Office of Inspector General

OFFICE OF TECHNOLOGY, FINANCIAL, AND ANALYTICS

INSPECTION REPORT -

ALLEGATIONS RELATED TO THE OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

DOE-OIG-21-29
July 2021

Department of Energy
Washington, DC 20585

July 7, 2021

Memorandum for The Secretary

From: Teri L. Donaldson
Inspector General

Subject: Inspection Report on "Allegations Related to the Office of Cybersecurity, Energy Security, and Emergency Response"

Highlights

What We Reviewed and Why

The Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) was established in 2018 to protect the reliable flow of energy to Americans from emerging threats by improving energy infrastructure security and to support the Department's national security mission. CESER is comprised of two divisions: the Infrastructure Security and Energy Restoration Division leads efforts to secure the Nation's energy infrastructure against all hazards, reduce the impact of disruptive events, and respond to and facilitate recovery from energy disruptions in collaboration with state and local governments and industry partners; and the Cybersecurity for Energy Delivery Systems Division mitigates the risk of energy disruption from cybersecurity incidents and other emerging threats within the energy environment. CESER received $120 million in fiscal year 2019 and $156 million in fiscal year 2020 and has requested approximately $185 million for fiscal year 2021.

In late 2019, the Office of Inspector General received multiple complaints related to CESER. For the purposes of this inspection, we summarized the details of the complaints into four allegations. Specifically, it was alleged that CESER lacked internal control policies and procedures and a full-time staff to oversee its budget. In addition, the Office of Inspector General received allegations that $7.5 million in CESER funds were allocated to Idaho National Laboratory (INL) to finance a startup company; software licenses purchased at a cost of up to $2.2 million were not used; and $2 million in CESER funds were inappropriately spent to update a General Services Administration (GSA) web portal. We conducted this inspection to determine the facts and circumstances surrounding the allegations related to CESER.

What We Found

Our review substantiated certain allegations related to CESER's management. In particular, we fully substantiated two of the allegations. Although we did not substantiate the remaining allegations, we did question the use of funds related to CESER's activities. We determined the following regarding each of the allegations:

- We substantiated that there was a lack of internal controls established for CESER even though the office received more than $275 million since its inception. Specifically, we found that written internal control policies and procedures were not developed for CESER to help ensure appropriate funds management. Further, a workforce management plan had not been developed, which could have guided the hiring of full-time budget personnel to oversee expenditures. These issues were particularly concerning because CESER's September 2019 Assurance Memo, which is required by the *Federal Managers' Financial Integrity Act*, asserted that CESER internal controls were operating effectively.

- We substantiated that CESER purchased $2.1 million in cybersecurity data analysis software licenses which were to be used to monitor utility companies. Because some of the licenses purchased were utilized as part of a 1-month pilot project, we were unable to substantiate the portion of the allegation that none of the licenses were used. While the licenses were purchased over the alleged time period, we identified that only a limited number of the licenses were provided to monitor utility companies more than a year after acquiring the software. However, there was a lack of industry interest in using the software, and ultimately the licenses were not used. As such, we determined that CESER had spent $2.1 million more than necessary for unused software.

- Although we determined that funds were provided to INL, we did not substantiate the allegation that they were used to fund a startup company. Specifically, we determined that $7.5 million in CESER funds were allocated to INL to further develop the Cyber Analytics Tools and Techniques program, which sought to enhance CESER's capability to analyze publicly accessible energy sector internet protocol addresses and determine if there was communication with malicious or suspect threat actors. However, we did not substantiate that the funds provided to INL were used to finance a startup company. While $4 million of the funds were returned to the Department's Office of the Chief Financial Officer after a change in management within CESER in February 2020, the project was being reconsidered near the end of our review. However, management indicated that this effort was paused pending completion of our review.

- We did not substantiate that $2 million was spent on updates to the GSA login.gov web portal. However, we determined that $2 million was allocated for an Interagency Agreement between CESER and GSA to provide consulting and implementation work from the login.gov team of engineers, designers, and product managers to improve user integration with the Cyber Analytics Tools and Techniques program. Despite the use of a

portion of the allocated CESER resources, a CESER official stated that the program remained non-operational at the time of our review. Therefore, we questioned the use of more than $128,000 in expenditures by CESER.

The issue we identified, related to the lack of established internal controls, was due, in part, to a lack of prioritization of this task. In particular, despite concerns being raised by several program officials, senior CESER management had not taken action to establish program-level internal controls, such as policies and procedures. In addition, senior management within CESER did not fully utilize support from other organizations, such as the Office of Electricity, which could have enhanced the control environment. The lack of program-level internal controls also contributed to identified weaknesses related to software acquisitions, the direction of program funds, and contracting for GSA services prematurely. Had adequate controls been implemented, the weaknesses could have been identified and actions taken to ensure activities were conducted in accordance with laws and regulations.

Overall, our review found that CESER spent approximately $2.2 million more than necessary related to the information technology acquisitions and services highlighted in the allegations. In addition, the program allocated $7.5 million for services without the appropriate controls in place to ensure it was the best use of taxpayer funds. To its credit, a number of positive actions have been taken within CESER since February 2020. For instance, CESER did not renew the data analysis software when the period of performance expired in November 2020. In addition, CESER has taken steps to improve its internal control structure. However, without additional improvements, many of the weaknesses identified during our review may continue to persist.

What We Recommend

We made four recommendations in our report designed to improve the management of CESER. Specifically, we recommended that the Acting Assistant Secretary for CESER: (1) develop and implement an internal control program that includes documented policies and procedures related to areas such as contract and financial management, procurement, and staffing; (2) ensure that Federal and Department procurement requirements are followed related to areas such as acquisition of commercial software licenses, contract management, and the use of Interagency Agreements; (3) evaluate and determine whether GSA's login.gov services should be utilized within CESER and, if not, ensure that funds are returned to CESER; and (4) ensure the Department's Office of the General Counsel has access to all meetings related to CESER's procurement process and a concurrence role when program decisions deviate from Federal requirements or Office of the General Counsel's advice.

Management Comments

Management concurred with the report's recommendations and indicated that it had initiated or planned corrective actions to address issues identified in the report. Management's comments and our responses are summarized in the body of the report. Management's formal comments are included in Appendix 4.

cc: Deputy Secretary
Chief of Staff
Chief Information Officer
Acting Chief Financial Officer

Table of Contents

Background and Objective 1

Results of Review

- Internal Controls 2
- Software Acquisitions 3
- Direction of Funds to a Startup Company 4
- Direction of Funds to the General Services Administration 4

Program Management 5

Impact to the Department 6

Recommendations 7

Management Comments 8

Office of Inspector General Response 8

Appendices

1. Commonly Used Terms 9
2. Objective, Scope, and Methodology 10
3. Related Report 11
4. Management Comments 12

Background and Objective

Background

Established in 2018, the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) addresses emerging threats to the Nation's critical energy infrastructure while helping to protect the reliable flow of power. CESER's mission is to lead the Department's emergency preparedness and coordinated response to disruptions to the energy sector, including physical and cyberattacks, natural disasters, and man-made events. In March 2019, a Memorandum of Agreement was executed between CESER and the Department's Office of Electricity. Under the Agreement, the Office of Electricity would provide financial, administrative, procurement, and human resources support to CESER until the newly established office was fully staffed with functional leads. This agreement concluded on September 30, 2019, at which time CESER assumed full operational responsibility.

To accomplish its mission, CESER is organized into two divisions: the Infrastructure Security and Energy Restoration Division leads efforts to secure the Nation's energy infrastructure against hazards, reduce the impact of disruptive events, and respond to and facilitate recovery from energy disruptions in collaboration with state and local governments and industry partners; and the Cybersecurity for Energy Delivery Systems Division mitigates the risk of energy disruption from cybersecurity incidents and other emerging threats within the energy sector. CESER received funding of $120 million in fiscal year (FY) 2019 and $156 million in FY 2020 and has requested approximately $185 million for FY 2021.

In late 2019, the Office of Inspector General received multiple complaints related to CESER. For the purposes of this inspection, we summarized the details of these complaints into four allegations. Specifically, it was alleged that CESER lacked internal controls, such as policies and procedures, and a full-time staff to oversee its budget. In addition, the Office of Inspector General received allegations that $7.5 million in CESER funds were allocated to Idaho National Laboratory (INL) to finance a startup company; software licenses purchased at a cost of up to $2.2 million were not used; and $2 million in CESER funds were inappropriately spent to update a General Services Administration (GSA) web portal.

Report Objective

We conducted this inspection to determine the facts and circumstances surrounding the allegations related to CESER.

Results of Review

Our review substantiated certain allegations related to CESER's management. In particular, we fully substantiated two of the allegations. Although we did not substantiate the remaining allegations, we did question the use of funds related to CESER's activities. Details regarding our findings related to each of the allegations are discussed throughout the report. In addition, we have made recommendations related to improving internal controls within the CESER program.

Internal Controls

We substantiated that there was a lack of internal controls, such as policies or procedures, developed to ensure CESER funds were managed appropriately. At the time of our inspection, CESER had received more than $275 million since its inception in 2018, yet CESER had no documented internal controls over obligating and expending those funds. Although required, CESER officials had not documented program-level controls to provide reasonable assurance that obligations and costs complied with applicable laws, and that funds, property, and other assets were safeguarded against waste, loss, unauthorized use, or misappropriation. For instance, a workforce management plan had not been developed that could have guided the hiring of budget personnel to oversee expenditures. At the time of our review, both current and former CESER officials stated that the Office of Electricity's internal control policies and procedures were implemented upon CESER's inception in accordance with the Memorandum of Agreement executed between the two organizations. However, despite multiple requests to CESER, we were not provided any internal control policies or procedures, including those from the Office of Electricity. According to the *Federal Managers' Financial Integrity Act of 1982,* internal controls are to be established in accordance with the U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government*. Those standards prescribe that management is responsible for designing and implementing internal control policies and procedures to safeguard assets and respond to risks in the internal control system.

During our review, a CESER official provided the FY 2019 *Risk Profile* for CESER, which was finalized in March 2019. The primary purpose of the risk profile was to provide an analysis of the risks that the organization faced in achieving its objectives arising from its activities and operations, and to identify appropriate options for addressing such risks. The risk profile identified contract, project, financial, and workforce management as "high" or "very high" risk for impairing CESER's ability to achieve one or more of its objectives. In response, the risk profile included CESER's strategy to reduce risks by evaluating its internal controls. Despite the risks, internal control policies and procedures were not developed.

In addition, operational deficiencies were identified by the Office of Electricity prior to ending its support for CESER's operations on September 30, 2019. For example, the lack of Federal leads for budget formulation and human capital were identified as critical deficiencies in the organization. The Government Accountability Office's *Standards for Internal Control in the Federal Government* states that organizations should select an oversight body who should have specialized skills, such as financial and budgetary expertise, as well as expertise in human capital management. In August 2019, CESER staff expressed concerns regarding the organization's ability to operate in the future. Of particular concern was the lack of staff to support budget and

human capital functions. At the time of our review in August 2020, CESER staffing remained a concern with many key positions, including budget, which was being performed by non-permanent staff detailed to CESER. Without permanent Federal leads in budget positions, officials could not ensure that sustainable support for CESER existed.

The issues we identified related to a lack of internal controls were particularly concerning because CESER's September 2019 Assurance Memo, which is required by the *Federal Managers' Financial Integrity Act of 1982*, asserted that CESER internal controls were operating effectively, contrary to our findings. For instance, the Memo specifically affirmed there was reasonable assurance that internal controls over operations, reporting, and compliance were working effectively. However, we concluded that the lack of an accurate assessment of internal controls directly impacted the effectiveness and efficiency of CESER's operations and resulted in non-compliance with laws and regulations.

Software Acquisitions

We substantiated that CESER purchased $2.1 million in cybersecurity data analysis software licenses which were to be used to monitor utility companies. Because some of the licenses were utilized, we were unable to substantiate the portion of the allegation that none of the licenses were used. Specifically, the complaint indicated that CESER made an initial $1 million purchase of BitSight[1] licenses for a 1-year period in 2018 but that none of the licenses were used during the first year. The same complaint asserted another planned expenditure of $1 million to renew the licenses in 2019. We received a second complaint indicating a similar situation where the licenses were purchased for a second year even though none of the licenses were used. While we found that the 3,500 licenses purchased were not used in the first year, the complaints that none of the licenses were used in the second year were not fully accurate. In particular, we determined that although $2.1 million was spent on the licenses over a 2-year period, none of the licenses were issued during the first year. During the second year, more than half of the 3,500 licenses were issued, but according to a CESER official, the licenses were actively used for only 1 month in early 2020. As such, we determined that CESER spent $2.1 million more than necessary for unused software.

CESER management commented that the software licenses were acquired to support a pilot project to provide energy sector cybersecurity analysts with access to the BitSight cybersecurity ratings platform for reporting and analytics across the entire energy sector. However, officials indicated that CESER underestimated the hesitation of energy sector participants to monitor information and agreed there was limited use of the licenses by potential users. A CESER official stated the licenses were only used during a 1-month period in early 2020 because of a lack of cybersecurity analysts to monitor the utilities. Based on our test work, we concluded that had CESER identified the need for BitSight services prior to purchasing the licenses, including acceptance and use by industry partners, the $2.1 million would have proven unnecessary. Federal Acquisition Regulation (FAR), Subpart 12.1, *Acquisition of Commercial Items – General*, requires agencies to describe the need for commercial products or services in enough

[1] BitSight is a commercially available cybersecurity ratings technology company that continuously analyzes publicly available data to generate cybersecurity risk ratings based on observed data and practices. The ratings and the associated information behind them can be used by organizations to manage their own cybersecurity risk.

detail to explain how the product or service would be used in terms of functions to be performed, performance requirements, or essential physical characteristics. Describing the agency's needs in these terms allows offerors to propose methods that would best meet the Government's needs. We noted that a need description for the licenses was documented in a draft project plan in January 2019, after the initial purchase of the licenses. However, that plan was never finalized.

Direction of Funds to a Startup Company

Although we determined that CESER funds were provided to INL, we did not substantiate the allegation that they were used to finance a startup company. In particular, we identified that $7.5 million was allocated to INL in September 2019 to further develop CESER's Cyber Analytics Tools and Techniques (CATT) program. The CATT program sought to enhance CESER's capability to analyze publicly accessible energy sector internet protocol addresses and determine if there was communication with malicious or suspect threat actors. Voreas Laboratories Incorporated (VLI) used technology developed by the Defense Advanced Research Projects Agency to generate information concerning malicious cyberattacks. Ultimately, CESER officials established a statement of work with VLI in November 2019 to support the efforts of the CATT program.

In February 2020, a CESER official determined that there was no need to further pursue the use of the technology developed by the Defense Advanced Research Projects Agency and approved a partial return of the funds directed to INL for VLI's services to the Department's Office of the Chief Financial Officer. CESER only de-obligated $4 million of the original amount and, according to an INL official, the remaining $3.5 million continued to be available to other vendors to support the CATT program. In response to our findings, officials indicated that CESER requested INL to restart its project and noted that it will conduct due diligence before making any procurement decisions. Ultimately, VLI was chosen as the subcontractor to support the project, and $4 million was re-allocated for VLI's services in September 2020. However, during a recent meeting, CESER officials stated this effort has been stopped due to our investigation.

In September 2020, when CESER officials updated the VLI statement of work, we determined that it did not meet FAR requirements for fair and open competition. Specifically, the statement of work did not include cost estimates or a determination by the contracting officer that the anticipated cost to the Government will be fair and reasonable. In addition, the contracting officer did not certify that the justification was accurate and complete to the best of their knowledge and belief. The Office of the General Counsel (General Counsel) also expressed concerns regarding competition requirements in January 2021, which were consistent with concerns they had expressed as far back as October 2019.

Direction of Funds to the General Services Administration

We did not substantiate that $2 million was spent on updates to the GSA login.gov web portal. However, we determined that $2 million was allocated for an Interagency Agreement between CESER and GSA to provide consulting and implementation work from the login.gov team of engineers, designers, and product managers to improve user integration with the CATT program. Based on our review, we identified an opportunity for improvement related to how CESER

allocated the funds to GSA. According to the Office of Management and Budget's *Office of Federal Procurement Policy* guidance*, Interagency Acquisitions*, agencies should exercise sound business discretion to maximize benefits when using interagency acquisitions to meet their mission needs. In this instance, CESER, the requesting agency, was required to demonstrate a *bona fide* need for the acquisition requested. Although CESER officials indicated that login.gov authentication services were needed to support the CATT program, a former CESER official stated that the program remained non-operational at the time of our review. While authentication services may have eventually been necessary, the obligation was premature when it occurred. In addition, a CESER official stated that the cybersecurity data analysis software licenses were also accessed through the GSA web portal, even though the Interagency Agreement between CESER and GSA was for user integration with the CATT program. CESER management indicated that this effort has been stopped and nearly $1.9 million remains available.

Program Management

The identified weakness related to the lack of established internal controls was due, in part, to a lack of prioritization of this task. In particular, we spoke to several officials involved with CESER at the time who stated that they had raised concerns regarding the need for internal controls, such as policies and procedures, but senior management had not taken action to establish such controls. In addition, support from other organizations that could have enhanced the control environment was not fully utilized. For example, although CESER had Office of Electricity officials on detail assignments, their advice was not utilized to develop internal controls to ensure CESER's programs were properly managed.

The lack of internal controls noted above was a significant contributor to the identified weaknesses related to expenditures for software acquisitions, GSA services, and the allocation of CESER funds. Although high-risk practices were identified, CESER did not take actions to implement internal controls, such as policies and procedures, to ensure compliance with governing laws and regulations. To its credit, the Department's General Counsel expressed concern over CESER's procurement process, which could have exposed the Department to legal risks. For instance, when CESER planned to acquire VLI's services, General Counsel officials warned CESER management that the procurement did not meet standards for a sole-source contract, such as preparing a request for proposal and following requirements for full and open competition. CESER management responded to our preliminary draft report, stating VLI had the exclusive technology required for the CATT program, so competition was not required. While we agree with this statement, the sole-source justification provided by CESER did not meet FAR requirements to support the decision. In addition, General Counsel informed CESER of legal risks associated with the VLI subcontract's proposed scope. However, these legal concerns did not appear to impact the direction of the CESER program. Finally, a General Counsel official informed us that they initially attended weekly meetings with CESER senior management to discuss legal implications of program decisions. However, General Counsel was eventually excluded from those meetings. In response to our review, CESER and General Counsel officials confirmed that General Counsel is now included in meetings to advise on the legal implications of program decisions.

Impact to the Department

Overall, our review found that CESER spent approximately $2.2 million more than necessary related to the information technology software acquisitions and services highlighted in our report. In addition, CESER allocated $7.5 million for services without the appropriate controls in place to ensure it was the best use of taxpayer funds. To its credit, CESER management has taken a number of positive actions related to acquisitions beginning in February 2020. For instance, the cybersecurity data analysis software licenses were not renewed when the period of performance expired in November 2020. In addition, management indicated that it plans to enhance internal controls by establishing a Financial Management division which, when fully staffed, should help address some of the issues we identified that were related to management of CESER's funds. CESER officials also provided recently developed internal control policies and procedures in response to our review. These actions are encouraging and, when fully implemented, should address many of our report's concerns.

However, without additional improvements, such as the development and implementation of an effective internal control program, many of the weaknesses identified during our review may continue to persist. Notably, a CESER official stated that the update to the organization's mission and function statements was recently completed as a part of a strategic planning process that includes staffing plans. This strategic planning process is ongoing and expected to be implemented in FY 2021.

Recommendations

To improve the management of the CESER program, we recommend that the Acting Assistant Secretary for CESER:

1. Develop and implement an internal control program that includes documented policies and procedures related to areas such as contract and financial management, procurement, and staffing.

2. Ensure that Federal and Department procurement requirements related to areas such as acquisition of commercial software licenses, contract management, and the use of Interagency Agreements are followed.

3. Evaluate and determine whether GSA's login.gov services should be utilized within CESER. If a determination is made not to use GSA's login.gov services, ensure that funds are returned to CESER.

4. Ensure the Department's General Counsel has access to all meetings related to CESER's procurement process and a concurrence role when program decisions deviate from Federal requirements or General Counsel's advice.

Management Comments

Management concurred with the report's recommendations and indicated that it had planned and initiated corrective actions to address issues identified during our review. For example, management stated that it recognizes the lack of internal controls to be a major concern and indicated that CESER had taken several actions to address this issue. Management also indicated that it will ensure due diligence prior to procurement decisions. In addition, management commented that it will ensure that unused funds from procurement actions will be returned if projects are terminated. Further, management noted that it is now routine practice to request General Counsel review, advice, and guidance on budget documents, procurement transactions, and changes that will impact the organizational structure. Throughout its comments, management indicated that many of the issues identified during our review occurred under previous CESER leadership.

Office of Inspector General Response

Management's comments and planned corrective actions were responsive to our recommendations. Management's comments are included in Appendix 4.

Appendix 1

Commonly Used Terms

Cyber Analytics Tools and Techniques	CATT
Department of Energy	Department
Federal Acquisition Regulation	FAR
Fiscal Year	FY
General Services Administration	GSA
Idaho National Laboratory	INL
Office of Cybersecurity, Energy Security, and Emergency Response	CESER
Office of the General Counsel	General Counsel
Voreas Laboratories Incorporated	VLI

Appendix 2

Objective, Scope, and Methodology

Objective

We conducted this inspection to determine the facts and circumstances surrounding the allegations related to the Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

Scope

The inspection was performed from March 2020 through February 2021. Our review covered allegations made against the CESER program in early fiscal year 2020 related to internal controls, contract management, and acquisition of goods and services. The inspection was conducted under Office of Inspector General project number S20TG012.

Methodology

To accomplish our inspection objective, we:

- Reviewed applicable laws, regulations, and directives related to contract management;
- Reviewed relevant reports issued by the Office of Inspector General and the Government Accountability Office;
- Held discussions with former and current officials from CESER; and
- Reviewed documentation pertaining to the allegations made against the CESER program, including obligating documents, electronic mail, purchase order and invoice documents, and a subcontract statement of work.

We conducted this allegation-based inspection in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. Those standards require that we plan and perform the inspection to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our inspection objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our inspection objective. Accordingly, we assessed significant internal controls and compliance with laws and regulations to the extent necessary to satisfy the inspection objective. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our inspection. Finally, we relied on computer-processed data and determined that the data provided was sufficiently reliable to support our decisions and recommendations.

An exit conference was held with management on May 27, 2021.

Appendix 3

Related Report

Government Accountability Office

- *CRITICAL INFRASTRUCTURE PROTECTION - Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid* (GAO-19-332, August 2019). This report described the cybersecurity risks facing the grid, assessed the extent to which the Department of Energy had defined a strategy for addressing grid cybersecurity risks, and assessed the extent to which Federal Energy Regulatory Commission approved standards addressing grid cybersecurity risks. The Government Accountability Office found that the electric grid faced significant cybersecurity risks, including terrorist attacks on the grid. In addition, industrial control systems that support grid operations were becoming more vulnerable to cyberattacks. While recent Federal assessments indicated that cyberattacks could cause widespread power outages in the United States, the scale of power outages that may result from a cyberattack was uncertain due to limitations in those assessments.

Management Comments

Management Response
OIG Final Report: "Allegations Related to the Office of Cybersecurity, Energy Security, and Emergency Response, S21TG012"
March 30, 2021

Transmittal Letter Input

MEMORANDUM FOR TERI L. DONALDSON
INSPECTOR GENERAL

FROM: PUESH M KUMAR
Puesh M. Kumar
Digitally signed by Puesh M. Kumar
Date: 2021.06.11 18:26:22 -04'00'
ACTING PRINCIPAL DEPUTY ASSISTANT SECRETARY
OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

SUBJECT: Draft Inspection Report on "Allegations Related to the Office of Cybersecurity, Energy Security, and Emergency Response, S21TG012"

Thank you for the opportunity to review and comment on the subject draft report. The Office of Cybersecurity, Energy Security, and Emergency Response (CESER) appreciates the auditors' audit work and provides the following comments below:

- CESER concurs with the positive benefits of continuing to strengthen the internal control program, including policies and procedures.
- CESER concurs with ensuring that Federal and Departmental procurement requirements are followed.
- CESER concurs with continuing to have the Department's General Counsel involved with program meetings – as they have on a weekly basis.

The attachment to this memorandum details actions planned to be taken by CESER in response to the recommendations listed in the draft report.

If you have any questions regarding this response, please contact Marsha L. Manning, Chief Operating Officer, the Office of Cybersecurity, Energy Security, and Emergency Response, at marsha.manning@hq.doe.gov, or Ian Moore, Audit Coordinator, the Office of Cybersecurity, Energy Security, and Emergency Response, at ian.moore@hq.doe.gov.

Enclosure

Enclosure

Management Response
OIG Final Report: "Allegations Related to the Office of Cybersecurity, Energy Security, and Emergency Response, S21TG012"

Recommendation #1: Establish and implement an internal control program that includes documented policies and procedures related to areas such as contract and financial management, procurement, and staffing.

DOE Response: Concur

The U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) recognizes the lack of internal controls, including policies and procedures and a full-time staff to oversee its budget, as a significant concern. A relatively new office, currently in its second year as a standalone program, CESER has taken several actions to address this issue.

The OIG report found that CESER's lack of internal controls was due, in part, to the fact that the function was not a priority for previous CESER leadership. The report also determined that, despite the fact that concerns were raised by several career staff, CESER leadership at the time did not take the necessary actions to establish program-level internal controls. Current CESER leadership is prioritizing these activities and remains committed to improvement through critical hiring and implementation of appropriate budget controls.

Specific actions taken to address the concerns include establishing internal controls throughout the financial management process. Standard Operating Procedures (SOPs) were established to include the development of Annual Operating Plans (AOPs), Spending Plans, and a detailed approval process for the execution of appropriated funds. To develop plans and monitor the execution of funds, CESER adopted the utilization of the Corporate Planning System (CPS). CPS is designed to track spending for individual projects across CESER. CPS has an internal electronic signature process with multiple levels of approval required prior to the execution of funds. In addition to technical experts and program managers approving the distribution of funds, CPS requires the Budget Analyst, as well as the Deputy Assistant Secretary (or proxy), to approve the use of the funding for each effort. This approval process includes detailed guidance documentation that is distributed to the field recipients to obligate funding. The implementation of these procedures includes documentation of senior leadership direction and approval at multiple levels to mitigate the risk of inappropriate use of funds and to increase transparency. CESER supported expanding the capabilities of the Office of Energy Efficiency and Renewable Energy Data Center (EDC). The EDC is a repository for data generated and maintained in CPS, Standard Accounting and Reporting System (STARS), and other business systems for DOE. The information fed into the EDC is used to generate dashboards, reports, and graphics to summarize the status of activities within CESER. The goal of this system is to provide a single point of current financial information for program managers and their support teams to assist in the monitoring and management of their portfolios of projects. Users can open this report at any time to see the most up-to-date information about their projects.

All CESER funds are managed at the Control-Parent level (Infrastructure Security & Energy Restoration (ISER), Cybersecurity for Energy Delivery Systems (CEDS), and Program Direction). Funds are not distributed to lower control points until ready for use. This minimizes the possibility of improperly allocating funds.

Enclosure

Management Response
OIG Final Report: "Allegations Related to the Office of Cybersecurity, Energy Security, and Emergency Response, S21TG012"

Recommendation #2: Ensure that Federal and Department procurement requirements related to areas such as acquisition of commercial software licenses, contract management, and the use of interagency agreements are followed.

DOE Response: Concur

CESER engaged in a pilot project to provide energy sector cybersecurity analysts with access to the BitSight cybersecurity ratings platform for reporting and analytics across the entire energy sector to support shared situational awareness of cybersecurity vulnerabilities in the sector. The effort was set to begin with the electricity and natural gas subsectors and then expand to the broader energy sector. Analysis of trends and identified vulnerabilities and deficiencies were to be enabled through BitSight reports and details about individual utilities available in DOE's instance of BitSight.

DOE was to evaluate feedback from the initial pilot to determine if changes to the structure of the program were needed. This effort would then expand the effort to the broader energy sector as appropriate. To that end, CESER purchased 3,500 "monitoring licenses." Of those, 2,004 of the monitoring licenses were actively used to inform threat intelligence information about the U.S. energy sector.

CESER asserts that 9 users were active using the 2,004 monitoring licenses issued, and the difference between 3,500 and 2,004 is the number that should be used by the Office of the Inspector General for assessing "unused software" costs. The unused licenses were going to be used for suppliers, manufacturers, and other companies who support the U.S. energy sector to support sector-wide situation awareness.

Ultimately, previous CESER leadership stopped the effort in its entirety and therefore the additional licenses were never used. Current CESER leadership also does not intend to renew that pilot program.

Estimated Completion Date: On-going exercise

Enclosure

Management Response
OIG Final Report: "Allegations Related to the Office of Cybersecurity, Energy Security, and Emergency Response, S21TG012"

Additionally, CESER has expanded its Budget and Financial Management permanent staff. Three budget analysts have been hired. Two of the analysts are certified Contracting Officer's Representatives (CORs). CESER has also hired a Senior Procurement Analyst to oversee the procurement activities. CESER is committed to ensuring financial documents undergo a thorough multi-step approval process. For example, DOE's Strategic Integrated Procurement Enterprise System (STRIPES) requires the Chief Operating Officer, Budget Approver, and Requisitioner to sign off on documents prior to their submission to the Contracting Office for review and execution.

These actions were taken to build the foundation for the establishment of an official Internal Controls process.

Estimated Completion Date: On-going Exercise

Enclosure

Management Response
OIG Final Report: "Allegations Related to the Office of Cybersecurity, Energy Security, and Emergency Response, S21TG012"

Recommendation #3: Evaluate and determine whether GSA's login.gov services should be utilized within CESER. If a determination is made not to use GSA's login.gov services, ensure that funds are returned to CESER.

DOE Response: Concur

CESER appropriately entered into an Inter-Agency Agreement (IAA) with the General Services Administration (GSA) with a period of performance for October 1, 2019 through September 30, 2021. CESER had integrated its digital services with the login.gov platform and required additional assistance from the login.gov team. CESER required consulting and implementation work from the login.gov team to improve user experience flow and integration with its CATT 2.0 program. The login.gov team consists of experienced engineers, designers, and product managers who develop and operate the login.gov product and platform. This gives them significant relevant expertise in implementing a user-centered design.

The aforementioned funding action and subsequent approval was submitted and approved through an agency policy process using an IAA. Due to changes in previous CESER leadership, this effort has been stopped. Of the $2,000,000 provided for use, $1,871,351 remains available. CESER requested that DOE's National Energy Technology Laboratory (NETL) review the IAA documentation between DOE/NETL and GSA for the award 89243319SFE000009 dated 9/30/2019. NETL legal counsel completed the requested review and replied that, based on information provided, no apparent deviations from applicable law and policy were noted.

Estimated Completion Date: FY2021

Enclosure

Management Response
OIG Final Report: "Allegations Related to the Office of Cybersecurity, Energy Security, and Emergency Response, S21TG012"

Recommendation #4: Ensure the Department's General Counsel has access to all meetings related to CESER's procurement process and a concurrence role when program decisions deviate from Federal requirements or General Counsel's advice.

DOE Response: Concur

The OIG report indicates that DOE General Counsel has been excluded from meetings where previously they attended weekly meetings with CESER senior management to discuss legal implications of program decisions. CESER disputes this observation, as CESER continues to hold weekly meetings between CESER leadership and representatives from the Office of General Counsel, including the Deputy General Counsel for Energy Policy and/or the Assistant General Counsel for Electricity and Fossil Energy. It is routine practice for CESER to request General Counsel review, advice and/or guidance on budget documents, procurement transactions, and changes that will impact the organizational structure. However, CESER acknowledges that prior CESER leadership failed to include General Counsel in certain meetings relating to the matters discussed in Sections 2 through 4 of this response. Current CESER leadership has reestablished regular coordination with DOE-GC on all relevant efforts.

Estimated Completion Date: On-going exercise

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 OIG.Reports@hq.doe.gov and include your name, contact information, and the report number. You may also mail comments to us:

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 202–586–1818. For media-related inquiries, please call 202–586–7406.