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

OFFICE OF THE
INSPECTOR GENERAL

April 7, 2010

The Honorable Darrell Issa
Ranking Member
Committee on Oversight and Government Reform
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, DC 20515-6143

Dear Representative Issa:

In response to your March 24, 2010, request for information on open audit recommendations, please find enclosed (1) a table of open audit recommendations at the U.S. Nuclear Regulatory Commission (NRC) and (2) a listing of the three most important open and unimplemented audit recommendations. The table shows that NRC is currently in the process of implementing 87 resolved audit recommendations and is considering actions to address 21 unresolved recommendations. The term resolved indicates that the agency has agreed with the audit recommendation and has proposed a course of action that my staff and I believe addresses the recommendation's intent. These recommendations will remain open until the agency completes its proposed course of action. Unresolved recommendations are those for which a course of action has yet to be agreed upon. All of the 21 unresolved recommendations listed at the end of the table are in this status because the agency is either still formulating its initial response to a recently issued audit report or OIG is analyzing the agency's first response. At this point, these 21 unresolved recommendations are not an issue.

In your March 24, 2010, letter, you also asked (1) about the current status of audit recommendations that were open at this time last year and (2) whether I have any suggestions for improving the Inspector General Act of 1978 or the Inspector General Reform Act. With regard to the first item, on April 29, 2009, I informed you that the agency was in the process of implementing 110 open audit recommendations. Of the 110 recommendations open at that time, 42 remain open and 68 are now closed. With regard to the second item, as a member of the Council of Inspectors General on Integrity and Efficiency (CIGIE) Legislation Committee, I fully endorse the consolidated input that you have received from the Committee. There is nothing unique to my office that warrants mention outside of that reporting mechanism.

Thank you for your strong support for the Inspector General mandate to prevent fraud, waste, and abuse. If you have questions, please contact me at 301-415-5930, or Stephen D. Dingbaum, Assistant Inspector General for Audits, at 301-415-5915

Sincerely,

Hubert T. Bell
Inspector General

Enclosures: As stated

Enclosure 1. NRC/OIG Open Audit Recommendations as of April 2, 2010				
Report # & Title	Short Title	Rec #	Status	Estimated $$ Benefit
OIG-01-A-03 Government Performance and Results Act: Review of the Fiscal Year 1999 Performance Report	Develop a Management Directive	1	Resolved	
OIG-01-A-03 Government Performance and Results Act: Review of the Fiscal Year 1999 Performance Report	Include guidance on reporting unmet goals	3	Resolved	
OIG-03-A-15 Audit of NRC's Regulatory Oversight of Special Nuclear Materials	Conduct periodic inspections	1	Resolved	
OIG-03-A-15 Audit of NRC's Regulatory Oversight of Special Nuclear Materials	Document risk informed approach	3	Resolved	
OIG-04-A-20 Audit of NRC's Incident Response Program	Conduct Periodic Reviews of Region's IRPs	4	Resolved	
OIG-05-A-09 Audit of the Budget Formulation Process	EDO, CFO Roles	1	Resolved	
OIG-05-A-09 Audit of the Budget Formulation Process	PRC Role	2	Resolved	
OIG-05-A-09 Audit of the Budget Formulation Process	Document Process	3	Resolved	
OIG-05-A-13 Audit of NRC's Telecommunications Program	Revise MD 2.3.	3	Resolved	
OIG-05-A-17 Audit of NRC's Decommissioning Program	Retain Supporting Documentation	1	Resolved	
OIG-05-A-18 Security Controls Over Personal Computers and Laptops - FISMA	Verify required security controls	3	Resolved	
OIG-05-A-18 Security Controls Over Personal Computers and Laptops - FISMA	Develop procedures for monitoring compliance with Executive Order 13103	6	Resolved	
OIG-06-A-24 Evaluation of NRC's Use of Probabilistic Risk Assessment In Regulating the Commercial Nuclear Power Industry	Full V&V for SAPHIRE and GEM	3	Resolved	
OIG-07-A-05 Audit of NRC's Technical Training Center	Rec. 01 - Revise MD 13.1	1	Resolved	
OIG-07-A-06 Audit of NRC's Regulation of Nuclear Fuel Cycle Facilities	Fuel Cycle Facility framework	1	Resolved	
OIG-07-A-14 Audit of NRC's Non-Capitalized Property	Rec. 07 Modify MD 13.1	7	Resolved	
OIG-07-A-14 Audit of NRC's Non-Capitalized Property	Rec. 11 Modify MD 13.1 to Notify AIGI	11	Resolved	
OIG-07-A-15 Audit of NRC's License Renewal Program	Establish backfit review process	7	Resolved	

OIG-07-A-18 Assessment of Security at NRC Buildings	Post signs directing pedestrian traffic	11	Resolved
OIG-07-A-19 Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year 2007	Develop and implement quality assurance procedures for POA&Ms.	11	Resolved
OIG-08-A-03 Audit of NRC's Alternative Dispute Resolution Program	Incorporate guidance in Enforcement Policy	2	Resolved
OIG-08-A-06 Memorandum Report: NRC's Planned Cybersecurity Program	Develop and implement plans for a cybersecurity oversight program	1	Resolved
OIG-08-A-10 Memorandum Report: Audit of NRC's Continuity of Operations Plan	Physical Security Survey Guidance	1	Resolved
OIG-08-A-11 Audit of NRC's Accounting and Control Over Time and Labor Reporting	Detailed System analysis	3	Resolved
OIG-08-A-11 Audit of NRC's Accounting and Control Over Time and Labor Reporting	Electronic Signatures	4	Resolved
OIG-08-A-13 Evaluation of NRC's Training and Development Program	New performance metrics	9	Resolved
OIG-08-A-16 Audit of NRC's Premium Class Travel	Update MD 14.1	1	Resolved
OIG-08-A-17 Audit of NRC's Enforcement Program	Develop guidance	1	Resolved
OIG-08-A-17 Audit of NRC's Enforcement Program	Define data collection requirements	2	Resolved
OIG-08-A-17 Audit of NRC's Enforcement Program	Develop QA process	3	Resolved
OIG-08-A-18 Independent Evaluation of NRC's Implementation of FISMA for FY 2008	Update the NRC System Information Control Database to identify all interfaces between systems	1	Resolved
OIG-08-A-18 Independent Evaluation of NRC's Implementation of FISMA for FY 2008	Develop procedures for NRC System Information Control Database	2	Resolved
OIG-08-A-18 Independent Evaluation of NRC's Implementation of FISMA for FY 2008	Develop process for verifying FDCC controls are implemented on all desktops/laptops	4	Resolved
OIG-08-A-19 Audit of NRC's Laptop Management	Develop a process for verifying security controls are implemented on agency laptops	4	Resolved
OIG-08-A-19 Audit of NRC's Laptop Management	Develop a protocol for updating agency laptops	5	Resolved
OIG-09-A-06 Audit of the Committee to Review Generic Communications	Develop agencywide backfit review process	1	Resolved

OIG-09-A-07 Audit of NRC's Occupant Emergency Program	Require annual, unannounced, full-scale evacuation drills	2	Resolved
OIG-09-A-07 Audit of NRC's Occupant Emergency Program	Update maps	10	Resolved
OIG-09-A-07 Audit of NRC's Occupant Emergency Program	Consistently place maps	11	Resolved
OIG-09-A-08 Audit of NRC's Agreement State Program	Develop an IMPEP self-assessment mechanism	1	Resolved
OIG-09-A-08 Audit of NRC's Agreement State Program	Develop guidance for identifying Agreement State information needed if State cannot perform its functions	2	Resolved
OIG-09-A-08 Audit of NRC's Agreement State Program	Develop standardized procedures for communicating to the Agreement States	3	Resolved
OIG-09-A-08 Audit of NRC's Agreement State Program	Develop a standardized data collection process as the basis of a national information sharing tool	4	Resolved
OIG-09-A-08 Audit of NRC's Agreement State Program	Revise IMPEP Procedures to include a review of events not recorded in NMED	5	Resolved
OIG-09-A-09 Audit of NRC's Warehouse Operations	Conduct security survey	2	Resolved
OIG-09-A-11 Information Systems Security Evaluation of the Technical Training Center	Complete hardening of badge access system	3	Resolved
OIG-09-A-11 Information Systems Security Evaluation of the Technical Training Center	Activate TTC's IDS	4	Resolved
OIG-09-A-11 Information Systems Security Evaluation of the Technical Training Center	Document backup implementation procedures	6	Resolved
OIG-09-A-13 Office of the Inspector General Information System Security Evaluation of Region II - Atlanta, GA	Document key management procedures.	1	Resolved
OIG-09-A-13 Office of the Inspector General Information System Security Evaluation of Region II - Atlanta, GA	Include the date combinations were last changed in the combination inventory.	2	Resolved
OIG-09-A-13 Office of the Inspector General Information System Security Evaluation of Region II - Atlanta, GA	Document combination management procedures.	3	Resolved
OIG-09-A-13 Office of the Inspector General Information System Security Evaluation of Region II - Atlanta, GA	Update documented backup procedures to reflect the actual backup procedures in place.	4	Resolved

OIG-09-A-13 Office of the Inspector General Information System Security Evaluation of Region II - Atlanta, GA	Develop and implement procedures to send backup info offsite.	5	Resolved
OIG-09-A-13 Office of the Inspector General Information System Security Evaluation of Region II - Atlanta, GA	Develop and document a contingency plan for the Region II seat-managed infrastructure servers.	6	Resolved
OIG-09-A-13 Office of the Inspector General Information System Security Evaluation of Region II - Atlanta, GA	Develop and document a contingency plan for the Region II NRC-managed servers.	7	Resolved
OIG-09-A-13 Office of the Inspector General Information System Security Evaluation of Region II - Atlanta, GA	Develop and document a contingency plan for the Region II badge access system server.	8	Resolved
OIG-09-A-13 Office of the Inspector General Information System Security Evaluation of Region II - Atlanta, GA	Evaluate vulnerabilities identified by the network vulnerability assessment, identify false positives, and resolve remaining vulnerabilities.	9	Resolved
OIG-09-A-13 Office of the Inspector General Information System Security Evaluation of Region II - Atlanta, GA	Perform a network vulnerability scan following remediation to verify all vulnerabilities have been resolved.	10	Resolved
OIG-09-A-14 Office of the Inspector General Information System Security Evaluation of Region IV - Arlington, TX	Develop and implement procedures for sending information system backup information to an offsite location.	1	Resolved
OIG-09-A-14 Office of the Inspector General Information System Security Evaluation of Region IV - Arlington, TX	Develop and document a contingency plan for the Region IV seat-managed infrastructure servers.	2	Resolved
OIG-09-A-14 Office of the Inspector General Information System Security Evaluation of Region IV - Arlington, TX	Develop and document a contingency plan for the Region IV NRC-managed servers.	3	Resolved
OIG-09-A-14 Office of the Inspector General Information System Security Evaluation of Region IV - Arlington, TX	Develop and document a contingency plan for the Region IV badge access system server.	4	Resolved
OIG-09-A-14 Office of the Inspector General Information System Security Evaluation of Region IV - Arlington, TX	Evaluate the vulnerabilities identified by the network vulnerability assessment, identify any false positives and resolve the remaining vulnerabilities.	5	Resolved

OIG-09-A-14 Office of the Inspector General Information System Security Evaluation of Region IV - Arlington, TX	Perform a network vulnerability scan following remediation to verify all vulnerabilities have been resolved.	6	Resolved
OIG-09-A-15 Office of the Inspector General Information System Security Evaluation of Region III - Lisle, IL	Develop and document a contingency plan for the Region III seat-managed infrastructure servers.	3	Resolved
OIG-09-A-15 Office of the Inspector General Information System Security Evaluation of Region III - Lisle, IL	Develop and document a contingency plan for the Region III NRC-managed servers.	4	Resolved
OIG-09-A-15 Office of the Inspector General Information System Security Evaluation of Region III - Lisle, IL	Evaluate the vulnerabilities identified by the network vulnerability assessment, identify any false positives and resolve the remaining vulnerabilities.	5	Resolved
OIG-09-A-15 Office of the Inspector General Information System Security Evaluation of Region III - Lisle, IL	Perform a network vulnerability scan following remediation to verify all vulnerabilities have been resolved.	6	Resolved
OIG-09-A-16 Audit of NRC's Grant Management Program	Resolve LSS Issues	1	Resolved
OIG-09-A-16 Audit of NRC's Grant Management Program	Update MD 11.6	2	Resolved
OIG-09-A-16 Audit of NRC's Grant Management Program	Interim Guidance	3	Resolved
OIG-09-A-16 Audit of NRC's Grant Management Program	Develop Training Program	4	Resolved
OIG-09-A-16 Audit of NRC's Grant Management Program	Trained Staff	5	Resolved
OIG-09-A-16 Audit of NRC's Grant Management Program	Tracking System	6	Resolved
OIG-09-A-16 Audit of NRC's Grant Management Program	QA on Files	8	Resolved
OIG-09-A-16 Audit of NRC's Grant Management Program	Issue regulation	9	Resolved
OIG-09-A-17 Audit of NRC's Oversight of Construction at Nuclear Facilities	Enhance CIP Guidance	1	Resolved
OIG-09-A-19 Audit of NRC's Material Control and Accounting Security Measures for Special Nuclear Materials at Fuel Cycle Facilities	Procedures	1	Resolved

OIG-09-A-19 Audit of NRC's Material Control and Accounting Security Measures for Special Nuclear Materials at Fuel Cycle Facilities	DOE Alternative	2	Resolved
OIG-09-A-20 Office of the Inspector General Information System Security Evaluation of Region I - King of Prussia, PA	Update the backup procedures found in the Region I Standard Operating Procedures for AIS Security.	1	Resolved
OIG-09-A-20 Office of the Inspector General Information System Security Evaluation of Region I - King of Prussia, PA	Develop and document a contingency plan for the Region I seat-managed infrastructure servers.	2	Resolved
OIG-09-A-20 Office of the Inspector General Information System Security Evaluation of Region I - King of Prussia, PA	Develop and document a contingency plan for the Region I NRC-managed servers.	3	Resolved
OIG-09-A-20 Office of the Inspector General Information System Security Evaluation of Region I - King of Prussia, PA	Evaluate the vulnerabilities identified by the network vulnerability assessment, identify any false positives and resolve the remaining vulnerabilities.	4	Resolved
OIG-09-A-20 Office of the Inspector General Information System Security Evaluation of Region I - King of Prussia, PA	Perform a network vulnerability scan following remediation to verify all vulnerabilities have been resolved.	5	Resolved
OIG-10-A-03 Audit of NRC's Management Directive 6.8, Lessons Learned Program	Develop and implement a strategy for communicating agencywide lessons learned and program activities to agency staff	1	Resolved
OIG-10-A-03 Audit of NRC's Management Directive 6.8, Lessons Learned Program	Implement the plan to release SPELL	2	Resolved
OIG-10-A-03 Audit of NRC's Management Directive 6.8, Lessons Learned Program	Re-affirm and communicate management's support for the program	3	Resolved
OIG-10-A-01 Audit of NRC's Physical Security Inspection Program for Category I Fuel Cycle Facilities	Security Training	1	Unresolved
OIG-10-A-01 Audit of NRC's Physical Security Inspection Program for Category I Fuel Cycle Facilities	Periodic Guidance Review	2	Unresolved
OIG-10-A-02 Audit of NRC's Quality Assurance Planning for New Reactors	Define QA review coordination requirements	1	Unresolved
OIG-10-A-02 Audit of NRC's Quality Assurance Planning for New Reactors	Develop a QA review process	2	Unresolved
OIG-10-A-02 Audit of NRC's Quality Assurance Planning for New Reactors	Determine impacts of document translation quality	3	Unresolved

OIG-10-A-02 Audit of NRC's Quality Assurance Planning for New Reactors	Incorporate assessment results of translation quality into oversight	4	Unresolved
OIG-10-A-04 Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2009	Interface Procedures	1	Unresolved
OIG-10-A-09 Audit of NRC's Personnel Security Clearance Program for Employees	Develop Reports	1	Unresolved
OIG-10-A-09 Audit of NRC's Personnel Security Clearance Program for Employees	Branch Chief Elements	2	Unresolved
OIG-10-A-09 Audit of NRC's Personnel Security Clearance Program for Employees	Deputy Director Elements	3	Unresolved
OIG-10-A-11 Social Engineering Assessment Report	Secure Coding Practices	1	Unresolved
OIG-10-A-11 Social Engineering Assessment Report	Malicious Activity	2	Unresolved
OIG-10-A-11 Social Engineering Assessment Report	Publicly Facing Information	3	Unresolved
OIG-10-A-11 Social Engineering Assessment Report	Authentication Controls	4	Unresolved
OIG-10-A-11 Social Engineering Assessment Report	Removable Storage	5	Unresolved
OIG-10-A-11 Social Engineering Assessment Report	NRC Network Access	6	Unresolved
OIG-10-A-11 Social Engineering Assessment Report	Malicious File Identification	7	Unresolved
OIG-10-A-11 Social Engineering Assessment Report	Security Training	8	Unresolved
OIG-10-A-11 Social Engineering Assessment Report	Security Announcement	9	Unresolved
OIG-10-A-11 Social Engineering Assessment Report	Training Assessment	10	Unresolved
OIG-10-A-11 Social Engineering Assessment Report	Visitor Policy	11	Unresolved
OIG-10-A-11 Social Engineering Assessment Report	Access Control	12	Unresolved

Enclosure 2. Three Most Important Open and Unimplemented NRC/OIG Recommendations

Date Issued	Audit Report	Recommendation	Status	Associated Cost Savings
5/26/03	Audit of NRC's Regulatory Oversight of Special Nuclear Materials (OIG-03-A-15)	Conduct periodic inspections to verify that material licensees comply with material control and accountability requirements, including, but not limited to, visual inspections of licensees' special nuclear material inventories and validation of report information.	NRC is making progress toward meeting the intent of this recommendation and anticipates compliance in 2012.	
9/26/06	Evaluation of NRC's Use of Probabilistic Risk Assessment in Regulating the Commercial Nuclear Power Industry (OIG-06-A-24)	Conduct a full verification and validation of SAPHIRE version 7.2 and GEM.	Several months after report was issued, OIG and NRC agreed that verification and validation of SAPHIRE version 8 would meet the intent of this recommendation. Implementation of version 8 is scheduled to occur this year.	
9/6/07	Audit of NRC's License Renewal Program (OIG-07-A-15)	Establish a review process to determine whether or not Interim Staff Guidance meets the provisions of 10 CFR 54.37(b), and document accordingly.	NRC is making progress toward meeting the intent of this recommendation. Initial actions toward compliance necessitated additional actions. A status update from NRC is due this month.	