U.S. Department of Energy

Office of Inspector General

Office of Audits and Inspections

AUDIT REPORT

The Department of Energy's Implementation of Voice over Internet Protocol Telecommunications Networks

DOE/IG-0915

June 2014

Department of Energy
Washington, DC 20585

June 26, 2014

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "The Department of Energy's Implementation of Voice over Internet Protocol Telecommunications Networks"

BACKGROUND

Advancements in the telecommunications industry have created the ability to consolidate resources and minimize the continued environmental impact of maintaining facilities to sustain lines of communication. For example, the use of Voice over Internet Protocol (VoIP) allows the transmission of voice communications primarily over the internet and reduces reliance on the public switched telephone networks that have historically been used. According to various industry authorities, the ability to transfer data and voice over a single network can reduce operating costs associated with traditional communications networks that separated data and voice because organizations no longer need to manage and support two networks. Additional savings can be realized through consolidation of larger, traditional landline systems because VoIP networks are not bound by geographic limitations. As such, high capacity networks can be deployed and provide telecommunications services to users in other areas or regions, potentially eliminating a significant portion of long distance charges.

The Department of Energy initiated and/or completed implementation of VoIP networks at more than 14 locations at a cost of over $56 million. While this technology potentially provides many benefits, it also presents additional security risks. The most serious threat to VoIP systems is an attack that results in massive increases in network traffic that can render a system inoperable. Because of the number of ongoing VoIP efforts and substantial costs involved, we initiated this audit to determine whether the Department planned and implemented its VoIP telecommunications networks in an efficient and secure manner.

RESULTS OF AUDIT

Our review identified opportunities to improve the efficiency and enhance cybersecurity of the Department's VoIP networks. In particular, we found:

- When upgrading aging telecommunications systems, programs and sites had undertaken a number of separate VoIP network implementations, a practice that potentially resulted in duplicative capabilities. For example, four sites at the Oak Ridge Reservation independently implemented separate VoIP networks or had performed pilot projects to

implement new networks. In addition, we observed planning and coordination weaknesses at Headquarters, the Hanford Site and the Pacific Northwest National Laboratory.

- Programs and sites had not always applied required cybersecurity controls to VoIP networks, thus increasing the risk of compromise. Contrary to Federal requirements, seven of the nine sites we reviewed had conducted limited or no vulnerability scanning and penetration testing on installed VoIP systems. We also identified weaknesses related to incomplete and/or untested contingency plans and failure to conduct or document the completion of periodic security control assessments.

The issues identified occurred, in part, because the Department had not developed and implemented a coordinated approach to support the implementation of VoIP efforts. Had the Department done so, the number of separate efforts undertaken likely could have been reduced and more effectively managed. We found that coordination between programs and sites that were implementing VoIP systems could have potentially decreased the more than $56 million in estimated implementation costs. For instance, programs and sites could have worked with one another to ensure that common VoIP resources such as hardware, support services and licensing costs were shared, as appropriate. The Department also had not adequately monitored the implementation of cybersecurity controls for VoIP systems. As an example, site office officials had not performed assessments of contractor VoIP network security at most of the sites reviewed.

Without improvements, the duplicative and fragmented VoIP implementation approach that we identified could continue unabated and result in additional, unnecessary expenditures of resources at programs and/or sites that have not yet upgraded to VoIP systems. In addition, the Pacific Northwest National Laboratory spent approximately $1 million to implement a system without adequately considering alternatives, a decision which ultimately resulted in additional expenditures. Furthermore, the Department's information systems and networks will be at increased risk of compromise if cybersecurity controls are not appropriately identified and implemented.

Notably, many of the programs and sites reviewed had proactively acknowledged that existing telecommunications systems such as older hard-wired phone systems were nearing end-of-life and were in need of upgrade to continue to meet mission needs. We acknowledge that upgrading to a VoIP solution is likely to improve the Department's telecommunications infrastructure. However, the path the Department is on is not fiscally sustainable or efficient.

As such, we made serveral recommendations designed to address the issues outlined in our report. We recognize that there are many nuances related to the Department's organizational structure involving Federal and contractor elements that need to be considered. We believe, however, that improvements are possible and that our recommendations, if fully implemented, should help the Department manage the implementation of this technology in a more efficient and secure manner.

MANAGEMENT REACTION

Management concurred with the report's recommendations and indicated that corrective actions had been taken related to the Department's ongoing VoIP efforts. Our review of management's

technical comments identified that additional work is necessary. Management's formal comments are included in Appendix 3.

Attachment

cc: Deputy Secretary
Under Secretary for Nuclear Security
Deputy Under Secretary for Science and Energy
Deputy Under Secretary for Management and Performance
Chief of Staff
Chief Information Officer

AUDIT REPORT ON THE DEPARTMENT OF ENERGY'S IMPLEMENTATION OF VOICE OVER INTERNET PROTOCOL TELECOMMUNICATIONS NETWORKS

TABLE OF CONTENTS

Audit Report

Appendices

THE DEPARTMENT OF ENERGY'S IMPLEMENTATION OF VOICE OVER INTERNET PROTOCOL TELECOMMUNICATIONS NETWORKS

DETAILS OF FINDING

The Department of Energy (Department) had not always planned and managed its implementation of Voice over Internet Protocol (VoIP) telecommunications networks in an efficient and secure manner. In particular, the Department had undertaken separate, potentially duplicative implementations of VoIP networks. Furthermore, cybersecurity controls intended to protect VoIP networks were not always appropriately implemented at all programs and sites reviewed.

VoIP Implementation

When upgrading aging telecommunications systems, the Department deployed separate, potentially duplicative VoIP networks. At the time of our audit, more than 14 locations had initiated and/or completed separate VoIP efforts costing in excess of $56 million for the acquisition of resources, including hardware, support services and licensing costs. In particular:

- Four sites reviewed at the Oak Ridge Reservation either had separate VoIP networks in place or had performed pilot projects to implement new networks. For instance, the Oak Ridge Office (ORO) had initiated a project to replace its landline telephone system with a VoIP solution through the Office of Science's (Science) Information Technology Modernization Plan which, when completed, will provide updated telecommunications services to Federal employees throughout Science. While ORO officials noted that this system had been implemented with the capacity to allow for expansion to include the other sites on the Oak Ridge Reservation, we found that other sites were independently carrying out their own VoIP activities. Specifically, Oak Ridge Associated Universities officials confirmed that their separate service provider-managed VoIP system was operational, and the East Tennessee Technology Park spent $21,000 on a VoIP pilot project in 2008 with the support of ORO but discontinued the effort after 24 months due to a lack of financial feasibility. In addition, the Oak Ridge National Laboratory began a separate project in 2011 to provide VoIP services to that site. Officials also told us that future phases of the Science VoIP initiative will expand ORO's network to provide telecommunications services to Federal employees at other site offices and Headquarters. However, this effort is potentially duplicative of services that may already be available at those sites, including the Office of the Chief Information Officer's (OCIO) VoIP network at Headquarters.

- Other sites had split existing telecommunications systems to implement separate VoIP networks. For example, even though they are located in the same geographic area, the Pacific Northwest National Laboratory (PNNL) and the Hanford Site (Hanford) each implemented or were implementing separate VoIP networks. Prior to 2007, certain buildings at PNNL were connected to the Hanford phone system. According to Hanford officials, when the site was planning its VoIP deployment, it invited PNNL to join; however, officials stated that PNNL declined. PNNL officials commented that, subsequent to 2007, the site decided to implement its own VoIP network because it

believed that moving to its own system permitted process improvements that better achieved objectives related to functional capacity, security, reliability and operational cost requirements. However, much, if not all, of what PNNL hoped to achieve could have been accomplished by consolidating its needs with the Hanford and implementing a joint VoIP network, thus avoiding duplicative efforts. The Hanford system was able to support approximately 22,000 lines of services – only about half of which were being used. The PNNL VoIP system was estimated to provide up to 7,000 lines of service. Proposed funding for the new PNNL network totaled approximately $2.8 million, while the Hanford VoIP initiative was completed at just under $7 million. Office of Environmental Management officials noted that the capacity of the Hanford VoIP network was designed for future growth to accommodate other Office of Environmental Management sites. While we agree with management's statement, we continue to maintain that additional capacity could have been used to meet PNNL's needs had the sites better coordinated.

In addition, PNNL expended significant resources to perform a partial system implementation even though a more cost effective alternative had been identified. The expenditures may have been avoidable had the recommendations of a site commissioned alternatives analysis been implemented. That analysis recommended that PNNL continue with its then-current solution for a period of time to allow the VoIP technology and markets to mature. However, officials chose to implement a limited 1,200 line system at a cost of approximately $1 million. Site officials have since chosen what they believe to be a more cost effective solution that added almost 6,000 lines at a cost of $1.8 million. Even though the analysis conducted for PNNL recommended that postponing the development of a VoIP network was the most cost effective solution, the Federal site office did not question PNNL's decision to proceed with its implementation.

Cybersecurity Controls

Sites had not always applied all required technical cybersecurity controls to VoIP networks. Contrary to security requirements issued by the National Institute of Standards and Technology, only limited vulnerability scanning and penetration testing was performed on the installed VoIP systems at seven of nine sites reviewed. VoIP networks are subject to the same security weaknesses that can affect the confidentiality, integrity and availability of data networks. Additionally, VoIP networks can provide additional threat vectors for traditional exploits and malware through the significant increase in network internet protocol addresses. As such, the timely identification and remediation of vulnerabilities that could cause attacks such as Denial of Service[1] within the network is imperative to ensure continued service.

Our testing also revealed a number of issues related to process-oriented general security controls that could increase the risk of compromise to the telecommunications networks and other interconnected information systems. In particular, contingency plans had not always been fully developed and tested on the VoIP system reviewed at PNNL, and the OCIO could

[1] A Denial of Service attack is an incident in which a user or organization is deprived of network services such as e-mail or VoIP, usually through an overload of network traffic to an internet protocol address.

not provide documentation demonstrating that contingency plans had been tested on a regular basis. Although PNNL officials noted that they had completed a disaster recovery plan, we found that the plan did not address the recovery of the site's VoIP system in the event of a loss of availability. As required by the National Institute of Standards and Technology, information system owners should develop, test and revise contingency plans on a regular basis as part of maintaining a system's operation.

Furthermore, two of nine sites reviewed did not perform required security control assessments. Specifically, PNNL and Oak Ridge National Laboratory did not perform or could not provide documentation to support that security assessments had been performed on a periodic basis. Periodic security assessments allow programs and sites to address changing security requirements, emerging threats, vulnerabilities, attack methods and the availability of new technologies. PNNL officials noted that they assessed the risks associated with VoIP systems. However, our review of PNNL's system security plan determined that the document did not include information about which National Institute of Standards and Technology controls were implemented on the network or provide assurance that such controls were tested and operating as intended.

Management of Telecommunications Infrastructure

The issues identified occurred, in part, because the Department had not ensured a coordinated and well-communicated approach related to the implementation of VoIP systems. In addition, a lack of effective monitoring of the various program/site level initiatives adversely impacted the Department's ability to ensure efficient and effective implementation of VoIP systems and corresponding cybersecurity controls.

Coordination and Planning

Department officials had not always ensured that a coordinated and well-communicated approach was executed during the implementation of VoIP networks. As such, many sites had undertaken ad-hoc VoIP implementation initiatives without consistent direction or appropriate coordination. For instance, even though the Department's OCIO was implementing a VoIP system at Headquarters, Science planned to establish its own capabilities through the Science VoIP initiative. Had the numerous ongoing projects been fully coordinated, the Department would have had the opportunity to perform appropriate studies and likely have been able to coordinate system implementations in a more cost effective and efficient manner. Absent effective coordination, one of the key advantages of VoIP was diminished – cost reduction through scalability. Specifically, coordination between programs and sites that were implementing VoIP could have potentially decreased the more than $56 million in estimated implementation costs and helped ensure that common VoIP resources such as hardware, support services and licensing costs were shared, as appropriate. Although Science officials commented that the program's Information Technology Modernization Plan would help ensure coordination of VoIP efforts, we noted that the plan was limited to Federal elements and did not include operating contractors.

A lack of planning also contributed to the implementation issues that were identified. In particular, while Science had outlined a three-phased approach to providing VoIP services to its

Federal employees, officials had not completed planning activities for efforts beyond the first phase, which was underway at ORO. As such, Science officials could not provide cost estimates for future efforts and had not fully considered the potential duplication issues we identified between the national laboratories and site offices. In addition, PNNL had not followed the recommendation of an alternatives analysis it commissioned which identified a more cost effective solution to its initial VoIP implementation.

In technical comments on our report, management stated that it had drafted an Information Resource Management Strategic Plan and planned to implement VoIP capabilities to all of the OCIO's current customers at Headquarters. While this is an encouraging first step, it may not fully address the issues identified during the audit because the scope of the planned efforts did not include Headquarters programs that were not current OCIO customers or any of the Department's field elements. In addition, technical comments from the Department's various programs generally did not provide evidence demonstrating increased cooperation across the Department.

Performance Monitoring

The Department had not adequately monitored the implementation of VoIP efforts or related cybersecurity controls. In particular, neither the OCIO nor program offices had conducted an adequate review or evaluation of the various VoIP implementations being undertaken. Monitoring and oversight of VoIP projects should have begun early in the process and could have allowed the Department to fully evaluate the benefits and need for VoIP networks. To date, the Department has yet to assign oversight responsibility for VoIP implementation to any centralized authority, such as the OCIO or a related information technology council.

We also found that the Department had not adequately monitored the implementation of cybersecurity controls for VoIP systems. Programs left the interpretation and implementation of cybersecurity controls up to site offices. However, we found that certain site offices had not adequately monitored the development and implementation of these controls. Specifically, site office officials had not ensured that performance assessments of VoIP network security had occurred at most of the sites reviewed. As a result of the lack of monitoring and/or guidance related to VoIP implementation, cybersecurity controls were not consistently applied or not applied at all across the Department and resulted in increased risks to systems and networks.

In response to our report, management indicated that efforts were underway to strengthen its performance monitoring program. For instance, the National Nuclear Security Administration indicated that VoIP networks will be included in various cybersecurity surveys and reviews and noted that it will reemphasize the need to ensure adequate security over VoIP systems. In addition, Science commented that it ensured effective performance monitoring related to cybersecurity as part of implementing and monitoring the VoIP controls recommended by Federal guidance and that VoIP controls are monitored through the results of independent surveys conducted by the Department's Office of Cyber Assessments. However, we learned through discussions with Office of Cyber Assessments personnel that VoIP systems at Science locations have not been tested. Ensuring that VoIP systems are within the scope of assessments can be a valuable management tool and further enhance performance monitoring activities.

Opportunities for Improvement

Without improvements in coordination, planning and ensuring effective performance monitoring, the Department will continue to implement a duplicative, decentralized and fragmented approach for managing VoIP systems. Had the Department examined and identified opportunities for consolidation of its multiple VoIP networks, it may have realized significant savings related to the implementation and support of its voice networks. For example, had the Department fully assessed its enterprise-wide telecommunications needs and appropriately coordinated and consolidated its efforts to the extent practical, it could have potentially reduced the $56 million spent on VoIP efforts. Enhanced performance monitoring of ongoing and future VoIP network implementations could also reduce expenditures. We noted that PNNL spent almost $1 million on its initial VoIP implementation. However, officials stated that after installing a solution that supported over 1,200 lines of service, the expansion of that project was halted to review another solution that they believed would be more cost effective – a solution that will provide almost 6,000 lines of service at a cost of $1.8 million. Going forward, effective coordination, monitoring and consolidation could save the Department significant amounts of increasingly scarce funds. Furthermore, lack of effective performance monitoring by programs and sites to appropriately identify and implement cyber security controls may increase the risk of compromise to information systems and networks.

As noted in the Department's recently developed Information Technology Modernization Strategy, it must seek opportunities to improve efficiency and reduce the cost of services. This strategy jointly tasks the Department's and National Nuclear Security Administration's Chief Information Officers with modernizing the information technology environment and identifying opportunities to share services, reduce costs and leverage new technologies. The corrective actions recommended in this report can help remediate the issues identified during our audit and facilitate the Department's implementation of its Information Technology Modernization Strategy as it begins examining alternatives for unified communications such as integration of instant messaging, web and video conferencing, voice, e-mail and calendaring.

Notably, some Department sites realized savings through the implementation of VoIP networks. Hanford reported that it realized savings of approximately $2 million per year through its VoIP implementation. These savings resulted from lowered operational costs related to reducing overall power consumption and reduced maintenance and labor costs. Officials at Los Alamos National Laboratory stated that they had realized similar savings.

RECOMMENDATIONS

To more effectively manage its Voice over Internet Protocol telecommunications networks in an efficient and secure manner, we recommend that the Under Secretary for Nuclear Security, the Deputy Under Secretary for Science and Energy and the Deputy Under Secretary for Management and Performance, in coordination with the Department's and National Nuclear Security Administration's Chief Information Officers:

1. Develop and implement an enterprise-wide telecommunications strategy that leverages existing resources; encourages communication, cooperation and planning by and among programs and sites; and eliminates unnecessary duplication and excess capacity; and

2. Ensure effective performance monitoring to strengthen cyber security over VoIP systems and networks, including correcting, through the implementation of appropriate controls, the cyber security weaknesses identified in this report.

MANAGEMENT RESPONSE

Management concurred with the report's recommendations and commented that corrective actions had been taken and/or initiated. Management commented that the Department's Information Resource Management Strategic Plan included language to improve collaboration when delivering management and technology solutions. Management also indicated that efforts were being made to ensure effective performance monitoring to strengthen cybersecurity over VoIP systems and networks. In technical comments, the National Nuclear Security Administration commented that it will evaluate potential enterprise-wide opportunities related to VoIP implementation and will reemphasize that VoIP systems must meet Federal cybersecurity requirements. Science management commented that it will work with the OCIO and other stakeholders to develop a strategic plan related to VoIP.

AUDITOR COMMENTS

Management's comments are generally responsive to our recommendations. However, although management concurred with the report's recommendations and considered corrective actions for both recommendations to be complete, technical comments submitted by various program offices related to coordination, planning and performance monitoring indicated that additional work is necessary to address the report's recommendations. We have addressed management's technical comments in the body of the report. Management's comments are included in Appendix 3.

OBJECTIVE, SCOPE AND METHODOLOGY

Objective

To determine whether the Department of Energy (Department) planned and implemented its Voice over Internet Protocol (VoIP) telecommunications networks in an efficient and secure manner.

Scope

We conducted the audit from November 2012 to June 2014, at Headquarters offices in Washington, DC and Germantown, Maryland; Oak Ridge National Laboratory, Y-12 National Security Complex, East Tennessee Technology Park, Oak Ridge Associated Universities and the Oak Ridge Office in Oak Ridge, Tennessee; Pacific Northwest National Laboratory, Richland Operations Office and the Hanford Site, in Richland, Washington; Los Alamos National Laboratory in Los Alamos, New Mexico; and Sandia National Laboratories in Albuquerque, New Mexico. This audit was conducted under Office of Inspector General project number A13TG009.

Methodology

To accomplish the audit objective, we judgmentally selected a sample of 10 Departmental sites. This selection was based on the sites' implementation of unclassified VoIP networks. Because a judgmental sample was used, results are limited to the sites or locations selected. Additionally, we:

- Evaluated the Department's policies and procedures regarding the communications equipment;
- Evaluated the costs associated with the Department's implementation of VoIP networks;
- Determined whether a risk-based approach had been implemented to assist in the security of communications equipment;
- Evaluated protective measures to determine if both physical and cyber related vulnerabilities had been considered for the Department's communications infrastructure;
- Reviewed actions taken to address prior findings and recommendations relevant to this audit area; and
- Identified opportunities for improving the Department's management of its unclassified communications resources.

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 objectives. Accordingly, we assessed significant internal controls and the Department's implementation of the *GPRA Modernization Act of 2010* and determined that it had not established performance measures for the management of its telecommunications infrastructure. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our evaluation. We did not rely on computer-processed data to satisfy our audit objectives.

Management waived an exit conference.

PRIOR REPORTS

- Evaluation Report on *The Department's Unclassified Cyber Security Program – 2013* (DOE/IG-0897, October 2013). The Department of Energy (Department) had taken a number of positive steps over the past year to correct cyber security weaknesses related to its unclassified information systems. In spite of these efforts, our testing revealed various weaknesses related to security reporting, access controls, patch management, system integrity, configuration management, segregation of duties and security management. The weaknesses identified occurred, in part, because Department elements had not ensured that policies and procedures were fully developed and implemented to meet all necessary cyber security requirements. In addition, the Department continued to operate a less than fully effective performance monitoring and risk management program. Absent improvements to its unclassified cyber security program, the Department's information and systems will continue to be at a higher than necessary risk of compromise.

- Audit Report on *Telecommunications Infrastructure* (DOE/IG-0537, December 2001). The report identified that duplicative data transmission infrastructures existed across the Departmental complex. Further, the Department had not optimized the acquisition of internet and video services. Specifically, organizations maintained about 190 data transmission circuits that duplicated capabilities of other Department-wide networks; a number of sites utilized open market sources to acquire internet service that could have been provided from existing capacity; and organizations were maintaining video teleconferencing capabilities that were incompatible with corporate networks. These problems occurred because the Department had not developed and implemented a coordinated approach to the acquisition and use of telecommunications equipment and services. Further, the Department had not adopted a comprehensive set of performance measures and incentives which would have encouraged both Federal employees and contractors to obtain necessary telecommunications capabilities as cost effectively as possible. As a consequence, the Department annually spends at least $4 million more than necessary to operate and maintain its telecommunications infrastructure.

MANAGEMENT COMMENTS

Department of Energy
Washington, DC 20585

May 9, 2014

MEMORANDUM FOR RICKEY R. HASS
DEPUTY INSPECTOR GENERAL
FOR AUDITS AND INSPECTIONS
OFFICE OF INSPECTOR GENERAL

FROM: ROBERT F. BRESE
CHIEF INFORMATION OFFICER

SUBJECT: Draft Report, "The Department's Implementation of Voice over Internet Protocol Telecommunications Networks" (A13TG009)

Thank you for the opportunity to comment on the subject draft report. The Department recognizes that the Inspector General's (IG) objective in this review was to determine whether DOE planned and implemented its Voice over Internet Protocol (VoIP) telecommunications networks in an efficient and secure manner. We appreciate the IG's efforts to review our programs and we agree with the IG's assertion that there is value in having an enterprise-wide telecommunications strategy.

The management response to the specific recommendations in the draft report is outlined below. Program-specific plans of action and technical comments are included in the appendices.

Recommendation 1: *Develop and implement an enterprise-wide telecommunications strategy that leverages existing resources, encourages communication, cooperation and planning by and among programs, and sites and eliminates unnecessary duplication and excess capacity.*

Management Response: Concur.

The Department's Information Resource Management (IRM) Vision to "Collaborate as an enterprise to deliver innovative management and technology solutions that support the Department's mission" and the supporting strategic goals contained in the Final Draft FY 2014-2018 IRM Strategic Plan addresses this recommendation.

Departmental organizations, to include the National Nuclear Security Administration (NNSA), the Office of Science (SC), and the Office of Environmental Management (EM) worked with the Office of the Chief Information Officer (OCIO) to develop the IRM Strategic Plan. EM is also working on a plan for the EM enterprise which will align with the overall IRM Strategy.

The planning and execution of the IRM Strategic Plan is an on-going process designed to ensure that the Department uses the most efficient and integrated approach to the provision of services. Recommendations resulting from the 120 day study will be factored into future efforts. Progress in implementing an enterprise-wide telecommunications strategy that leverages existing resources, encourages communication, cooperation, and planning by and among programs and

sites and eliminates unnecessary duplication and excess capacity is demonstrated by the Office of the Chief Information Officer (OCIO) receiving approval from the Working Capital Fund Council on April 15, 2014 to roll out VoIP technology to all Headquarters EITS customers.

The Department considers this recommendation closed.

Recommendation 2: *Ensure effective performance monitoring to strengthen cyber security over VoIP systems and networks, including correcting, through the implementation of appropriate controls, the cyber security weakness identified in this report.*

Management Response: Concur.

Across the Department, efforts are already being made to ensure effective performance monitoring to strengthen cyber security over VoIP systems and networks, as detailed in Attachment A. The Department considers this recommendation closed.

If you have any questions, please refer to Appendix A for the appropriate point of contact.

Attachments
- Attachment A – Program-specific Actions
- Attachment B – Technical Comments
- Attachment C – Monetary Impact

FEEDBACK

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We aim to make our reports as responsive as possible and ask you to consider sharing your thoughts with us.

Please send your comments, suggestions and feedback to OIGReports@hq.doe.gov and include your name, contact information and the report number. Comments may also be mailed to:

Office of Inspector General (IG-12)
Department of Energy
Washington, DC 20585

If you want to discuss this report or your comments with a member of the Office of Inspector General staff, please contact our office at (202) 253-2162.