AUDIT REPORT

Audit of NRC's Information Technology Governance

OIG-14-A-04-December 9, 2013

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

December 9, 2013

MEMORANDUM TO: Mark A. Satorius
Executive Director for Operations

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

SUBJECT: AUDIT OF NRC'S INFORMATION TECHNOLOGY GOVERNANCE (OIG-14-A-04)

Attached is the Office of the Inspector General's (OIG) audit report titled *Audit of NRC's Information Technology Governance.*

The report presents the results of the subject audit. Following the November 22, 2013, exit conference, agency staff indicated that they had no formal comments for inclusion in 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

EXECUTIVE SUMMARY

BACKGROUND

Information technology (IT) governance is the leadership, structures, and processes that ensure that an organization's IT sustains and extends the organization's strategies and objectives. Its overall objective is to ensure that the organization can sustain its operations and implement strategies required to meet future objectives using IT. IT governance is necessary to manage information and employ IT to improve the productivity, effectiveness, and efficiency of agency programs.

OBJECTIVE

The audit objective was to assess the effectiveness of the Nuclear Regulatory Commission's (NRC) IT governance structure in meeting the agency's current and future IT needs.

RESULTS IN BRIEF

NRC's IT governance is not fully meeting stakeholder needs. Federal guidance states that proper guidance documentation and communication are important factors in the success of agency programs. However, NRC's IT governance framework and processes have not been effectively documented and communicated. The Office of the Inspector General found that the most prevailing issue area that stakeholders communicated was a general lack of confidence in the Office of Information Services' (OIS) ability to deliver an acceptable level of customer service. Additionally, confusion surrounding reassignment of OIS staff roles exists. As a result, NRC may not be able to fully meet the agency's future IT needs.

RECOMMENDATIONS

This report makes four recommendations to improve the effectiveness of NRC's IT governance structure in meeting the agency's future IT needs.

AGENCY COMMENTS

An exit conference was held with the agency on November 22, 2013. Prior to this meeting, after reviewing a discussion draft, agency management provided supplemental information that has been incorporated into this report, as appropriate. As a result, agency management stated their general agreement with the findings and recommendations in this report and opted not to provide formal comments for inclusion in this report.

ABBREVIATIONS AND ACRONYMS

CIO	Chief Information Officer
CONOPS	OIS Reorganization Concept of Operations
IPEC	Information Technology/Information Management Portfolio Executive Council
IT	Information Technology
ITB	Information Technology/Information Management Board
NRC	Nuclear Regulatory Commission
OMB	Office of Management and Budget
OIG	Office of the Inspector General
OIS	Office of Information Services

TABLE OF CONTENTS

I. BACKGROUND

Information technology (IT) governance is the leadership, structures, and processes that ensure that an organization's IT sustains and extends the organization's strategies and objectives. Its overall objective is to ensure that the organization can sustain its operations and implement strategies required to meet future objectives using IT. The increasing use of technology has created a critical dependency on IT that requires a specific focus on governance. Accordingly, IT governance is necessary to manage information and employ IT to improve the productivity, effectiveness, and efficiency of agency programs.

Federal Guidance

The Clinger-Cohen Act of 1996 was designed to improve the way the Federal Government invests in IT. Since this law was enacted, the Chief Information Officers (CIO) in Federal organizations have been assigned primary responsibility for the management of Federal IT investments. This includes specific procedural and policy-related responsibilities such as capital planning, security, and enterprise architecture, as well as activities for shaping the information culture of the agency such as leadership and management.

In December 2010, the Office of Management and Budget (OMB) issued its *25 Point Implementation Plan to Reform Federal Information Technology Management*, outlining activities to reform IT management throughout the Federal Government.[1] The plan recommends more effective management of large-scale IT programs by streamlining governance and improving accountability. According to the plan, this involves reforming and strengthening investment review boards to enable them to more adequately manage agency portfolios, redefining the role of

[1] In January 2013, the Nuclear Regulatory Commission's (NRC) Office of the Inspector General (OIG) issued audit report OIG-13-A-09, *Audit of NRC's Progress in Carrying Out the 25 Point Implementation Plan to Reform Federal Information Technology Management*. This report is publicly available in the NRC Agencywide Documents Access and Management System; see accession number ML13023A105.

agency CIOs to focus on portfolio management, and rolling out face-to-face, evidence-based reviews of agency IT programs.

In a 2011 memorandum,[2] OMB reiterated the need for CIOs to focus "on delivering IT solutions that support the mission and business effectiveness of their agencies and overcome bureaucratic impediments to deliver enterprise-wide solutions." One of the four areas singled out for increased attention was IT governance. The memorandum highlighted the role of the CIO to drive the investment review process and to have responsibility over the entire IT portfolio for an agency. The memorandum also stated that CIOs must work with Chief Financial Officers and Chief Acquisition Officers to ensure portfolio analysis is an integral part of the yearly budget process for an agency.

NRC Guidance

NRC's primary internal guidance for IT governance is Management Directive 2.8, *Project Management Methodology (PMM)*. The directive identifies this methodology as the only approved methodology for IT investment management. This methodology facilitates effective selection, approval, management, oversight, reporting, and documentation of IT investments throughout their entire life cycle. This directive defines the major components of the methodology and assists NRC offices in locating more detailed information necessary to implement and use this methodology for managing IT investments.

NRC IT Organizational Structure

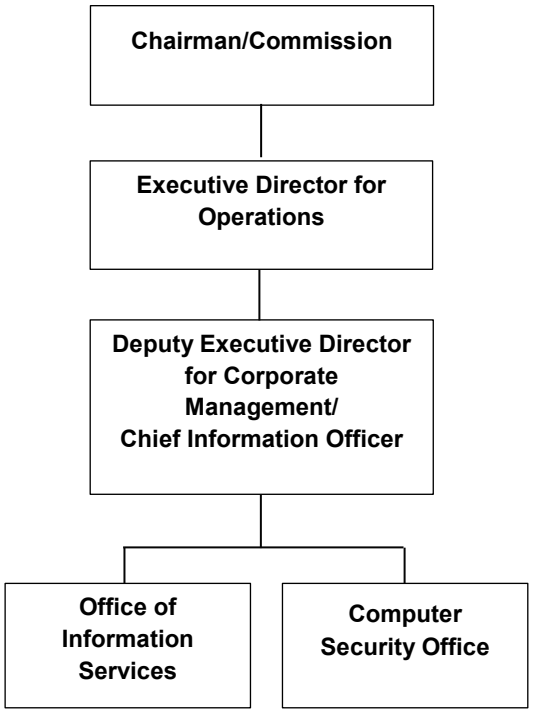
NRC's Deputy Executive Director for Corporate Management also serves as the agency's CIO. The CIO oversees NRC's agencywide Information Technology/Information Management program, and reports directly to NRC's Executive Director for Operations.

The Office of Information Services (OIS) and the Computer Security Office report to the CIO. OIS is the primary office responsible for implementing NRC's IT governance. The office manages and operates the agency's IT infrastructure, provides information and records services, and coordinates

[2] OMB Memorandum M-11-29, *Chief Information Officer Authorities*, August 8, 2011.

programs to assist with the development and maintenance of NRC's business applications. OIS also manages the agency's IT strategic planning, capital planning, and enterprise architecture activities. The Computer Security Office oversees the agency's IT security program, including policy, training, and authorization of IT systems. Figure 1 shows NRC's IT organizational structure.

Figure 1: NRC IT Organizational Structure



Source: OIG

IT Governance at NRC

In January 2012, NRC's CIO and Chief Financial Officer announced a plan to streamline and optimize the IT governance process. The plan included:

- Replacing the Information Technology Senior Advisory Council with a new Information Technology/Information Management Portfolio Executive Council (IPEC) consisting primarily of NRC office directors.

- Replacing the Information Technology Business Council with the Information Technology/Information Management Board (ITB), which is an expanded version of the council that currently reviews IT changes.

The IPEC is an executive management body established to determine NRC IT strategic direction and to manage the agency's IT portfolio. The IPEC sets current fiscal year priorities and determines the funding of IT investments that integrate into the IT portfolio. The IPEC is co-chaired by the CIO and Chief Financial Officer and consists of nine voting members and seven advisory members. Its voting members consist primarily of office directors from major NRC offices.

The ITB reports to the IPEC and is a review body established to review and recommend changes to the agency's IT architecture, including the portfolio of IT systems, technologies, and standards. The ITB's goal is to help align IT investments and technology standards with NRC's mission and ensure that the investments are made according to agency priorities. The ITB reviews new proposals and current IT investments, alignment with strategic direction, ability to integrate into NRC's IT architecture, conformance with technology standards, and potential risks to NRC's IT environment. Its members are office branch chiefs from the majority of NRC program and regional offices, including several representatives from OIS.

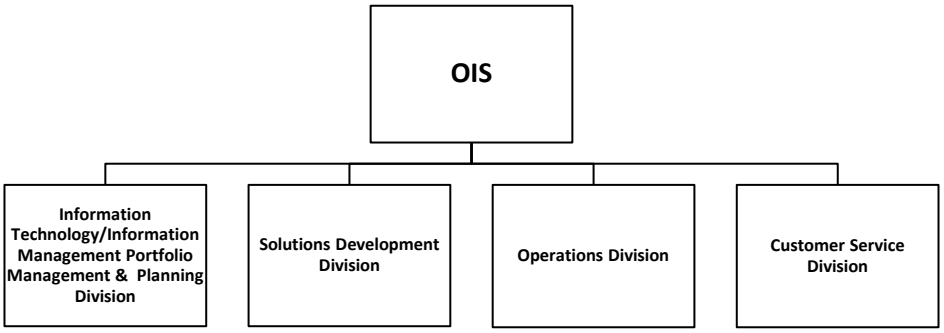
OIS Reorganization

In April 2013, OIS initiated an office-wide reorganization. There were several reasons provided by OIS for the reorganization, namely:

- The desire to become a more customer-centric organization.
- Continued pressures to contain the IT budget.
- Increased reliance on IT to accomplish NRC business.
- A rapidly evolving IT environment.
- The requirement to meet external mandates from oversight agencies.

OIS had traditionally focused on infrastructure services and managing delivery of its technology products and services; however, industry guidance suggests a more holistic approach to managing services from end-to-end. Managing the entire business service along with its underlying components would more likely assure that OIS delivers the required functionality and service levels to its stakeholders. The new structure is intended to focus on service functions, improve outreach and customer services, develop an enterprise-level approach, and establish an overall sense of continuity. Figure 2 illustrates OIS' new organizational structure as of April 2013.

Figure 2: OIS Organizational Structure



Source: OIG

To provide direction and guidance, OIS created the OIS Reorganization Concept of Operations (CONOPS). The purpose of the CONOPS document is to help OIS staff understand the reorganization and achieve desired results. The CONOPS provides guidance and a basic framework to assist OIS staff in understanding their roles and responsibilities and how the new organization works.

II. OBJECTIVE

The audit objective was to assess the effectiveness of NRC's IT governance structure in meeting the agency's current and future IT needs. The report appendix contains information on the audit scope and methodology.

III. FINDING

NRC's IT Governance Could Be Improved

NRC's IT governance is not fully meeting stakeholder needs. Federal guidance states that proper guidance documentation and communication are important factors in the success of agency programs. However, NRC's IT governance framework and processes have not been effectively documented and communicated. As a result, NRC may not be able to fully meet the agency's future IT needs.

Requirements for Effective IT Governance

Documentation and communication are important factors in the success of agency programs. Federal standards require agency processes to be clearly documented and communicated. In implementing these standards, management is responsible for developing internal controls – such as detailed agency guidance, policies, procedures, and practices – to fit their agency's operations and help staff understand and carry out their responsibilities.

Documentation Is Required

Guidance documents help ensure that management's directives are carried out. The U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government*[3] requires clearly documenting processes at an appropriate level of detail to allow management to effectively monitor the activity. The documentation must be properly managed, maintained, and made available in order to meet its intended

[3] GAO/AIMD-00-21.3.1, November 1999.

purpose. In addition, OMB recognizes the value of clearly documenting agency guidance. OMB maintains that well-designed guidance documents, if used properly, can appropriately direct agency employees and increase efficiency.

Communication Is Required

Relevant, reliable, and timely communication is required to control operations and achieve objectives. Information should be communicated to those who need it, and within a timeframe that enables them to carry out their responsibilities. Effective communication should occur in a broad sense with information flowing down, across, and up the organization. In addition, management should ensure there are adequate means of communicating with, and obtaining information from, external stakeholders that may have a significant impact on the agency achieving its goals.

Stakeholder Needs Not Being Met

NRC's IT governance is not fully meeting stakeholder[4] needs. During this audit, OIG interviewed 42 of NRC's management and staff, many of whom expressed concerns with several areas of NRC's IT governance process.

For example:

- Lack of confidence in OIS' ability to deliver an acceptable level of customer service.
- Effectiveness of the IPEC and ITB.
- Customer Service Division is incomplete.
- Milestones are incomplete or undocumented.
- Confusion surrounding reassignment of OIS staff roles.

Lack of Confidence in OIS' Ability to Deliver an Acceptable Level of Customer Service

Perhaps the most prevailing issue area that stakeholders communicated was a general lack of confidence in OIS. OIG interviewed NRC employees from program and regional offices who have worked with OIS

[4] For the purpose of this audit, the term "stakeholders" refers to all OIS customers, such as NRC program and regional offices.

on IT projects. Many stakeholders expressed concerns over OIS' inability to deliver acceptable customer service.

A common theme was that stakeholders did not trust OIS to meet NRC's IT needs based on their previous experiences. Some of the responses included:

- OIS needing to be more customer-focused.
- OIS not understanding program offices' type of work or systems.
- OIS not having the capacity to do the job.
- OIS being more of a regulator and adding extra burdens to program offices.
- Some offices seek IT solutions from OIS only to end up doing the work themselves.

Due to this lack of confidence, some stakeholders within NRC have circumvented OIS and the IT governance process and have created their own systems, also known as "shadow IT" systems.[5]

Effectiveness of the IPEC and ITB

Stakeholders interviewed widely praised the IPEC and ITB as a step in the right direction and a significant improvement over their predecessors. However, both entities have come under some criticism as some question their effectiveness.

IPEC and ITB Working Relationships

Some stakeholders criticized the working relationship between the IPEC and ITB. The IPEC, as a steering committee composed of office directors and division directors, is supposed to make strategic decisions after they are given alternatives resulting from the ITB's research on the technical issues. However, there were instances where IPEC members found that business cases and topics discussed were far more technical and detail-

[5] Shadow IT is hardware or software within an enterprise that is not supported by the organization's central IT department. The term often carries a negative connotation because it implies that the IT department has not approved the technology or does not even know employees are using it. Shadow IT can introduce security risks when unsupported hardware and software are not subject to the same security measures that are applied to supported technologies.

oriented than they anticipated. An IPEC member believed the ITB needed to simplify its presentations so the IPEC could more easily make executive decisions. Additionally, an ITB member was concerned that the ITB was not making any hard decisions.

On the other hand, another IPEC member believed that some IPEC members were not fully engaged with the IT governance process. The IPEC member remarked that business leads must take ownership of their systems. An ITB member opined that the IPEC should be more involved with searching for IT solutions rather than just administratively processing transactions. An OIS manager expressed concern that IPEC members sometimes send their deputies to attend IPEC meetings and these deputies are typically not as familiar with the other systems outside of their area or business line.

ITB Composition

Stakeholders also commented on the ITB's composition and scope. The ITB consists of 18 members covering a majority of NRC's program offices and each regional office. An ITB member opined that the scope was "out of control with too many fingers in the pie." Another ITB member intimated that some of the other ITB members may not be qualified. Finally, a different ITB member asserted that only individuals from the Office of Administration, the Computer Security Office, and OIS should compose the ITB. In contrast, there were several members who expressed that their regional or program office deserved an equal voice and did not want membership restricted.[6]

Approval Timeliness

According to stakeholders, another issue involving both the IPEC and ITB is how long it takes to get any IT system or software approved. There is currently no timetable or limit as to how long a decision may take. A program office manager claimed that some staff believe that it takes too long to get through the IT governance process. An NRC regional office

[6] OIG was recently informed that the ITB was in the midst of a transition that would divide the group into two parts: the ITB itself and a new architectural council. The ITB will focus on business needs while the architectural council will focus on technological issues and consist solely of members from OIS and the Computer Security Office.

manager said that speed is essential, and waiting 6 to 8 weeks for a decision from OIS is unacceptable. Another manager indicated that the approval process can be burdensome because it takes too much time. The manager believed the ITB had the right intentions, but can act as a restraint as his staff is always asking how long it will take for OIS to do something. An OIS staff member admitted that these decisions can take time, confirming that the IT approval process is slow and it can take a few weeks to go through all of the steps.

It should be noted that the ITB and IPEC member responsibilities are collateral duties and are added to the existing workloads of the members' primary jobs. One ITB member opined that members of the ITB do not have enough time for full integration and sequencing of their activities necessary to support the approval and control process. With his numerous roles in connection with the ITB, he does not have much time to focus on everything in addition to all of his regular responsibilities.

Customer Service Division Is Incomplete

As stated earlier, one of the driving forces behind the OIS reorganization was the desire to have OIS become more customer focused. During the reorganization in April 2013, OIS realigned its IT/IM services within four divisions, with an emphasis on the Customer Service Division. However, as of August 2013, the Customer Service Division was the only division that still had several vacant managerial positions. It is anticipated that the OIS reorganization will not be fully complete until the second quarter of 2014 due to OIS' implementation of its new customer service strategy.

Milestones Are Incomplete or Undocumented

Progress toward some reorganization plan milestones is behind schedule and other milestones are undocumented. For example, in the OIS reorganization Implementation Plan, the development and revision of position descriptions was scheduled for completion in May 2013, but has not been completed. In addition, the OIS reorganization Communication Plan does not document whether any tasks have been completed.

Confusion Surrounding Reassignment of OIS Staff Roles

One of the major challenges OIS faced when going through its recent reorganization was reassigning roles and responsibilities to numerous staff. The reorganization created some confusion – not only among stakeholders – but also among OIS staff regarding past and current responsibilities. During the early stages of the reorganization, an OIS manager claimed that very few OIS staff had transitioned to their new roles as the reorganization was an ongoing process. The manager said staff needed to figure out their new roles, what old work they were taking with them, and who they were transferring their old work to. Another OIS manager admitted that some of the IT functions were not picked up as part of the new structure and therefore may have been overlooked. This may have resulted in higher workloads and stress levels on some OIS managers and staff. Finally, an Office of Administration manager remarked that work was moving from person to person, apparently leading to some short-term confusion. Some OIS personnel were not sure what they were supposed to be doing because some of the decisions regarding the reorganization had yet to be made. Meanwhile, some stakeholders stated that they were not sure who to speak with in OIS since people have changed positions and new divisions have been created.

OIS Is Making Improvements

While there has been some dissatisfaction from stakeholders, several have also responded that they are quite satisfied with OIS and that things are much improved from the past. Further, OIS recognized that improvements were needed and therefore assisted in creating the IPEC and ITB. In addition, OIS initiated its internal reorganization with a major focus on improving customer service.

Framework and Processes Not Effectively Documented or Communicated

The documentation of NRC's IT governance framework and processes is not comprehensive and has not been effectively communicated to its stakeholders. For example OIG found:

- Governance charters lack specificity.
- Management Directive 2.8 is outdated.
- The CONOPS is incomplete.
- An overall lack of effective communication.

Framework and Processes Not Effectively Documented

Governance Charters Lack Specificity

The IPEC and ITB charters lack specific details on IT governance processes. The charters are neither thorough nor specific enough to achieve their intended purposes. The groups' charters seek to align IT investments with NRC's business objectives; however, the charters do not mention how to achieve this intended purpose. For example, the charters do not include information such as:

- A minimum threshold for which ITB/IPEC approval may not be needed.
- A format for presenting IT cases.
- A format for evaluating and approving IT cases.
- Timelines and standards for making decisions and delivering services.
- A process for communicating IPEC decisions to program offices or other interested parties.
- A process for following up after a system is implemented.
- A process for measuring the success of IPEC and ITB decisions.

An ITB member from a regional office talked about a specific IT issue his office was facing and said he was not sure if this issue fit the ITB charter.

Additionally, when asked how the success of their final decisions is measured, some IPEC members said that they either did not know or did not believe they had a formal way of doing this.

Management Directive 2.8 Is Outdated

Management Directive 2.8, *Project Management Methodology (PMM)*, is the sole guidance used for the IT investment management process, yet is more than 6 years old and incomplete. NRC's policy is to ensure that IT

investments are planned, built, selected, managed, and evaluated to maximize the value and minimize the risks of those investments in accordance with Federal statutes and regulations. However, the directive does not address how IT aligns with the agency's objectives, and does not even use or define the term "IT governance." Furthermore, NRC's Project Management Methodology Web page depicts an older IT governance structure.

The Concept of Operations (CONOPS) Is Incomplete

The CONOPS provides guidance and a basic framework to assist OIS staff in understanding their roles and responsibilities and how the new OIS organization works; however, the CONOPS is still in draft and is incomplete. Stakeholder interviews describe a lack of clarity for who in OIS is responsible for what. Based on OIG's review, there is no indication as to how OIS tracks and documents the evolving nature of the OIS organization and its effect on operations and the CONOPS framework. There is also no indication of how OIS is tracking and measuring the expected benefits of the reorganization.

According to industry best practices, when implementing an IT governance framework, it is important to evaluate the implementation efforts by developing measures to assess progress in meeting objectives. Lessons learned and recommendations for improving the investment process should be developed, documented, and distributed to all stakeholders.

Framework and Processes Not Effectively Communicated

The IT governance framework and processes have not been effectively communicated to stakeholders. OIS management has not communicated the requirements of the ITB/IPEC evaluation and approval process, including details of individual roles and responsibilities, service followup, project tracking, and matrices to measure the success of its decisions that directly affect program and regional offices. This has resulted in a lack of stakeholder buy-in. According to industry best practices, to effectively implement a new IT governance framework, organizations should obtain buy-in by involving all key stakeholders to ensure key perspectives are considered and facilitate adoption. Taking these steps increases the

likelihood that the new IT governance process will be adopted despite the significant cultural change it represents. An OIS manager stated that OIS had openly communicated the upcoming reorganizational changes to stakeholders, but did not believe OIS was necessarily required to obtain buy-in from stakeholders.

It should be noted that OIS management provided OIG an Implementation Plan and a Communications Plan concerning the office's reorganization. OIS also sought feedback from its staff prior to the reorganization by conducting several meetings and sending out emails and surveys asking for staff comments. While OIS took these positive steps, OIG found that some confusion still existed among stakeholders and OIS staff and that the information provided by OIS may not have been communicated effectively. For example, in addition to stakeholders' issues previously mentioned in this report, OIS employees exhibited some contradictions displaying a lack of effective communication. For instance:

- One OIS employee stated that the OIS reorganization was fully operational, another said it would be fully operational by October 2013, and another said it would be fully operational in 2nd quarter of 2014.
- One OIS employee said that people were still transitioning and trying to figure out their new roles, while another OIS employee said that OIS staff had been settled in their roles for quite some time.
- An ITB member questioned why even small program office purchases must go through the ITB, while an IPEC member countered that program offices can purchase whatever they want as long as they have the money for it.

Agency's IT Needs May Not Be Met

NRC may not be able to fully meet the agency's future IT needs without comprehensive and communicated documentation of NRC's IT governance framework and processes. Specifically, there is a lack of assurance that IT services and management can be adequately provided to the agency. Some stakeholders believe that OIS has not provided sufficient customer service and have yet to be convinced that OIS can be counted upon to deliver an acceptable level of service. As a result, some

stakeholders have been circumventing OIS and the governance process by approving or creating their own shadow IT systems. This, in turn, creates a less effective IT governance process which may result in possible IT security breaches, compliance issues, and investment waste.

Recommendations

OIG recommends that the Executive Director for Operations:

1. Revise the IPEC and ITB charters to more clearly define:
    - Roles and responsibilities.
    - The evaluation, approval, and decision followup process.

2. Revise NRC Management Directive 2.8 to include:
    - Current IT governance stakeholder requirements.
    - A definition of IT governance, structure, and processes.

3. Update and finalize the CONOPS to be consistent with current practice, including a schedule for full implementation.

4. Develop and implement a comprehensive IT governance communication strategy that:
    - Promotes buy-in from regional and program office stakeholders by requesting feedback.
    - Clearly explains policies and procedures of the IPEC and ITB charters, as well as the CONOPS, to all stakeholders.
    - Provides easily retrievable access to the updated charters and CONOPS.

IV. AGENCY COMMENTS

An exit conference was held with the agency on November 22, 2013. Prior to this meeting, after reviewing a discussion draft, agency management provided supplemental information that has been incorporated into this report, as appropriate. As a result, agency management stated their general agreement with the findings and recommendations in this report and opted not to provide formal comments for inclusion in this report.

Appendix

OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

The audit objective was to assess the effectiveness of NRC's IT governance structure in meeting the agency's current and future IT needs.

SCOPE

The audit reviewed NRC's activities related to IT governance with special emphasis on framework and processes. OIG conducted this performance audit from March 2013 through October 2013 at NRC headquarters in Rockville, MD. Internal controls 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

To address the audit objective, OIG auditors interviewed 42 NRC managers and staff. Furthermore, OIG reviewed Federal and internal agency guidance, including:

- *Standards for Internal Control in the Federal Government.*
- Clinger-Cohen Act of 1996.
- Paperwork Reduction Act of 1995.
- E-Government Act of 2002.
- *25 Point Implementation Plan to Reform Federal Information Technology Management.*
- OMB Memorandum M-11-29, *Chief Information Officer Authorities.*
- NRC Management Directive 2.6, *Information Technology Infrastructure.*
- NRC Management Directive 2.8, *Project Management Methodology (PMM).*

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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

The audit was conducted by Beth Serepca, Team Leader; Robert Woodward, Audit Manager; Michael Blair, Senior Analyst; Ziad Buhaissi, Senior Auditor; and Neil Doherty, Senior Analyst.