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

OFFICE OF THE
INSPECTOR GENERAL

November 12, 2015

MEMORANDUM TO: Victor McCree
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)

REFERENCE: DIRECTOR, OFFICE OF NUCLEAR SECURITY AND INCIDENT RESPONSE, MEMORANDUM DATED OCTOBER 29, 2015

Attached is the Office of the Inspector General's (OIG) analysis and status of the recommendations as discussed in the agency's response dated October 29, 2015. Based on this response, recommendations 1, 2, and 3 remain in resolved status. Recommendations 4 and 5 were closed previously. Please provide an updated status of the resolved recommendations by January 31, 2017.

If you have any questions or concerns, please call me at 415-5915 or Beth Serepca, Team Leader, at 415-5911.

Attachment: As stated

cc: Attachment: As stated

F. Brown, OEDO
J. Jolicoeur, OEDO
B. Pham, OEDO
J. Arildsen, OEDO
B. Holian, NSIR
EDO_ACS Distribution

Audit Report

AUDIT OF NRC'S PROTECTION OF SAFEGUARDS INFORMATION

OIG-12-A-12

Status of Recommendations

Recommendation 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.
Agency Response Dated October 29, 2015:	In response to Recommendation 1 from the Office of the Inspector General's (OIG's) audit of the NRC's Management of the Baseline Security Inspection Program (OIG-12-A-10), the Office of Nuclear Security and Incident Response (NSIR) assembled a working group with representatives from the Office of Nuclear Reactor Regulation (NRR), the Office of Information Services (OIS), and the Computer Security Office to assess various alternatives for a technologic solution for tracking security inspection findings in a secure environment. Based on group discussion and after analyzing the solution, NSIR agrees with OIS's and NRR's assessment to pursue a Reactor-Replacement Program System (RRPS)-based solution that encompasses specific NSIR requirements. NSIR has considered all viable solutions and considers this solution to be the most cost effective with no additional cost to NSIR and the agency. NSIR and NRR will continue to meet to ensure that NSIR requirements are accounted for as part of the RRPS development effort. RRPS is still in the development phase and is expected to be fully implemented in calendar year (CY) 2017. In addition, OIS and NSIR will maintain this path forward regarding any plan related to the upgrade of the Safeguards Information Local Area Network and Electronic Safe (SLES). NSIR considers this effort to effectively address the OIG recommendation to develop and maintain a centralized database of security findings data without introducing any additional technical or computer security risk.

Audit Report

AUDIT OF NRC'S PROTECTION OF SAFEGUARDS INFORMATION

OIG-12-A-12

Status of Recommendations

Recommendation 1 (cont.):

OIG Analysis:	The proposed corrective action addresses the intent of OIG's recommendation. OIG will close this recommendation when OIG staff has reviewed documentation of NSIR's data collection and analysis procedures, and has verified that the centralized security database functions as intended in accordance with Recommendation 1.
Status:	Resolved.

Audit Report

AUDIT OF NRC'S PROTECTION OF SAFEGUARDS INFORMATION

OIG-12-A-12

Status of Recommendations

Recommendation 2:	Formalize and implement a process for maintaining current and accurate data within a centralized database.
Agency Response Dated October 29, 2015:	NSIR is continuing to develop an office procedure to ensure that data from the security inspection reports is archived in a centralized database. NSIR expects to have an office procedure in place for tracking and trending security findings concurrent with the rollout and implementation of the new RRPS in CY 2017. This procedure will be finalized following the establishment of the recommended database(s).
OIG Analysis:	The proposed corrective action addresses the intent of OIG's recommendation. OIG will close this recommendation after OIG staff has reviewed NSIR's new office procedure for maintaining current and accurate security findings data in a centralized database and has verified implementation of this new guidance.
Status:	Resolved.

Audit Report

AUDIT OF NRC'S PROTECTION OF SAFEGUARDS INFORMATION

OIG-12-A-12

Status of Recommendations

Recommendation 3:	Formalize and implement a process for ensuring Safeguards Information (SGI) findings data is current and accessible for use in trending security findings issues.
Agency Response Dated October 29, 2015:	In response to Recommendation 3 from the OIG's audit of the NRC's Management of the Baseline Security Inspection Program (OIG-12-A-10), NSIR assembled a working group with representatives from NRR, OIS and the NSIR Cyber Security Directorate to assess various alternatives for a technologic solution for tracking security inspection findings in a secure environment. As discussed in the status of Recommendation 2, NSIR will develop an office procedure to ensure that SGI findings are categorized and archived into a centralized database in a manner consistent with the sensitivity designation of the information in conjunction with the rollout and implementation of RRPS occurring in CY 2017. It is important to note that the RRPS under development does not currently include the capability to protect and store SGI inspection data. Under the security baseline inspection program, 200-250 inspections are conducted annually with approximately 10-percent of those inspection results containing findings designated as SGI. As stated in Recommendation 1, the working group identified and evaluated the alternatives for the establishment of a secure database that would ensure the accessibility and usability of SGI findings data by the NRC staff. See Enclosure 2, "Analysis of Alternatives – Technology Solution for Tracking NSIR Inspection Findings," for more detailed information. NSIR will pursue Option 5, RRPS-based solution, with NSIR requirements partially incorporated into RRPS. This solution would add some of NSIR's requirements into RRPS, while continuing to store SGI information in SLES. RRPS development efforts will take into account any NSIR tracking

Recommendation 3 (cont.):

and trending requirement, and account for any minor business process difference. Inspection reports containing SGI will continue to be stored in SLES, and referenced by the associated document (i.e., NS) number in RPPS. This solution further leverages NRC's investment in RRPS at no additional cost to the agency and tracking and trending functions can be performed within RRPS, taking advantage of document and system security built into the platform. This option further assists the staff in reducing the manual tracking burden. The projected implementation date is scheduled to occur in CY 2017.

OIG Analysis: The proposed corrective action addresses the intent of OIG's recommendation. OIG will close this recommendation after OIG staff has verified that the NSIR office procedure referenced under Recommendation 2 contains instructions specific to SGI findings data and has confirmed implementation of this new office procedure in accordance with Recommendation 2.

Status: Resolved.