power plants. In contrast, headquarters-based Force-on-Force staff who expressed an opinion felt that that the exercises fairly test licensee security programs and appropriately fulfill NRC's regulatory[15] and statutory[16] requirements to evaluate licensees using credible, challenging scenarios reflecting DBT characteristics.[17]

[14] Force-on-Force teams conduct operational testing during the pre-exercise planning week to ensure licensees' IDS equipment functions as designed and complies with standards in NRC Regulatory Guide 5.44. Teams also conduct challenge testing, which probes the IDS for vulnerabilities that an adversary might exploit. According to IP 71130.03, challenge testing is to simulate DBT-adversary actions and is not bounded by NRC Regulatory Guide 5.44 Option 1 or 2 standards.

[15] NRC guidance requires inspection team leaders to select scenarios that challenge licensees' protective strategies, and to ensure that scenarios target site-specific vulnerabilities. See IP 71130.03, p.31.

[16] According to the 2005 Energy Policy Act, NRC shall conduct exercises that "to the maximum extent practicable, simulate security threats in accordance with any design basis threat applicable to a facility." See Pub L. No. 109-58, "The 2005 Energy Policy Act," §651, August 8, 2005.

[17] NRC Regulatory Guide 5.69 provides Force-on-Force teams guidance for planning and conducting exercises. IP 71130.03 includes an addendum, or "tactics guide," to help inspection teams apply DBT-adversary characteristics to exercise scenarios.

Staff Differences Result From Rapid Program Change, Lack of Systematic Communication, and Other Factors

Differences between headquarters and regional staff interpretations of inspection guidance have resulted primarily from rapid program change and lack of systematic communication. The professional backgrounds of staff and team dynamics are additional factors. First, the Force-on-Force inspection program has undergone significant organizational and procedural changes since August 2008. NSIR staff have briefed licensee personnel and industry representatives on these changes and their implications, yet policy and procedural changes have not been effectively communicated to regional staff in a systematic fashion. Regional managers said they communicate with NSIR management on an as-needed basis. Regional security inspectors learn of new policies and procedures by memos, e-mail, and their respective regional managers. Some information is communicated by headquarters-based staff to regional inspectors on site during Force-on-Force inspections.

Counterpart meetings are another means of sharing information; however, several regional staff suggested that these meetings would be more beneficial if held on a routine basis.

Second, regional and headquarters staff have different professional backgrounds, which influences team dynamics and inspection conduct. Regional physical security inspectors tend to have greater depth of experience with inspections and NRC's regulatory processes. Both headquarters and regional staff consider on-the-job training important for developing key skills such as communicating with licensees and documenting findings. In contrast, most headquarters-based Force-on-Force team members have less than 2 years of experience conducting Force-on-Force inspections.[18] However, all of the current Force-on-Force inspectors have previous military and/or law enforcement experience, which has some applicability to evaluating licensee security programs and planning offensive missions for exercises. This mix of personnel with different backgrounds, skills, and lengths

[18] The Force-on-Force program instituted formal training program for inspectors in the first quarter of FY 2009. As of April 2009, 9 of 12 Force-on-Force inspectors were certified basic inspectors; one inspector was fully certified.

of service—which is inherent in Force-on-Force team composition—impacts inspection planning and conduct as Force-on-Force team leaders try to leverage individuals' skills and apply lessons learned in conducting their work.[19]

Staff Differences Can Undermine NRC's Credibility With Licensees and Degrade Morale

Although the Force-on-Force program has management controls in place to ensure the consistency and transparency of inspections, lack of agreement on policy and procedures between regional and headquarters staff can undermine NRC's credibility with licensees. Regional staff told auditors that they need clear understanding of agency policy so they can explain NRC's actions to licensees. Otherwise, they risk contradicting their colleagues or misinforming licensee personnel, which can undermine the image of inspectors as competent, impartial regulators. Moreover, auditors found that unresolved disagreements between headquarters and regional staff can degrade morale by raising staff concerns about NSIR management's receptiveness to their ideas and concerns.

Recommendations

OIG recommends that the Executive Director for Operations:

1. Develop and implement a plan for routine communications between headquarters management and regional staff involved in the Force-on-Force program.

2. Encourage cross-training and rotational opportunities for headquarters and regional staff involved in the Force-on-Force program.

[19] Based on interview feedback, auditors found that the role of regional inspectors in Force-on-Force inspections depends upon various factors such as inspection team needs, team leader prerogative, and regional inspectors' seniority and expectations.

IV. AGENCY COMMENTS

At a July 21, 2009, exit conference, NRC senior managers agreed with the report contents and provided editorial suggestions. This final report incorporates revisions made, where appropriate, as a result of the agency's suggestions.

Appendix A

Title 10, Code of Federal Regulations, Section 73.1a and b

(a) ***Purpose*.** This part prescribes requirements for the establishment and maintenance of a physical protection system which will have capabilities for the protection of special nuclear material at fixed sites and in transit and of plants in which special nuclear material is used. The following design basis threats, where referenced in ensuing sections of this part, shall be used to design safeguards systems to protect against acts of radiological sabotage and to prevent the theft or diversion of special nuclear material. Licensees subject to the provisions of §73.20 (except for fuel cycle licensees authorized under Part 70 of this chapter to receive, acquire, possess, transfer, use, or deliver for transportation formula quantities of strategic special nuclear material), § 73.50, and §73.60 are exempt from § 73.1(a)(1)(i)(E), §73.1(a)(1)(iii), 73.1(a)(1)(iv), §73.1(a)(2)(iii), and §73.1(a)(2)(iv). Licensees subject to the provisions of §72.212 are exempt from §73.1(a)(1)(iv).

(1) Radiological sabotage.

(i) A determined violent external assault, attack by stealth, or deceptive actions, including diversionary actions, by an adversary force capable of operating in each of the following modes: A single group attacking through one entry point, multiple groups attacking through multiple entry points, a combination of one or more groups and one or more individuals attacking through multiple entry points, or individuals attacking through separate entry points, with the following attributes, assistance and equipment:

(A) Well-trained (including military training and skills) and dedicated individuals, willing to kill or be killed, with sufficient knowledge to identify specific equipment or locations necessary for a successful attack;

(B) Active (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack) or passive (e.g., provide information), or both, knowledgeable inside assistance;

(C) Suitable weapons, including handheld automatic weapons, equipped with silencers and having effective long range accuracy;

(D) Hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system; and

(E) Land and water vehicles, which could be used for transporting personnel and their hand-carried equipment to the proximity of vital areas; and

(ii) An internal threat; and

(iii) A land vehicle bomb assault, which may be coordinated with an external assault; and

(iv) A waterborne vehicle bomb assault, which may be coordinated with an external assault; and

(v) A cyber attack.

(2) Theft or diversion of formula quantities of strategic special nuclear material.

(i) A determined violent external assault, attack by stealth, or deceptive actions, including diversionary actions, by an adversary force capable of operating in each of the following modes: a single group attacking through one entry point, multiple groups attacking through one or more groups and one or individuals attacking through multiple entry points, or individuals attacking through separate entry points, with the following attributes, assistance and equipment:

(A) Well-trained (including military training and skills) and dedicated individuals, willing to kill or be killed, with sufficient knowledge to identify specific equipment or locations necessary for a successful attack;

(B) Active (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack) or passive (e.g., provide information), or both, knowledgeable inside assistance;

(C) Suitable weapons, including handheld automatic weapons, equipped with silencers and having effective long range accuracy;

(D) Hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safe-guards system;

(E) Land and water vehicles, which could be used for transporting personnel and their hand-carried equipment; and

(ii) An internal threat; and

(iii) A land vehicle bomb assault, which may be coordinated with an external assault; and

(iv) A waterborne vehicle bomb assault, which may be coordinated with an external assault; and

(v) A cyber attack.

(b) ***Scope***

(1) This part prescribes requirements for:

(i) The physical protection of production and utilization facilities licensed under parts 50 or 52 of this chapter,

(ii) The physical protection of plants in which activities licensed pursuant to part 70 of this chapter are conducted, and

(iii) The physical protection of special nuclear material by any person who, pursuant to the regulations in part 61 or 70 of this chapter, possesses or uses at any site or contiguous sites subject to the control by the licensee, formula quantities of strategic special nuclear material or special nuclear material of moderate strategic significance or special nuclear material of low strategic significance.

(2) This part prescribes requirements for the physical protection of special nuclear material in transportation by any person who is licensed pursuant to the regulations in parts 70 and 110 of this chapter who imports, exports, transports, delivers to a carrier for transport in a single shipment, or takes delivery of a single shipment free on board (F.O.B.) where it is delivered to a carrier, formula quantities of strategic special nuclear material, special nuclear material of moderate strategic significance or special nuclear material of low strategic significance.

(3) This part also applies to shipments by air of special nuclear material in quantities exceeding: (i) 20 grams or 20 curies, whichever is less, of plutonium or uranium-233, or (ii) 350 grams of uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope).

(4) Special nuclear material subject to this part may also be protected pursuant to security procedures prescribed by the Commission or another Government agency for the protection of classified materials. The provisions and requirements of this part are in addition to, and not in substitution for, any such security procedures. Compliance with the requirements of this part does

not relieve any licensee from any requirement or obligation to protect special nuclear material pursuant to security procedures prescribed by the Commission or other Government agency for the protection of classified materials.

(5) This part also applies to the shipment of irradiated reactor fuel in quantities that in a single shipment both exceed 100 grams in net weight of irradiated fuel, exclusive of cladding or other structural or packaging material, and have a total radiation dose in excess of 100 rems per hour at a distance of 3 feet from any accessible surface without intervening shielding.

(6) This part prescribes requirements for the physical protection of spent nuclear fuel and high-level radioactive waste stored in either an independent spent fuel storage installation (ISFSI) or a monitored retrievable storage (MRS) installation licensed under part 72 of this chapter, or stored at the geologic repository operations area licensed under part 60 or part 63 of this chapter.

(7) This part prescribes requirements for the protection of Safeguards Information (including Safeguards Information with the designation or marking: Safeguards Information—Modified Handling) in the hands of any person, whether or not a licensee of the Commission, who produces, receives, or acquires that information.

(8) This part prescribes requirements for advance notice of export and import shipments of special nuclear material, including irradiated reactor fuel.

(9) As provided in part 76 of this chapter, the regulations of this part establish procedures and criteria for physical security for the issuance of a certificate of compliance or the approval of a compliance plan.

Appendix B

SCOPE AND METHODOLOGY

The objective of this audit was to evaluate NRC's Force-on-Force inspection program to determine if design and implementation of the program are consistent, thorough, reasonable, and in accordance with NRC standards. The audit focused on the program's development from the first triennial inspection cycle through the current second triennial inspection cycle.

Auditors reviewed Federal Government laws and regulations applicable to the Force-on-Force inspection program, including:

- The 2005 Energy Policy Act, Section 651.
- 10 Code of Federal Regulations, Sections 73.1 and 73.55.

Auditors also reviewed NRC guidance governing baseline security inspection procedures, regulatory processes, employee training standards, and regulatory implementation guidance issued to licensees. Guidance included:

- Inspection Procedure 71130.03: *Contingency Response.*
- Inspection Procedure 71130.04: *Equipment Performance, Testing, and Maintenance.*
- Inspection Procedure 71130.05: *Protective Strategy Review.*
- Inspection Manual Chapter 0609, Appendix E: *Baseline Security Significance Determination Process for Power Reactors.*
- Inspection Manual Chapter 1245, *Qualification Program for the Office of the Nuclear Reactor Regulation Program.*
- Regulatory Guide 5.44, *Perimeter Intrusion Alarm Systems.*
- Regulatory Guide 5.69, *Guidance for the Application of the Radiological Sabotage Design-Basis Threat in the Design.*
- *Development, and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements.*

Auditors interviewed NSIR managers, Force-on-Force inspectors, security risk analysts, and security inspectors and managers from all four NRC regional offices to identify their respective roles responsibilities in the program. Staff with experience in both the first and second inspection cycles were asked to compare and contrast the two cycles, and to comment on programmatic changes undertaken since the first inspection cycle. Auditors reviewed e-mail correspondence and observed a secure video-teleconference involving headquarters and regional staff to corroborate interviews

and better understand internal deliberations over policy and procedure. Auditors interviewed industry representatives and licensee personnel to gather external perspectives on program performance and NRC management's receptivity to industry concerns. In addition, auditors observed two Force-on-Force inspections and one industry outreach conference.

Auditors reviewed staff training records to verify NRC's new training and qualification tracking mechanism for Force-on-Force staff. Auditors analyzed budget and FTE data to measure program resource trends, and also analyzed time and attendance data to measure workload associated with Force-on-Force inspections.

OIG conducted this audit between January 2009 and June 2009 in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objective.

Major contributors to this report were: Beth Serepca, Team Leader; Paul Rades, Audit Manager; Jaclyn Storch, Senior Analyst; and Maxinne Lorette, Senior Auditor.