U.S. Department of Energy
Office of Inspector General
Office of Audits and Inspections

Audit Report

The Department's Management of the Smart Grid Investment Grant Program

OAS-RA-12-04

January 2012

Department of Energy
Washington, DC 20585

January 20, 2012

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "The Department's Management of the Smart Grid Investment Grant Program"

INTRODUCTION AND OBJECTIVE

The Energy Independence and Security Act of 2007 charged the Department of Energy with establishing the Smart Grid Investment Grant (SGIG) program. More recently, the American Recovery and Reinvestment Act of 2009 (Recovery Act) provided the Department's Office of Electricity Delivery and Energy Reliability (OE) with $3.5 billion to fund the SGIG program and to assist in modernizing the Nation's power grid. The SGIG program was to facilitate the installation of state-of-the-art information technologies and, ultimately, improve grid reliability and enable consumers to reduce the amount of energy used. The program required that the portion of a recipient's project paid for with Federal funds not exceed 50 percent of the total project cost. The Department awarded all of its available grant funds to 99 recipients, with awards ranging in value from $397,000 to $200 million.

Reliability of the grid, specifically, ensuring that the Nation's power grid is adequately protected from malicious cyber attacks has been and continues to be an area of concern in both the public and private sectors. Our report on the *Federal Energy Regulatory Commission's Monitoring of Power Grid Cyber Security* (DOE/IG-0846, January 2011) disclosed weaknesses related to the Critical Infrastructure Protection cyber security standards. In addition, the U.S. Government Accountability Office's report on *Electricity Grid Modernization* (GAO-11-117, January 2011) identified weaknesses regarding the implementation and enforcement of Smart Grid cyber security guidelines. Given the importance of developing an effective and secure Smart Grid, we performed this audit to determine whether the Department adequately administered and monitored the SGIG program.

RESULTS OF AUDIT

Although the Department had taken a number of positive actions, our audit revealed several opportunities to enhance management of the SGIG program. The problems that we discovered could jeopardize achievement of Recovery Act goals. In particular, we found that:

- Department officials approved Smart Grid projects that used Federally-sourced funds to meet cost-share requirements. Although specifically prohibited by regulation, one grantee inappropriately used $1.8 million in Federal funds to meet grant cost-share obligations. This practice is prohibited under the SGIG program because it effectively

increased the Federal portion of the project to more than the maximum 50 percent cost-share. In addition, one recipient was reimbursed twice for the same costs related to transportation. The transportation costs were reimbursed as both direct cost and as part of the overhead cost calculation, and represented reimbursement of almost $300,000 more than appropriate through June 2011; and,

- Three of the five cyber security plans (required to be submitted by grantees) which we reviewed were incomplete, and did not always sufficiently describe security controls and how they were implemented. Department officials noted that Federal involvement was limited when managing grants, but they had required grant recipients to develop cyber security plans that supported the strategy outlined in the grant application and described a minimum set of security elements, such as risk assessment and system security incident response. However, a Department review revealed that 36 of 99 cyber security approaches submitted as part of the grant application lacked one or more required elements. In our review of security plans, we noted that the plans did not always include sufficient information related to risk assessments and/or other important elements, and, that they did not fully address many of the weaknesses initially identified by the Department.

The issues we found were due, in part, to the accelerated planning, development, and deployment approach adopted by the Department for the SGIG program. In particular, the Department had not always ensured that certain elements of the SGIG program were adequately monitored. There was no assurance that the Department's grant monitoring methodology was completely effective. Furthermore, officials approved cyber security plans for Smart Grid projects even though some of the plans contained shortcomings that could result in poorly implemented controls. We also found that the Department was so focused on quickly disbursing Recovery Act funds that it had not ensured personnel received adequate grants management training.

Without improvements, there remains a risk that the goals and objectives of the Smart Grid program may not be fully realized. From a business management perspective relating to taxpayer-provided funding, we questioned reimbursements totaling more than $2 million for activities related to the use of Federal funds to meet cost-share obligations and duplicate cost reimbursement.

Notably, the Department had taken actions to ensure that submitted SGIG proposals were reviewed and evaluated prior to providing financial assistance to projects that enabled improvements and modernization of the electric transmission and distribution system. For instance, OE developed an extensive process for assessing the impacts and benefits of the various Smart Grid projects. Reviews were performed on proposals by subject matter experts, technical topic managers, and a merit review committee. In addition, program officials performed a number of monitoring functions over recipients' activities associated with the grants. These are positive actions; however, in our view, additional effort is necessary to ensure that the grants are adequately managed over their lifecycle so that program objectives can be met. As such, we have made several recommendations that, if fully implemented, should help improve the Department's ability to effectively administer and monitor the SGIG program.

MANAGEMENT REACTION

Management generally concurred with the report's recommendations and indicated that it will take steps to respond to the recommendations. Management, however, expressed concerns with a number of assertions made in our report. Management's comments, including its concerns and our response, are more thoroughly discussed in the body of the report and are included in their entirety in Appendix 3.

Attachment

cc: Deputy Secretary
Associate Deputy Secretary
Assistant Secretary, Office of Electricity Delivery and Energy Reliability
Chief of Staff
Acting Chief Financial Officer
Chief Information Officer

REPORT ON THE DEPARTMENT'S MANAGEMENT OF THE SMART GRID INVESTMENT GRANT PROGRAM

TABLE OF CONTENTS

Management and Cyber Security Controls

Appendices

The Department's Management of the Smart Grid Investment Grant Program

Management and Cyber Security Controls

Our review revealed several opportunities to improve certain aspects of the Department of Energy's (Department) Smart Grid Investment Grant (SGIG) program. In particular, although the initial Funding Opportunity Announcement stated that Federally-sourced funds were not to be used for cost-share requirements, we determined that the Department had approved one Smart Grid project that utilized Federal funds to meet cost-share requirements. In addition, we identified one recipient that was reimbursed twice for the same costs related to transportation. Furthermore, cyber security plans developed by recipients were not always complete, and did not sufficiently describe security controls and how they were to be implemented.

Approval of Smart Grid Projects

We found that the Department had approved one Smart Grid project even though the grant recipient's application noted its intent to use Federally-sourced reimbursements from work performed by its partner utilities on the same grant to meet a portion of its required cost-share. The SGIG program required that the recipient's cost-share be at least 50 percent of the total project cost and no funds from a Federal source be used to meet this requirement. We observed, however, that for one particular grant the recipient retained its partners' Federally-sourced reimbursement to meet the cost-share requirements for its portion of the project. As a result, we determined that the Department had funded 60 percent of the recipient's project – significantly more than the mandated 50 percent limit. As such, we questioned the Department's reimbursement of more than $1.8 million in American Recovery and Reinvestment Act of 2009 (Recovery Act) funds for that particular grant.

Cost Reimbursement

The Department did not always follow effective business practices when reimbursing grant recipients. In particular, we identified one recipient that was reimbursed twice for the same costs related to transportation. While the recipient billed costs totaling almost $600,000 and was reimbursed one-half of that amount for direct transportation, it had also included transportation costs as part of its overhead rate calculation. As these costs should be properly classified as an element of the recipient's indirect costs, we questioned the reimbursement of almost $300,000 more than necessary through June 2011. Office of Electricity Delivery and Energy Reliability (OE) officials stated that all indirect rates would

be reviewed and reconciled prior to closing out individual grants and recipients would be responsible for reimbursing the Department for any overpayments. However, we believe this practice presents an unnecessary risk because the Department may have difficulty recovering funds from recipients if they become unable to meet the terms of their grant agreements.

Cyber Security

Cyber security plans submitted by recipients were not always complete or they did not describe intended controls in sufficient detail. As part of the grant application process, OE required each applicant to submit its approach to cyber security as part of its award application. Using a two-tier review conducted by subject matter experts, officials identified one or more required elements lacking in 36 of 99 (36 percent) cyber security approaches submitted in the grant applications. When the grants were awarded, the Department instructed recipients to develop a cyber security plan consistent with the approaches presented as part of the grant application process. In addition, cyber security plans were to, at a minimum, describe the recipients' approaches to detecting, preventing, and communicating with regard to, responding to, and recovering from system security incidents. Further, cyber security plans were required to contain detailed descriptions of the recipients' risk assessment processes, risk mitigation strategies, and other elements of their cyber security programs. However, although the Department approved these updated plans, our review found that the initial weaknesses had not always been fully addressed, and did not include a number of security practices commonly recommended for Federal government and industry systems. For instance:

- One recipient's cyber security plan provided only a summary description of its cyber security processes. While the plan addressed cyber security concerns related to the Smart Grid, it did not provide adequate details related to the risk assessment or mitigation processes. In addition, cyber security elements were discussed in general terms, and quality assurance and overall impact on grid security was not presented in detail. For instance, the recipient's approach to detecting, preventing, and communicating system security incidents was not adequately described. In particular, the plan stated that the recipient used monitoring, logging, and alerting technologies to detect incidents and exploits, but did not detail how these systems worked in its specific environment. Also, no detail was provided to explain how detected incidents were contained

and corrected to restore systems. Without a thorough description of these processes, the Department, grantee, and other related parties cannot determine if those elements are being properly implemented.

- Another recipient submitted a cyber security plan that was based on guidance developed by the National Institute of Standards and Technology (NIST). However, the plan contained only the minimal elements required by the Department in the Funding Opportunity Announcement and did not provide sufficient detail regarding how the elements would be implemented in the recipient's environment. For example, the plan indicated that the recipient had a risk assessment and mitigation process in place. However, the recipient commented that, while risks and mitigation strategies were included in the plan, a formal risk assessment had never been performed. Without a formal risk assessment and associated mitigation strategy, threats and weaknesses may go unidentified and expose the recipient's systems to an unacceptable level of risk.

Despite the shortcomings in cyber security plans described above, we were informed that recipients were given the 3-year duration of the award to implement agreed-upon cyber security controls. We acknowledge that the security plans will evolve as systems are developed and implemented. However, this practice may be problematic in that any existing gaps in a recipient's security environment could allow system compromise before controls are implemented. Likewise, approved elements that were not well-defined in the plan could leave the system susceptible to compromise even after the cyber security plan had been fully implemented. For example, without a well-defined risk management process, potential risks may go unidentified and related mitigating controls may not be implemented. Notably, Department officials told us that they are addressing risks by requiring that Technical Project Officers (TPO) and subject matter experts review the cyber security posture and recommend updates to cyber security policies when they perform their annual site visits to grant recipients. Additionally, to the Department's credit, it created a website tailored to the cyber security needs of the SGIG projects, conducted webinars to provide technical assistance, and conducted a cyber security information exchange with all recipients to share the results of site visits and best practices.

In comments on our report, Department officials noted that, due to the nature of grants, Federal government involvement in the management of projects was limited, and indicated that including

the requirement to develop a cyber security plan in the grant terms and conditions was an extra measure taken to ensure that this area was addressed. We commend the Department for its efforts to develop a cyber security strategy; however, we believe that continuing attention is needed to help strengthen grantee plans. Department officials told us that they are committed to monitoring grantees throughout the 3-year implementation cycle to ensure that plans are updated as needed.

Performance Monitoring and Training

The issues identified were due, in part, to the accelerated planning, development, and deployment approach adopted by the Department for the SGIG program. In particular, the Department had not ensured that the methodology used by the TPOs was completely effective for monitoring Smart Grid grants. In addition, because the Department was focused on quickly disbursing Recovery Act funds, it had not ensured personnel had received adequate training to manage grants.

Performance Monitoring and Oversight

The Department had not ensured that the TPOs effectively monitored the SGIG program. In particular, we found that the TPOs were not involved in the review and approval of indirect costs submitted by recipients during the grant application process. Rather, the contracting officers were responsible for approving the components of indirect cost rates as part of the grant award. Therefore, most TPOs compared the indirect rates claimed for reimbursement to the rate approved in the award agreement and did not perform any further checks as to the validity of the rate. In addition, most of the TPOs did not have a complete understanding of how indirect costs were calculated and applied by recipients. Had the TPOs coordinated with the contracting officers and completed effective reviews of indirect costs, certain cost-related issues discovered during our review may have been identified and remediated. In preliminary comments on our report, officials noted that the contracting officer had provisionally approved recipients' indirect rates and would verify the costs at the end of the grants with final cost incurred audits. However, the lack of coordination between the TPO and contracting officer led to the Department reimbursing one recipient twice for the same costs related to transportation. While reimbursements are subject to final audit and recovery if deemed inappropriate, relying on the audit as a general control mechanism creates a higher than necessary risk that the Department will be unable to recover funds from recipients when grant funds have been completely expended.

We also found that the Department's approach to limit Federal involvement in grant implementation contributed to cyber security plans that lacked thorough descriptions by recipients as to how all minimum security controls would be implemented in their respective environments. While officials were aware of the many weaknesses in the plans, they approved them even though they did not sufficiently detail the minimum standards specified in the award terms. As a result, the approved cyber security plans did not adequately address security risks or planned cyber security controls.

Training

Department officials had not ensured that all personnel involved in the SGIG program received adequate training related to managing grants under their purview. Specifically, in an accelerated effort to establish a new grants management office, OE hired many new employees and enlisted the help of employees within other areas of the Department to oversee the SGIG program. However, we noted that only 2 of 10 TPOs were trained and certified in accordance with Department policies and procedures. One of these two individuals had received certification that allowed him to oversee only grants and cooperative agreements under $10 million. However, each of the TPOs was monitoring Smart Grid projects well above that threshold, including five individuals that were responsible for grants ranging from $100 million to $200 million. In comments to our draft report, OE officials noted that they planned to ensure that the TPOs receive the necessary training for the certification that allows them to oversee grants and cooperative agreements above the $10 million threshold.

Realization of Goals and Objectives

Without improvements in monitoring and oversight of the SGIG program, there is a significant risk that certain goals and objectives of the Smart Grid may not be fully realized. For example, reimbursement of costs that do not support Smart Grid goals do not enhance the overall reliability of the power grid and divert funds from other projects that could help the grid to function in a more efficient and cost-effective manner. As noted in the report, we questioned reimbursements totaling more than $2 million for activities related to the use of Federal funds to meet cost-share obligations and duplicate cost reimbursement. Had the Department only reimbursed costs that fully supported the modernization goals of the SGIG program, it could have applied the questioned amounts towards other projects or awarded additional grants. In addition, as our review only evaluated 20 of

the 99 grants awarded, the amount of Recovery Act funds the Department paid to recipients for projects that do not support the program's goals may be higher.

Issues with grantee cyber security plans for Smart Grid projects could also result in poorly implemented controls, leaving the power grid susceptible to compromise by malicious individuals.

RECOMMENDATIONS

To help improve the Department's ability to effectively administer and monitor the SGIG program, we recommend that the Assistant Secretary, Office of Electricity Delivery and Energy Reliability ensure that:

1. The allowability of the costs questioned in this report is determined and program procedures are updated, as needed;

2. Grantees' cyber security plans are complete, including thorough descriptions of potential security risks and related mitigation through necessary cyber security controls;

3. An effective methodology for monitoring the SGIG program is developed and implemented; and,

4. Technical Project Officers are adequately trained and certified to manage the grants under their purview.

MANAGEMENT REACTION AND AUDITOR COMMENTS

Management generally concurred with the report's recommendations and indicated that action was planned, or had been initiated to respond to the four recommendations in the report. Management's proposed or initiated corrective actions are responsive to our recommendations. Management's comments indicated concerns with a number of assertions related to cost reimbursement and cyber security made in our report. We have addressed management's comments below and made technical changes to the report, as appropriate. Management's comments are included in their entirety in Appendix 3.

Cost Reimbursement

Management commented that it believed it had acted in full compliance with the law and Federal procurement regulations with regards to reimbursing costs related to recapturing the residual value of obsolete meters and the use of Federally-sourced reimbursements to meet a portion of recipients' cost share requirements. In addition, management indicated that it believed

the language in the report incorrectly implied intentional and willful violation of these regulations when projects were chosen for award. Specifically, management commented that it made the decision to reimburse the costs of the obsolete meters based on two considerations. The cost principles in the Federal Acquisition Regulations (FAR) allowed the recipient to claim losses on the disposition of depreciable property. Additionally, the reimbursed costs for outdated meters supported the goals of the SGIG program and the cost recovery treatment by local utility regulators allowed for recovery of these costs. Management also believed it had not allowed one recipient to use Federally-sourced funds to meet its cost-share requirement.

After further evaluation, we agree that the FAR allows grant recipients to claim reimbursement for the residual value of obsolete meters and have made changes to remove this information from the report, as necessary. However, we continue to disagree that Federally-sourced funds were not used to meet the cost-share requirements for one grant recipient. In particular, the recipient's project budget documentation clearly shows it would contribute only a small amount of its own funds to the project, and planned to use Federally-sourced reimbursements from its partners to meet the remaining cost-share requirements. As noted in the report, at the time our analysis was performed the Department had funded roughly 60 percent of the recipient's project even though the SGIG program required that no funds from a Federal source be used to meet cost-share requirements and that Federal contribution not exceed 50 percent of the total project cost. While management observed that our report could lead one to the impression that the Department's actions were completed in a willful or intentionally negligent manner, we do not assert that such was the case.

Cyber Security

Management also commented that there are currently no Federal or state standards or regulations that mandate cyber security processes or practices for electric distribution systems. Therefore, to ensure its recipients take cyber security seriously in the absence of such rules, the Department required each project to develop a cyber security plan that was signed by a corporate officer. The plans were then reviewed by the Department's cyber security experts, and approved by individual recipient's TPOs. Management further relayed its concern regarding the potential for confusion about the required contents for each SGIG project's cyber security plan, as stated in the report. In particular, management noted that our statement regarding cyber security plan requirements, such as

detailed descriptions of the recipients' risk assessment processes, risk mitigation strategies, and cyber security controls, were never included in any Department guidance to the recipients. In fact, the cyber security plans were intended to be flexible enough to be tailored to specific project needs and, management felt, should focus on the recipient's cyber security methodologies and provide sufficient details on the approaches. Finally, management stated that the cyber security plans were reviewed by cyber security subject matter experts, the final version was approved by the Department, and a progress review of the recipient's cyber security implementation was an integral part of the annual site visit. As a result of the site visit review, many recipients are in the process of updating and strengthening their cyber security plans.

We agree with management's statements regarding the lack of cyber security standards or regulations for electric distribution systems, as noted in the report. However, awards were granted to recipients with control over all aspects of the Nation's electric grid, to include both transmission and distribution systems. Therefore, we believe that the SGIG program provided the Department a unique opportunity to promote strong cyber security programs among its recipients; an area which, based on the issues identified during our audit, could have been more thoroughly explored. We also believe that the Department should take steps to ensure the submitted cyber security plans are complete, being implemented, and are updated as situations warrant. While we agree that a cyber security plan should be flexible enough for tailoring to each project, the plan should contain sufficient information to assess the grant recipient's cyber security posture.

We agree with management's statement that Department guidance to recipients did not require detailed descriptions of cyber security controls. However, the SGIG Program Management Plan identified the requirement for recipients' cyber security plans, to include detailed descriptions of the recipient's risk assessment and mitigation processes and other standards to which the projects would adhere. This information was formally provided to the recipients as part of the project deliverables lists in the terms and conditions of the grant agreement.

Appendix 1

OBJECTIVE

To determine whether the Department of Energy (Department) adequately administered and monitored the Smart Grid Investment Grant (SGIG) program.

SCOPE

The audit was performed between November 2010 and January 2012, at Department Headquarters in Washington, DC and various grant recipients in Texas and Arizona. Reimbursement information for additional grant recipients was also reviewed.

METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable laws and Department policies, including those pertaining to securing Smart Grid technologies;
- Reviewed applicable guidance issued by the National Institute of Standards and Technology and the Federal Energy Regulatory Commission;
- Reviewed prior reports issued by the Office of Inspector General and the U.S. Government Accountability Office;
- Obtained documentation from and held discussions with officials from the Department's Office of Electricity Delivery and Energy Reliability;
- Reviewed invoices submitted by grant recipients for appropriateness; and,
- Reviewed selected approved recipient cyber security plans for completeness.

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 finding and conclusions based on our audit objectives. Accordingly, we assessed significant internal controls and the Department's implementation of the *Government Performance and Results Act of 1993* and determined that it had established performance measures for management of its SGIG activities. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our audit. We did not rely on computer-processed data to satisfy our audit objective. An exit conference was held with Department officials on January 12, 2012.

RELATED REPORTS

Office of Inspector General Report

- *Federal Energy Regulatory Commission's Monitoring of Power Grid Cyber Security* (DOE/IG-0846, January 2011). Although the Federal Energy Regulatory Commission (Commission or FERC) had taken steps to ensure the Critical Infrastructure Protection (CIP) cyber security standards were developed and approved, such standards did not always include controls commonly recommended for protecting critical information systems. In addition, the CIP standards implementation approach and schedule approved by the Commission were not adequate to ensure that systems-related risks to the Nation's power grid were mitigated or addressed in a timely manner. Despite their importance to protecting the power grid, the CIP standards did not include a number of security controls commonly recommended for government and industry systems, including both administrative and mission-related systems. These problems existed, in part, because the Commission had only limited authority to ensure adequate cyber security over the bulk electric system. While the Energy Policy Act established the Commission's authority to approve, remand, or direct changes to proposed reliability standards, the Commission did not have the authority to implement its own reliability standards or mandatory alerts in response to emerging threats or vulnerabilities.

U.S. Government Accountability Office Report

- *Electricity Grid Modernization* (GAO-11-117, January 2011). The National Institute of Standards and Technology (NIST) had developed and issued, in August 2010, a first version of its Smart Grid cyber security guidelines. The agency developed the guidelines – for entities such as electric companies involved in implementing Smart Grid systems – to provide guidance on how to securely implement such systems. However, NIST did not address the risk of attacks that use both cyber and physical means. In addition, NIST identified other key elements that surfaced during its development of the guidelines that need to be addressed in future guideline updates. Until the missing elements are addressed, there is an increased risk that Smart Grid implementation will not be secure as otherwise possible. In addition, FERC began, in 2010, a process to consider an initial set of Smart Grid interoperability and cyber security standards for adoption, but had not developed a coordinated approach to monitor the extent to which industry is following these standards. While the *Energy Independence and Security Act of 2007* gave FERC authority to adopt Smart Grid standards, it did not provide FERC with specific enforcement authority. Additionally, although regulatory fragmentation complicated oversight of Smart Grid interoperability and cyber security, FERC had not developed an approach coordinated with other regulators to monitor whether industry was following the voluntary standards it adopted.

MANAGEMENT COMMENTS

Department of Energy
Washington, DC 20585

November 14, 2011

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

FROM: PATRICIA A. HOFFMAN
ASSISTANT SECRETARY
ELECTRICITY DELIVERY AND ENERGY RELIABILITY

SUBJECT: Response to Office of Inspector General's (IG) Draft Audit Report "The Department's Management of the Smart Grid Investment Grant Program"

The Office of Electricity Delivery and Energy Reliability (OE) appreciates the opportunity to respond to the Office of Inspector General's (IG) Draft Audit Report "The Department's Management of the Smart Grid Investment Grant Program."

Under the Smart Grid Investment Grant (SGIG) program, OE manages $8 billion of taxpayer and private funds. OE takes the responsibility of managing each of the 99 SGIG projects very seriously to ensure that funds are being spent properly and that they are accomplishing their intended purpose: "...to accelerate the modernization of the nation's electric transmission and distribution systems and promote investments in smart grid technologies, tools, and techniques which increase flexibility, functionality, interoperability, cyber-security, situational awareness, and operational efficiency."

OE understands that such a large, important, and complex program requires a level of monitoring and oversight that is much higher than normally applied in typical grant programs. In fact, OE's management processes and procedures for the SGIG program go well beyond standard grant management practices and include specific requirements to help ensure that grant recipients deliver the intended results in a timely and cost-effective manner and with reduced risks for U.S. taxpayers.

OE's responses to the four recommendations in the Audit Report are listed below. In addition, OE is including Attachment 1, which contains supplementary information and raises specific concerns with several of the Audit Report's findings and conclusions.

Recommendation 1: Conduct a review to make a determination as to the allowability of the costs questioned in this report and update program procedures, as needed.

Response: In view of the prior consultations with DOE's Offices of Procurement and General Counsel, OE believes that the decisions to award questioned projects, and allow reimbursement of certain "stranded meter" costs, were based on proper interpretations of the applicable laws and regulations and that OE followed accepted practices for determining allowable costs. (See Attachment 1 for further information.)

Action: OE will conduct a review of these decisions in consultation with DOE's Offices of Procurement and General Counsel. This review will be completed no later than March 30, 2012.

Recommendation 2: Develop and implement an effective methodology for monitoring the SGIG program.

Response: OE believes it is implementing an effective methodology for monitoring the SGIG program. (See Attachment 1 for further information.) OE has taken a number of steps that are significantly more rigorous than those required under DOE regulations for grant management. Examples of these include: (1) submission of monthly versus quarterly progress reports to ensure problems can be identified early, (2) development of performance measurement baselines to track progress, (3) development of risk baselines and logs to ensure recipients are implementing effective risk mitigation strategies, (4) performance of onsite reviews to verify first hand that projects are performing work according to plans, (5) provision of federal funding on a cost reimbursement basis after the work has been performed and verified rather than providing the funding in advance, and (6) use of routine and on-going interactions with the recipients by the Technical Project Officers (TPO) to augment monthly reviews of reports and invoices. This approach was captured in the Program Management Plan (PMP) developed in 2010 from the onset of the Program.

Action: OE will review its current methodology for monitoring the SGIG program and implement changes to further strengthen the existing SGIG Program Management Plan, as appropriate, by no later than March 30, 2012

Recommendation 3: Ensure that grantees' cyber security plans are complete, including thorough descriptions of potential security risks and related mitigation through necessary cyber security controls.

Response: OE has developed a cyber security approach that is intended to improve cyber security practices and ensure that recipients do not place the power system at risk. (See Attachment 1 for further information.) While there are mandatory cyber security standards for the bulk electric system, there are no federal or state cyber security standards or regulations that define cyber processes or practices for electric distribution systems.

To make sure the recipients take cyber security seriously even when formal rules do not exist, DOE requires each project to develop a cyber security plan (CSP), have it signed by corporate officers or similar officials, have it reviewed by OE cyber security experts, and then have it approved by the TPO. The intent of OE's requirement for recipients to develop CSPs is to document cyber security methodologies and approaches in sufficient detail to understand the overall approach but retain flexibility to meet the unique aspects of each project. OE's management approach starts with the CSP but continues as an on-going process throughout the life cycle of each SGIG project.

Action: OE will continue to ensure that the cyber security plans of the recipients are complete and are being implemented properly. OE is in the process of conducting a review of all of the reports from the on-site reviews and will require recipients to update their CSPs, as appropriate, no later than April 30, 2012.

Recommendation 4: Ensure that Technical Project Officers (TPOS) are adequately trained and certified to manage the grants under their purview.

Action: OE will have all of the TPOs trained and certified at the TPO II level by no later than September 30, 2012.

Should you have any questions, please contact me at (202) 586-1411 or Stacy Byrd at (202) 586-5370.

Attachment

IG Report No. OAS-RA-12-04

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

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

This page intentionally left blank.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://energy.gov/ig

Your comments would be appreciated and can be provided on the Customer Response Form.