# AUDIT REPORT

Audit of NRC's Management of the Baseline Security Inspection Program

OIG-12-A-10   March 8, 2012

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

March 8, 2012

MEMORANDUM TO:     R. William Borchardt
                   Executive Director for Operations


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


SUBJECT:           AUDIT OF NRC'S MANAGEMENT OF THE BASELINE
                   SECURITY INSPECTION PROGRAM (OIG-12-A-10)


Attached is the Office of the Inspector General's audit report titled, *Audit of NRC's Management of the Baseline Security Inspection Program.*

This report presents the results of the subject audit.  Agency comments provided at the February 29, 2012, exit conference have been incorporated, as appropriate, into this report.

Please provide information on actions taken or planned regarding each of the recommendations within 30 days of the date of this memorandum.  Actions taken or planned are subject to OIG follow-up in accordance with Management Directive 6.1.

We appreciate the cooperation extended to us by the members of your staff during this audit.  If you have any questions or wish to discuss anything prior to the exit conference, please call me at 415-5915 or Beth Serepca, Team Leader, at 415-5911.

Attachment:  As stated

cc:    N. Mamish, OEDO
       K. Brock, OEDO
       J. Arildsen, OEDO
       C. Jaegers, OEDO

# EXECUTIVE SUMMARY

## BACKGROUND

### Baseline Security Inspection Program

The Nuclear Regulatory Commission's (NRC) baseline security inspection program is the agency's primary means for ensuring that nuclear power plants across the United States are protected in accordance with Federal Government regulations.[1]  Specifically, the baseline security inspection program has six objectives:

1.  To gather sufficient, factual information to determine with high assurance if a licensee's security system and material control and accounting program[2] can protect against radiological sabotage, and the theft or loss of special nuclear material.

2.  To determine a licensee's ability to identify, assess, and correct security issues in proportion with the significance of these issues.

3.  To determine if licensees, working with external agencies, are capable of deterring and protecting against the Design Basis Threat.[3]

4.  To validate performance indicator data, which NRC uses in conjunction with inspection findings to assess the security performance of power reactor licensees.

5.  To help NRC monitor plants' security status and conditions.

---

[1] Chapter 10 Part 73 of the Code of Federal Regulations (10 CFR 73) establishes security regulations for operating nuclear power plants.

[2] The basic objective of material control and accounting is to prevent the loss or misuse of Special Nuclear Material (i.e., enriched uranium or plutonium).

[3] The Design Basis Threat describes the capabilities of adversaries, such as terrorist groups, that could attack a nuclear power plant.  The Design Basis Threat is based on classified and other sensitive information, and NRC revises it periodically to reflect current security issues.  An unclassified version appears in 10 CFR 73.1(a).

6. To identify significant issues that may have generic or crosscutting applicability to the safe and secure operation of licensees' facilities.

To meet these objectives, NRC conducts routine inspections at nuclear power plants that focus on specific issue areas such as access controls, protective strategy, security training, and safeguards information (SGI) controls.[4]

**Significance Determination Process**

The Significance Determination Process (SDP) is the process by which NRC staff assess the risks and potential effects of inspection findings. In following the SDP, NRC staff systematically analyze apparent violations and characterize them under the following color-code scheme:

- Green = Very low safety significance.
- White = Low to moderate safety significance.
- Yellow = Substantial safety significance.
- Red = High safety significance.

NRC staff close Green findings in their inspection reports without additional analysis, but White, Yellow, and Red findings require more in-depth analysis using SDP assessment tools. Since 2004, NRC has created several assessment tools for different types of security violations. These tools and their respective issue areas are:

- Physical Protection [Access Controls, Access Authorization, Physical Protection, Contingency Response].
- Material Control and Accounting of Radiological Materials.
- Unsecured Safeguards Information.
- Significance Screen.[5]
- Force-on-Force Exercise Performance.

---

[4] SGI is defined as information the disclosure of which could reasonably be expected to have a significant adverse effect on the health and safety of the public and/or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of material or facilities subject to NRC jurisdiction. This information is not classified as National Security Information or Restricted Data.

[5] The Significance Screen is used to assess violations such as security personnel sleeping on duty; pipes leading from outside a plant into the plant's Protected Area without adequate barriers or monitoring; and unauthorized firearms brought inside a plant by employees or contractors.

**PURPOSE**

The objective of this audit was to evaluate NRC's management of the baseline security inspection program, including specific program features such as the Significance Determination Process.

**RESULTS IN BRIEF**

NRC has appropriate management controls to ensure the baseline security inspection program meets its objectives. However, a more systematic approach to analyzing security findings data beyond the regional level can help NRC staff better identify licensee performance trends. Further, periodic reviews of SDP assessment tools and systematic testing of new and revised SDP assessment tools can help staff apply SDP assessment tools in a more transparent and consistent manner.

**RECOMMENDATIONS**

This report makes five recommendations to improve NRC's management of the baseline security inspection program. A list of these recommendations appears on page 18 of this report.

**Agency Comments**

At an exit conference on February 29, 2012, agency management provided informal comments on a draft of this report. The Office of the Inspector General incorporated some of these comments into the report as appropriate. As a result, the agency opted not to provide formal comments for inclusion in this report.

# ABBREVIATIONS AND ACRONYMS

ADAMS      Agencywide Documents Access and Management System

CFR      Code of Federal Regulations

FTE      Full-Time Equivalents

FY      Fiscal Year

IMC      Inspection Manual Chapter

MD      Management Directive

NRC      Nuclear Regulatory Commission

OIG      Office of the Inspector General

PIM      Plant Issues Matrix

ROP      Reactor Oversight Process

RPS      Reactor Program System

SDP      Significance Determination Process

SGI      Safeguards Information

SLES      Safeguards Information Local Area Network and Electronic Safe

# TABLE OF CONTENTS

## I.    BACKGROUND

The Nuclear Regulatory Commission's (NRC) baseline security inspection program is the agency's primary means for ensuring that nuclear power plants across the United States are protected in accordance with Federal Government regulations.[6]  Specifically, the baseline security inspection program has six objectives:

1. To gather sufficient, factual information to determine with high assurance if a licensee's security system and material control and accounting program[7] can protect against radiological sabotage, and the theft or loss of special nuclear material.

2. To determine a licensee's ability to identify, assess, and correct security issues in proportion with the significance of these issues.

3. To determine if licensees, working with external agencies, are capable of deterring and protecting against the Design Basis Threat.[8]

4. To validate performance indicator data, which NRC uses in conjunction with inspection findings to assess the security performance of power reactor licensees.

---

[6] Chapter 10 Part 73 of the Code of Federal Regulations (10 CFR 73) establishes security regulations for operating nuclear power plants.

[7] The basic objective of material control and accounting is to prevent the loss or misuse of Special Nuclear Material (i.e., enriched uranium or plutonium).

[8] The Design Basis Threat describes the capabilities of adversaries, such as terrorist groups, that could attack a nuclear power plant.  The Design Basis Threat is based on classified and other sensitive information, and NRC revises it periodically to reflect current security issues.  An unclassified version appears in 10 CFR 73.1(a).

5. To help NRC monitor plants' security status and conditions.

6. To identify significant issues that may have generic or crosscutting applicability to the safe and secure operation of licensees' facilities.

To meet these objectives, NRC conducts routine inspections at nuclear power plants that focus on specific issue areas such as access controls, protective strategy, security training, and safeguards information (SGI) controls.[9] Personnel at NRC's four regional offices plan and conduct baseline security inspections at nuclear power plants within their respective regions. Headquarters staff in NRC's Office of Nuclear Security and Incident Response (NSIR) support baseline security inspections through policy and guidance development, licensee performance data review, and review of escalated licensee violations. NSIR staff also conduct Force-on-Force inspections—the only type of baseline security inspections conducted by headquarters staff with support from regional staff.[10] In Fiscal Year (FY) 2012, NRC allocated 11.5 Full-Time Equivalents (FTE) for headquarters activities in the baseline security inspection program, and 5.7 FTE for program activities at each of the four regions for a total of 34.3 FTE. NRC staff expect these resource levels to remain constant in FY 2013.

---

[9] SGI is defined as information the disclosure of which could reasonably be expected to have a significant adverse effect on the health and safety of the public and/or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of material or facilities subject to NRC jurisdiction. This information is not classified as National Security Information or Restricted Data.

[10] Force-on-Force inspections require licensees to demonstrate their security capabilities through tactical exercises in which mock terrorist groups simulate attacks against nuclear power plants. Congress mandated triennial Force-on-Force inspections in the 2005 Energy Policy Act.

Figure 1 shows NRC's regions, as well as the locations of regional and headquarters offices, and the agency's Technical Training Center.

**Figure 1: Map of the United States and NRC Regions**
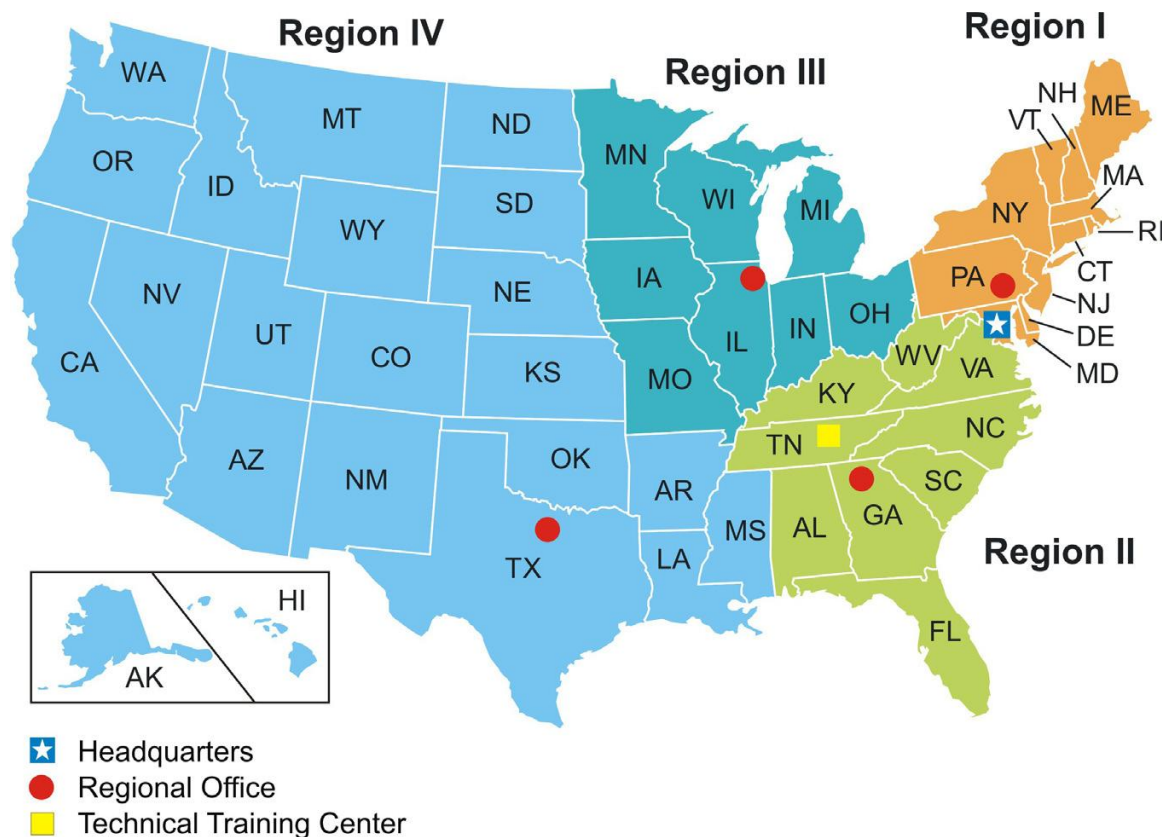


Source: NRC

**Significance Determination Process**

The Significance Determination Process (SDP) is the process by which NRC staff assess the risks and potential effects of inspection findings. In following the SDP, NRC staff systematically analyze apparent violations and characterize them under the following color-code scheme:

- Green = Very low safety significance.
- White = Low to moderate safety significance.
- Yellow = Substantial safety significance.
- Red = High safety significance.

NRC staff close Green findings in their inspection reports without additional analysis, but White, Yellow, and Red findings require more in-depth analysis using SDP assessment tools. Since 2004, NRC has created several assessment tools for different types of security violations. These tools and their respective issue areas are:

- Physical Protection [Access Controls, Access Authorization, Physical Protection, Contingency Response].
- Material Control and Accounting of Radiological Materials.
- Unsecured Safeguards Information.
- Significance Screen.[11]
- Force-on-Force Exercise Performance.

---

[11] The Significance Screen is used to assess violations such as security personnel sleeping on duty; pipes leading from outside a plant into the plant's Protected Area without adequate barriers or monitoring; and unauthorized firearms brought inside a plant by employees or contractors.

Figure 2 shows security barriers, which are one of many security system elements that NRC staff inspect at nuclear power plants.

**Figure 2: Security Barriers at a Nuclear Power Plant**



Source: NRC

White, Yellow, and Red findings require additional review by NRC staff. First, NRC notifies licensees of a finding, and licensees must then formally respond by either accepting the finding and committing to corrective actions, or by contesting the finding. Second, NRC management must review findings to ensure that their staff have applied SDP assessment tools correctly. Third, if licensees contest findings, they may provide mitigating information or other analysis to explain why they believe findings should be downgraded. NRC staff must factor this information into their final decision. Lastly, the technical complexity of a particular finding can impact the amount of time and effort needed by NRC staff and licensee personnel to support their respective positions.

Greater-than-Green findings are relatively uncommon in the baseline security inspection program.  In 2010, for example, NRC issued 112 Green findings, and 6 Greater-than-Green findings.[12]

Correct and consistent application of SDP assessment tools is essential to the Reactor Oversight Process (ROP), which is NRC's framework for regulating the nuclear power industry.  The ROP is based upon principles of risk-informed decisionmaking and transparency.  Accordingly, NRC should:

- Focus inspections on activities where the potential risks are greater.
- Apply greater regulatory attention to nuclear power plants with performance problems.
- Use objective measurements of performance of nuclear power plants.
- Give both the public and the nuclear industry timely and understandable assessments of plant performance.
- Respond to violations of regulations in a predictable and consistent manner that reflects the potential safety impact of the violations.
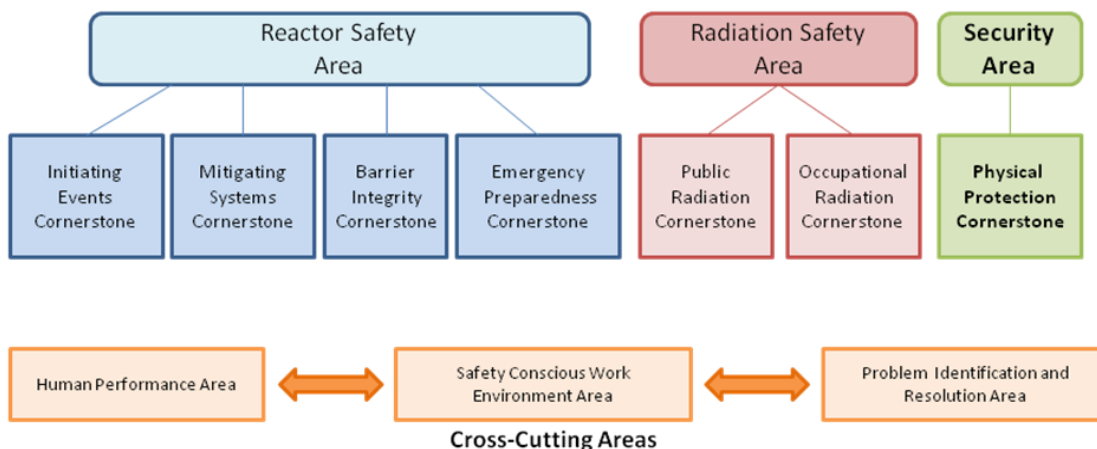
The ROP categorizes NRC's oversight activities into seven distinct "cornerstones" of safe operation, one of which is physical protection.  NRC also assesses licensee performance in the context of cross-cutting issues, such as problem identification and resolution, which may affect multiple ROP cornerstones.

---

[12] These do not include results of Force-on-Force inspections.

Figure 3 illustrates the ROP cornerstones and their relation to key oversight areas and cross-cutting issue areas.

**Figure 3: Reactor Oversight Process Framework**

**Reactor Oversight Process Framework: Key Oversight Areas And Cornerstones**

| Reactor Safety Area | | | | Radiation Safety Area | | Security Area |
|---|---|---|---|---|---|---|
| Initiating Events Cornerstone | Mitigating Systems Cornerstone | Barrier Integrity Cornerstone | Emergency Preparedness Cornerstone | Public Radiation Cornerstone | Occupational Radiation Cornerstone | **Physical Protection Cornerstone** |

| Human Performance Area | ⟷ | Safety Conscious Work Environment Area | ⟷ | Problem Identification and Resolution Area |
|---|---|---|---|---|

**Cross-Cutting Areas**

Source: NRC

> The ROP is complemented by NRC's enforcement program, which, in this context, focuses on violations that are caused by deliberate misconduct. NRC may pursue enforcement action against licensees while staff are determining a finding's significance within the ROP framework. Enforcement action can result in the issuance of civil penalties against licensees.

## II.    PURPOSE

The audit objective was to evaluate NRC's management of the baseline security inspection program, including specific program features such as the Significance Determination Process.  Appendix B contains information on the audit scope and methodology.

## III.    FINDINGS

NRC has appropriate management controls to ensure the baseline security inspection program meets its objectives.  However, a more systematic approach to analyzing security findings data beyond the regional level can help NRC staff better identify licensee performance trends.  Further, periodic reviews of SDP assessment tools and systematic testing of new and revised SDP assessment tools can help staff apply SDP assessment tools in a more transparent and consistent manner.

## A. NRC Can Improve Internal Control Over Baseline Security Inspection Program Data

Federal Government and NRC guidance on internal control[13] recommend the use of data analysis to inform program operations and management. NRC maintains data on security inspection findings, but does not systematically analyze it to identify trends among NRC regions and licensee fleets.[14] This occurs because NRC's baseline security inspection program emphasizes analysis of individual licensee performance and performance of licensees within each of the four NRC regions. As a result, NRC may miss opportunities to improve monitoring and management of security issues, inspection procedures, and tools.

### Effective Internal Control Is Key To Maintaining Visibility Over Program Operations and Results.

Federal Government and NRC internal control guidance recommend that program managers analyze appropriate information sources used in the baseline security inspection program to inform program operations and decisions and to ensure programs achieve intended results. Internal controls comprise the plans, methods, and procedures used to meet missions, goals, and objectives. These controls include managers at all levels analyzing trends and measuring results against targets. Controls must be developed as programs are initially implemented, as well as when they are reengineered. Additionally, managers should employ a variety of activities ensuring that edit checks are used in controlling data entry and that access to data and data systems is appropriately controlled.

---

[13] Standards for Internal Control in the Federal Government (GAO/AIMD-00-21.3.1) U.S. General Accounting Office, Washington DC: 1999 and NRC Management Directive 4.4,"Management Controls," May 18, 2004.

[14] A fleet refers to a group of nuclear power plants operated by one licensee. Plants belonging to a licensee's fleet can be located in one or more NRC regions.

## NRC Does Not Perform Systematic Cross-Regional or Cross-Fleet Analysis of Security Trends

NRC maintains and uses multiple information sources to monitor plant performance, but managers do not perform systematic analysis to assess trends across NRC regions or licensee fleets.  For example, NRC maintains many information sources pertaining to inspection findings and has visibility over individual plant performance through the use of inspection reports stored in the Agencywide Documents Access and Management System (ADAMS),[15] inspection reports stored in the Safeguards Information Local Area Network and Electronic Safe (SLES),[16] mid- and end-of-cycle assessments, the Plant Issues Matrix (PIM), Reactor Program System (RPS) data, and annual reports to Congress. However, NRC does not perform systematic cross-regional or cross-fleet analysis of security inspection trends.  Figure 4 shows information sources used in the baseline security inspection program.

---

[15] ADAMS is the official recordkeeping system through which NRC provides access to vast "libraries" or collections of documents related to the agency's regulatory activities.

[16] SLES is NRC's information repository for all SGI.

**Figure 4: NRC Baseline Security Inspection Program Information Sources**

| Information Source | Description |
|---|---|
| **Inspection Reports** | Inspection reports, written by NRC inspectors, provide NRC with all the details of the final disposition of findings uncovered during NRC inspections of power reactors. Details include the date of the inspection, the number and types of findings, and the safety significance (color designation of the finding). |
| **SLES** | NRC's repository for all inspection reports and other documents containing SGI. |
| **Mid/End Cycle Plant Assessment Reports** | Reports issued at the beginning of March and September of each year for each reactor site. The reports state whether the plant is receiving increased oversight and the number of planned inspections. |
| **PIM** | The PIM provides a consolidated listing of individual plant issues (i.e., inspection findings) that NRC uses to assess plant performance. |
| **RPS** | A system used by NRC to enter administrative data about inspection scheduling and limited data regarding inspection results. |
| **Annual Report to Congress** | A report that provides a basic count of inspection findings for the year. |

Source: Office of the Inspector General (OIG) analysis of information sources

Additionally, regional branch chiefs stated that they can request that headquarters generate reports in response to individual staff requests, but reports focus on individual regions and requesters' individual data needs. However, the headquarters representative responsible for responding to such requests told OIG that this type of analysis is labor intensive and requires piecing together data from the multiple sources listed above.

Incidentally, it is important for NRC to perform cross-regional and cross-fleet analysis for purposes of identifying areas that may need more regulatory emphasis. This analysis can also be used to make strategic program decisions, inform the tools and inspection procedures that are used to develop findings, and ensure the program is achieving its intended results.

Likewise, comprehensive cross-regional and cross-fleet analysis is important because NRC performs baseline security inspection activities at 104 reactor units within 65 reactor sites throughout NRC's four regions (see Figure 5). Moreover, approximately 45 percent of power reactor licensees manage more than one reactor site, and approximately 20 percent maintain reactor sites in more than one region. See Appendix A for a table showing power reactor sites by licensee operator and their locations by NRC region.

**Figure 5: Breakdown of Regional Reactor Sites and Reactor Units**

|  | Region 1 | Region 2 | Region 3 | Region 4 | Totals |
|---|---|---|---|---|---|
| **Reactor Sites** | 17 | 18 | 16 | 14 | 65 |
| **Reactor Units** | 26 | 33 | 24 | 21 | 104 |

Source: OIG analysis of NRC data

**NRC Management Does Not Emphasize Trend Analysis Across Regions and Fleets**

OIG found that NRC does not perform trend analysis across regions and fleets because program management emphasizes analysis of individual plant performance, and trends within each of the four regions. Additionally, NRC does not actively maintain and manage a centralized database for analyzing security inspection findings across regions and fleets as evidenced by OIG's analysis of NRC's current information sources.

Further, OIG could not determine if data in existing data systems is complete and accurate. Two of the data systems NRC headquarters staff use to access information may not be complete or accurate.

- First, RPS is used to collect information about scheduling inspections and also collects basic data points about findings. NRC does not use a single, consistent process for data entry or define data management controls for users of this database. The headquarters official responsible for obtaining and analyzing data from this system stated that, up until very recently, the data could not be reconciled in this system because regional officials had not consistently included the official in their distribution of findings reports.

- Second, NRC maintains, in addition to the information stored in RPS, a separate secure database – SLES – that holds inspection finding reports containing SGI data. OIG found that, for various reasons, this information is not easy to obtain or analyze and, in some cases, was not obtainable at all.

**Improved Data Collection and Analysis Will Enhance NRC's Ability To Regulate and Improve Program Operations, Program Tools and Procedures, and Program Results**

Despite the lack of trending across regions and fleets, OIG found no material adverse effect on NRC operations. However, NRC may miss opportunities to improve monitoring and management of security issues, inspection tools and procedures, and program results. Additionally, improved data management and analysis can help NRC staff identify trends that merit additional oversight or regulatory emphasis. This, in turn,

can give NRC greater assurance that the inspection program is meeting its objective to conduct fact-based assessments of licensee security program performance.

## **Recommendations**

OIG recommends that the Executive Director for Operations:

1.  Develop and maintain a centralized database of security findings data to be used for evaluating licensee performance trends, and communicating this information to NRC staff, industry, and appropriate public stakeholders.

2.  Formalize and implement a process for maintaining current and accurate data within a centralized database.

3.  Formalize and implement a process for ensuring SGI findings data is current and accessible for use in trending security findings issues.

**B.    NRC Lacks Consensus on Content and Application of SGI and Significance Screen Tools**

The ROP sets general standards for NRC's oversight of power reactors, and emphasizes objectivity, transparency, and consistency in NRC's assessments of licensee performance.  NRC staff and industry representatives expressed concern about the technical basis and application of the SGI and Significance Screen tools.[17]  Although NRC solicited staff comments in developing these assessment tools, NRC did not test draft versions of the tools and, further, does not have procedures for systematically reviewing SDP assessment tools on a periodic basis.  Staff consensus and understanding of SDP assessment tools is critical to ensuring that staff can apply these tools in accordance with ROP standards and avoid undue resource burdens on NRC and licensees.

**The ROP Emphasizes Transparent, Consistent Regulation**

The ROP sets general transparency and consistency standards for NRC's oversight of the nuclear power industry.  Specifically, NRC should aim for objective measurements of licensee performance and translate those measurements into timely assessments that the public and licensees can understand.  Moreover, NRC should respond to licensee violations in a consistent manner that reflects the potential safety impact of the violations.

**NRC Staff and Industry Concerns and Questions Focus on SGI and Significance Screen Assessment Tools**

Interviews and surveys of NRC staff and nuclear power industry representatives regarding the security SDP showed that two assessment tools—SGI and the Significance Screen—produced the greatest amount of critical feedback.  OIG received a broad range of comments regarding the content and application of these tools.  OIG also received suggestions about how to improve these assessment tools.  Additionally, some comments reflected a lack of understanding of assessment tool features, as well as doubts regarding the reliability of assessment results.

---

[17] See the "Background" section of this report for information on security SDP assessment tools.

OIG could not reconcile divergent staff and industry comments on the SGI and Significance Screen tools, yet several points stand out. First, some staff questioned the technical basis of criteria used to escalate findings. For example, both the SGI and Significance Screen rely on time standards to measure exploitability, but the rationale for these metrics was not clear to some NRC and industry personnel. Second, respondents questioned how these tools weigh mitigating information, and whether this information is analyzed after a finding has been prematurely escalated. Third, respondents questioned how some SGI and Significance Screen findings can be coded as White or Yellow when violations appear unlikely to impact plant safety or security. Lastly, some staff and industry personnel questioned the potential for escalation bias in the Significance Screen. The tool focuses on several particular security issues, and uses time and consequence criteria that increase the likelihood of White or Yellow findings.

**NRC Revises SDP Tools, but Does Not Systematically Test and Update Assessment Tools**

In reviewing the history of security SDP development, OIG found that NRC has tested other SDP tools prior to implementation but did not do so with the SGI and Significance Screen tools. NRC solicited staff and industry comments on draft tools, but did not test the draft tools by analyzing past or hypothetical findings to determine how the draft tools would work in a practical context. This differs from NRC's 2004 SDP pilot effort, during which headquarters and regional staff screened approximately 50 findings to determine whether the results would be reasonable. Similarly, NRC's current effort to update the Force-on-Force SDP involves a findings screening analysis.

OIG's review also showed that NRC updates SDP assessment tools on a circumstantial basis and does not have procedures to ensure that updates are performed consistently. The SGI and Significance Screen tools resulted from a 2007-2008 Enhancement Team effort that NRC initiated in response to staff concerns about particular security issues. Further, that Enhancement Team's leader has since retired from NRC, thereby limiting the institutional knowledge necessary to guide future SDP updates in the absence of formal procedures or best practice guidance.

**Consensus and Understanding of SDP tools Is Important for Regulatory Transparency**

Consensus and understanding among NRC staff regarding SDP assessment tools is critical to ensuring that staff can apply these tools easily and consistently in accordance with Reactor Oversight Process standards.  This does not preclude professional disagreement over particular findings.  However, staff must understand the rationale for findings so they can present them logically to licensees and uphold NRC's integrity as a fair and impartial regulator.  Further, NRC staff should have confidence in the soundness of escalated findings, given that the SDP requires extra staff resources for review and final disposition, and also impacts licensees with costs for responding to NRC and taking compensatory measures.[18]

**<u>Recommendations</u>**

OIG recommends that the Executive Director for Operations:

4.  Formalize and implement procedures for testing draft SDP tools by staff to determine how draft tools would screen past violations and/or hypothetical security violations.

5.  Formalize and implement a process for performing periodic review of existing security SDP tools to check for consistency of application and results.

---

[18] Greater-than-Green (e.g., White) findings can take between 5 and 18 months to close, depending on the complexity of each case.  Beyond the additional staff effort required to process these findings, licensees may need to conduct independent analysis to support their positions in enforcement conferences with NRC.  Further, licensees may be obligated to upgrade plant infrastructure at considerable cost if NRC maintains its position on an escalated finding.

## IV.    CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations:

1.  Develop and maintain a centralized database of security findings data to be used for evaluating licensee performance trends, and communicating this information to NRC staff, industry, and appropriate public stakeholders.

2.  Formalize and implement a process for maintaining current and accurate data within a centralized database.

3.  Formalize and implement a process for ensuring SGI findings data is current and accessible for use in trending security findings issues.

4.  Formalize and implement procedures for testing draft SDP tools by staff to determine how draft tools would screen past violations and/or hypothetical security violations.

5.  Formalize and implement a process for performing periodic review of existing security SDP tools to check for consistency of application and results.

# V.    AGENCY COMMENTS

At an exit conference on February 29, 2012, agency management provided informal comments on a draft of this report.  The Office of the Inspector General incorporated some of these comments into this report as appropriate.  As a result, the agency opted not to provide formal comments for inclusion in this report.

# POWER REACTOR SITES BY LICENSEE OPERATOR AND NRC REGION

| Licensee | Region 1 | Region 2 | Region 3 | Region 4 | Total |
|---|---|---|---|---|---|
| Ameren UE | | | | 1 | 1 |
| Arizona Public Service Co. | | | | 1 | 1 |
| Constellation Energy | 3 | | | | 3 |
| Detroit Edison Co. | | | 1 | | 1 |
| Dominion Generation | 1 | 2 | 1 | | 4 |
| Duke Energy Power Company, LLC | | 3 | | | 3 |
| Energy Northwest | | | | 1 | 1 |
| Entergy Nuclear Operations, Inc. | 4 | | 1 | 4 | 9 |
| Exelon Generation Co., LLC | 4 | | 6 | | 10 |
| FirstEnergy Nuclear Operating Co. | 1 | | 2 | | 3 |
| Florida Power & Light Co. | 1 | 2 | 1 | | 4 |
| FPL Energy Point Beach, LLC | | | 1 | | 1 |
| Indiana/Michigan Power Co. | | | 1 | | 1 |
| Nebraska Public Power District | | | | 1 | 1 |
| Nuclear Management Co. | | | 2 | | 2 |
| Omaha Public Power District | | | | 1 | 1 |
| Pacific Gas & Electric Co. | | | | 1 | 1 |
| PPL Susquehanna, LLC | 1 | | | | 1 |
| Progress Energy | | 4 | | | 4 |
| PSE&G Nuclear | 2 | | | | 2 |
| South Carolina Electric & Gas Co. | | 1 | | | 1 |
| Southern California Edison Co. | | | | 1 | 1 |
| Southern Nuclear Operating Co. | | 3 | | | 3 |
| STP Nuclear Operating Co. | | | | 1 | 1 |
| Tennessee Valley Authority | | 3 | | | 3 |
| TXU Generating Company LP | | | | 1 | 1 |
| Wolf Creek Nuclear Operating Corp. | | | | 1 | 1 |
| Total | 17 | 18 | 16 | 14 | 65 |

Source: OIG analysis of NRC data

# OBJECTIVE, SCOPE, AND METHODOLOGY

### OBJECTIVE

The audit objective was to evaluate NRC's management of the baseline security inspection program, including specific program features such as the Significance Determination Process.

### SCOPE

The audit focused on reviewing NRC's oversight of the baseline security inspection program and the Significance Determination Process. We conducted this performance audit at NRC headquarters and at the four NRC regions, from July 2011 through January 2012. Internal control and ROP principles related to the audit objective were reviewed and analyzed. Throughout the audit, auditors were aware of the possibility or existence of fraud, waste, or misuse in the program.

### METHODOLOGY

OIG reviewed relevant Federal regulations and internal guidance pertaining to NRC's regulatory authorities to oversee security inspections, including Chapter 10 Part 73 of the Code of Federal Regulations. OIG also reviewed NRC inspection manual chapters (IMC), NRC management directives (MD), and internal control guidance pertaining to the oversight of baseline security inspections including:

- IMC 0308 – Basis Document for Security Cornerstone of the Reactor Oversight Process.
- IMC 0609 Appendix E, Part I – Baseline Security Significance Determination Process for Power Reactors.
- MD 8.13 – Reactor Oversight Process.
- MD 8.7 – Reactor Operating Experience Program.
- MD 4.4 – Management Controls.
- Standards for Internal Control in the Federal Government.

OIG also reviewed inspection reports housed in ADAMS and SLES, performed an electronic survey of regional inspectors, and conducted interviews with headquarters personnel (Rockville, MD), regional

personnel, industry representatives, and the Nuclear Energy Institute. These interviews were conducted to obtain insights into NRC's oversight of baseline security inspections and the significance determination process. The audit team also observed inspection activities at Three Mile Island Nuclear Generating Station.

We conducted this performance audit 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 findings and conclusions based on our audit objective.

The audit work was conducted by Beth Serepca, Team Leader; Paul Rades, Audit Manager; Melissa Schermerhorn, Senior Management Analyst; John Tornabane, Management Analyst; and Kevin Nietmann, Senior Technical Advisor.