



U.S. DEPARTMENT OF  
**ENERGY**

Office of  
Inspector General

# SEMIANNUAL REPORT TO CONGRESS

---

*for Period Ending*  
March 31, 2021

# TABLE OF CONTENTS

<b>MESSAGE FROM INSPECTOR GENERAL .....</b>	<b>2</b>
<b>STATISTICAL HIGHLIGHTS</b>	
<i>Investigations .....</i>	<i>4</i>
<i>Audits and Inspections .....</i>	<i>5</i>
<b>POSITIVE OUTCOMES .....</b>	<b>6</b>
<b>TABLE OF REPORTS</b>	
<i>Investigative Outcomes.....</i>	<i>9</i>
<i>Audits.....</i>	<i>11</i>
<i>Inspections.....</i>	<i>14</i>
<b>RESULTS</b>	
<i>Legislative and Regulatory Reviews .....</i>	<i>15</i>
<i>Interference with Inspector General Independence .....</i>	<i>15</i>
<i>Resistance to Oversight Activities or Restricted/Significantly Delayed Access .....</i>	<i>15</i>
<i>Investigations Involving Unauthorized Public Disclosure of Classified Access .....</i>	<i>15</i>
<i>Reviews Closed and Not Disclosed to the Public .....</i>	<i>15</i>
<i>Investigations Involving Senior Government Employees .....</i>	<i>16</i>
<i>Whistleblower Activities .....</i>	<i>16</i>
<i>Hotline Activity .....</i>	<i>17</i>
<i>Comments Not Provided by the Department Within 60 Days .....</i>	<i>17</i>
<i>Reports Lacking Management Decision .....</i>	<i>17</i>
<i>Disagreement with Management Decision .....</i>	<i>17</i>
<i>Recommendations Not Implemented .....</i>	<i>18</i>
<i>Peer Reviews .....</i>	<i>22</i>
<b>SUMMARIES</b>	
<i>Investigative Outcomes.....</i>	<i>23</i>
<i>Audit Reports.....</i>	<i>32</i>
<i>Inspection Reports .....</i>	<i>42</i>
<i>Semiannual Reporting Requirements Index .....</i>	<i>45</i>

## MESSAGE FROM THE INSPECTOR GENERAL

During this reporting period, we passed the 1-year mark of operating in a full telework posture, and I could not be prouder of the Office of Inspector General (OIG) staff for their continued hard work and flexibility. The statistics and positive outcomes displayed in this *Semiannual Report to Congress* show their dedication and how they continued the OIG's mission while taking on additional responsibilities such as childcare, distance learning, and dependent care.

During the reporting period from October 1, 2020, through March 31, 2021, the Office of Audits (OA) continued its primary mission of auditing major Department of Energy programs, projects, and major contractors, while also supporting OIG-wide projects and initiatives. Over the last 6 months, OA completed several projects, resulting in 15 published reports, and continued its work on several projects to assess the Cooperative Audit Strategy. Many of these projects, including our Special Project Report, were recently issued, and will be highlighted in the next reporting period. Additionally, the Department disallowed more than \$8 million of questioned costs previously identified by the OA.

The Office of Investigations (OI) issued 11 investigative reports, referred 38 individuals for prosecution, obtained 6 indictments, and 2 criminal convictions, and initiated 5 civil actions. Our investigators continued to work jointly with other agencies and made several major referrals to the Department of Justice. The invaluable work of OI led to more than \$2 million in recoveries and will continue to deter fraud while helping the Department further its mission.

Inspections, Intelligence Oversight, and Special Projects (OIIS), including the OIG Hotline, issued 3 reports this period, and received more than 1,300 complaints from concerned employees and the public. The Hotline worked closely with the OIG and the Department to ensure all complaints were reviewed and referred for action as necessary. During the reporting period, OIIS also worked closely with OI to support several of their investigative efforts and continued developing a detailed risk assessment of the Department's intelligence mission, as our office increases its oversight capability in this area.

The Office of Technology, Financial, and Analytics (OTFA) continued to make progress with access to systems, and to perform real time analysis of data in support of OIG audits, inspections, and investigations. OTFA also issued reports identifying actions to help strengthen the Department in the areas of vulnerability management, web application integrity, firewall configuration, and end user response to phishing.

I'm also excited to announce that in March of this year, we expanded our administrative remedies capabilities. We welcomed our new Special Counsel for Administrative Remedies who will build our suspension and debarment program and will serve as our lead legal expert on suspension and debarment matters. The new administrative remedies division has already developed cases and provided recommendations on administrative remedies both internally to the OIG and to the Department's Suspension and Debarment Officials.

In closing, I'm so proud of everything our office has accomplished, and excited for what it will continue to accomplish as we move into the second half of the fiscal year and continue our mission on behalf of the Nation.



Teri L. Donaldson  
Inspector General

## STATISTICAL HIGHLIGHTS

### INVESTIGATIONS

#### INVESTIGATIVE ACTIVITIES

Cases Open as of October 1, 2020	198
Cases Opened	59
Cases Closed	36
Cases Open as of March 31, 2021	221
Multi-Agency Joint Cases Opened During Period	9
Qui Tam <sup>1</sup> Investigations Opened During Period	3
Total Open Qui Tam Investigations as of March 31, 2021	13
Total Investigative Reports <sup>2</sup> Issued During Period	11
Administrative Discipline and Other Management Actions	11
Suspensions/Debarments <sup>3</sup>	10
Total Persons <sup>4</sup> Referred to a Prosecuting Authority	38
Department of Justice Referrals	31
State/Local Referrals	7
Referrals Accepted for Prosecution <sup>5</sup>	22
Total Indictments <sup>6</sup> /Criminal Informations	6
Indictments/Criminal Informations Resulting from Prior Period	6
Referrals	6
Criminal Convictions	2
Pre-trial Diversions	0
Civil Actions	5
Dollars Recovered <sup>7</sup> (Fines, Settlements, Recoveries)	\$2,030,027

<sup>1</sup>For more information on Qui Tams, go to:

[http://www.justice.gov/usao/eousa/foia\\_reading\\_room/usam/title9/crm00932.htm](http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00932.htm)

<sup>2</sup>Investigative Reports issued by the Office of Investigations include Reports of Investigation and Investigative Reports to Management.

<sup>3</sup>This number includes proposed debarments issued under the Federal Acquisition Regulation (FAR). We report proposed debarments under the FAR because those actions have the same effect as a debarment or a suspension. Insofar as we are providing these numbers to show the effect of OIG referrals, including debarments proposed under the FAR presents a more complete picture. Please note, however, that proposed debarments under the FAR are not final actions.

<sup>4</sup>Persons is defined as an individual or an entity. For example, two co-owners and their business entity would be counted as three persons.

<sup>5</sup>Some referrals accepted during the 6-month period were referred for prosecution during a previous reporting period.

<sup>6</sup>Sealed Indictments are included.

<sup>7</sup>Some of the money collected was the result of investigations involving multiple agencies.

## STATISTICAL HIGHLIGHTS

### AUDITS AND INSPECTIONS

#### AUDITS AND INSPECTION ACTIVITIES

Total Reports Issued	18
Audit Reports Issued	15
Inspection Reports Issued	3

#### BETTER USE OF FUNDS

	TOTAL NUMBER	BETTER USE OF FUNDS
Reports issued before the reporting period that included recommendations for better use of funds for which decisions on dollars had not been made as of September 30, 2020	3	\$20,900,000
Reports issued during the reporting period that include recommendations for better use of funds (regardless of whether a decision on dollars has been made)	0	\$0
Reports that include recommendations for better use of funds for which a decision on dollars was made during the reporting period	0	\$0
(i) Agreed to by management		\$0
(ii) Not agreed to by management		\$0
Reports that include recommendations for better use of funds for which decisions on dollars have not been made at the end of the reporting period	3	\$20,900,000
<b>Better Use of Funds:</b> Funds that could be used more efficiently by implementing recommended actions. <b>Management Decision:</b> Management's evaluation of the finding and recommendations included in the audit report and the issuance of a final decision by management concerning its response.		

#### QUESTIONED COSTS

	TOTAL NUMBER	QUESTIONED COSTS	UNSUPPORTED COSTS	TOTAL COSTS
Reports issued before the reporting period that included questioned and/or unsupported costs for which decisions on dollars had not been made as of September 30, 2020 <sup>1</sup>	24	\$1,252,464,982	\$261,342,245	\$1,513,807,227
Reports issued during the reporting period that include questioned or unsupported costs (regardless of whether a decision on dollars has been made)	0	\$0	\$0	\$0
Reports that include questioned and/or unsupported costs for which a decision on dollars was made during the reporting period	6	\$40,060,289	\$340,343	\$40,403,632
(i) Value of disallowed costs		\$8,376,441	\$150	\$8,376,591
(ii) Value of costs not disallowed		\$31,686,848	\$340,193	\$32,027,041
Reports that include questioned and/or unsupported costs for which decisions on dollars have not been made at the end of the reporting period	18	\$1,212,401,693	\$261,001,902	\$1,473,403,595
<b>Definitions:</b> <b>Management decision:</b> Management's evaluation of the finding and recommendations included in the audit report and the issuance of a final decision by management concerning its response. <b>Questioned costs:</b> A cost that is (1) unnecessary; (2) unreasonable; or (3) an alleged violation of law, regulation, contract, etc. <b>Unsupported costs:</b> A cost that is not supported by adequate documentation.				

<sup>1</sup>DOE-OIG-18-17: The Department is unable to recover \$2,500,000 in questioned costs due to the bankruptcy of a financial assistance award recipient.

## POSITIVE OUTCOMES

During this reporting period, the Department took positive actions as a result of OIG work conducted during the current or previous periods. Here are some examples:

- ✚ In response to an OIG referral, the National Nuclear Security Administration (NNSA) conducted a review into an allegation that employees with Honeywell Federal Manufacturing & Technologies at the Kansas City National Security Complex, Test Engineering Division, were asked to participate in an inter-department initiative to create "training videos." It was alleged that the manager leading the initiative advised employees to bill their hours to other projects, as there was no specific funding for the initiative. After a subsequent review by NNSA, the incident was substantiated. NNSA determined that the manager did not seek guidance from Program Management and/or the Finance Department and incorrectly instructed all 32 employees to charge their time to direct charge codes, for a direct total cost of \$47,128. In their response, NNSA listed all corrective actions being taken, including cost transfers of \$47,128 from direct to indirect, publishing a knowledge share on indirect vs. direct time charging guidance, and addressing the performance of the managers responsible.
- ✚ As a result of an OIG investigation, a contractor employee at the Pacific Northwest National Laboratory resigned in lieu of termination by the contractor. During an OIG interview, the former contractor employee admitted to intentionally falsifying timecards, leaving work early without taking leave, arriving to work late, and teleworking without evidence of completing work activities. The former contractor employee's timecards included hours charged to a project on which no work had been completed. The former contractor employee had approximately 500 hours that were unaccounted for in a 6-month period. This is an ongoing investigation.
- ✚ As a result of an OIG investigation, a former West Virginia University (WVU) Professor was debarred from receiving Federal funds or contracts for a period of 3 years. An investigation conducted by the Federal Bureau of Investigation (FBI) found that the former professor falsely requested and received a leave of absence from his WVU teaching responsibilities to care for his family, when in fact he was working overseas to meet the requirements of his foreign government talent recruitment plan. The former professor pleaded guilty to one count of Federal Program Fraud and was sentenced to 3 months of imprisonment, 1 year of supervised release, and ordered to pay restitution in the amount of \$20,189 and a fine of \$9,363. An FBI investigation and the subject's guilty plea led to an OIG finding that the former professor was the Principal Investigator on two Department Office of Science awards during the time period of the charged fraudulent activity.
- ✚ Management indicated that it had already taken action to address 24 of the 44 recommendations made in the report on a Department Site's Cybersecurity Program. These actions were related to vulnerability management, web application integrity, firewall configuration, and end user response to phishing.

- ✚ We conducted a joint evaluation with the Department of Defense (DoD) OIG that resulted in each OIG issuing an evaluation report on the Aircraft Monitor and Control (AMAC) system nuclear certification. In our report, we identified that NNSA's oversight of the AMAC system testing requirements for nuclear weapons delivery was impacted by disagreements with the Air Force. Specifically, there was discord between the two Federal entities concerning the number of aircraft to test, as well as changes to test requirements made by the Air Force outside of the AMAC Project Officers Group, which is a joint Air Force and NNSA group that is responsible for defining AMAC system specifications and test criteria. As a result of our report, the Deputy Secretary of Defense for Nuclear Matters and the Assistant Staff Director for the Nuclear Weapons Council met with NNSA, the Department of Energy OIG, and DoD OIG officials to discuss the report recommendations in-depth and provide additional insight. This action is responsive to our recommendation to determine whether the AMAC Project Officers Group should adhere to Department of Defense 5030.55\_Air Force Manual 63-103 requirements to report issues affecting safety, cost, performance, or other significant matters that cannot be resolved at the Project Officers Group level to the Nuclear Weapons Council or its subordinate committees.
  
- ✚ The NNSA issued guidance to its field sites requiring them to periodically review whether their laboratories are receiving and transmitting final Cooperative Research and Development Agreement reports to the Department's Office of Scientific and Technical Information for dissemination to the public. Under the National Competitiveness Technology Transfer Act of 1989, the Department's laboratories are authorized to use Cooperative Research and Development Agreements to facilitate the development and transfer of technology to the general science community, private firms, and the public. Our audit found that the Department and its laboratories had not taken sufficient corrective action to address previously identified weaknesses in the management of final technical reports.
  
- ✚ The Department issued Department Order 224.3A, Audit Coordination, Resolution, and Follow-up, in October 2020. The revised order addressed longstanding issues regarding the Department's Audit Resolution and Follow-up Processes first identified by the OIG in 2010 and reiterated in subsequent reports in 2016 and 2020.
  
- ✚ In response to our FY 20 audit on the Department's Storage and Disposition of Explosives Material at Selected Sites, NNSA, in conjunction with contractors, has begun to take corrective actions to address issues identified during our review. NNSA is in the process of evaluating explosives inventory system requirements across the Enterprise. Additionally, one site is in the process of transitioning from a stand-alone inventory system to a new system that will include integrated tracking through disposition, showing storage of compatible explosives material and Net Explosives Weight. Additionally, NNSA, in conjunction with its Field Offices, is evaluating inventory policies to include container-labeling and visual inspection requirements to support ongoing effectiveness of explosives inventory programs across the complex. Further, NNSA, in coordination with its Field Offices, is evaluating the implementation of storage compatibility procedures to ensure consistent implementation across the complex.



- ✚ During an ongoing inspection, an allegation regarding information related to employees' coronavirus testing, test results, and status was brought to our attention. Specifically, it was alleged that Y-12 Fire Department officials, including medical department personnel, disclosed employees' information without their consent or authorizations, and these disclosures do not fall under any of the exceptions currently in place during the pandemic national emergency. The allegation was referred to NNSA for action. NNSA, in conjunction with the M&O contractor, Consolidated Nuclear Energy, LLC, conducted an investigation and partially substantiated some of the allegations, but determined that no violations of the Privacy Act or the Health Insurance Portability and Accountability Act occurred. The investigation resulted in one recommendation to Consolidated Nuclear Energy, LLC's Office of Health and Safety.
- ✚ One of the recommendations from the *Inspection Report on Mitigation of Risks from Natural Disasters at Lawrence Berkeley National Laboratory* report was to effectively implement existing requirements to notify Berkeley Laboratory's Emergency Management Program when hazardous materials have been approved for procurement at Berkeley Laboratory. Extensive corrective actions for this recommendation were completed on October 7, 2020, when the Bay Area Site Office issued the All-Hazards Planning Basis Program Plan Rev003.

## TABLE OF REPORTS

### INVESTIGATIVE OUTCOMES

All of our investigations that result in a reportable outcome are disclosed to the public in our Semiannual Report. Reportable outcomes are defined as public and nonpublic reports, indictments, convictions, disciplinary actions, monetary recoveries, contractor debarments, and other similar results. The following reportable outcomes occurred from the period from October 1, 2020, through March 31, 2021.

SUMMARY TITLE	PAGE
Sentencing and Indictment in Procurement Integrity Act Investigation	23
Former Department Subcontractor Sentenced in Foreign Corrupt Practices Act Investigation	23
Sentencing in Grant Fraud Investigation	24
Sentencing in Theft of Government Property Investigation	24
Sentencings and Guilty Plea in Theft of Government Property Investigation	24
Guilty Plea and Sentencing for Attempted Burglary	25
Superseding Indictment in Small Business Technology Transfer Fraud Investigation	25
Arrest in Theft of Government Funds Investigation	25
Indictment in Small Business Innovation Research Grant Fraud Investigation	26
Research Professor Arrested for Grant Fraud	26
Indictment in Narcotics Possession Investigation	26
Arrest in Offenses Against Children Investigation	26
Criminal Complaint and Suspensions Filed in Grant Fraud Investigation	26
Former Laboratory Employee Charged in Theft of Government Property Investigation	27
Civil Settlement in Grant Fraud Investigation	27
Settlement Agreement in Grant Fraud Investigation	27
Settlement Agreement in False Claims Act Investigation	28
Civil Settlement Agreement in Civil False Claims Investigation	28

SUMMARY TITLE	PAGE
Civil Settlement Agreement in Civil False Claims Investigation	28
Notice of Termination and Debarment in Theft of Intellectual Property Investigation	28
Debarment in False Statements Investigation	29
Restitution Paid by Former Contractor Employee	29
Employee Terminated in Theft of Government Property Investigation	29
Debarment in Federal Program Fraud Investigation	29
Notice of Suspension in Per Diem Claims Investigation	30
Notice of Termination in Timecard Fraud Investigation	30
Contractor Employee Terminated in Theft of Government Property Investigation	30
Contractor Employee Resigns in Lieu of Termination	30
Recovery of Funds in False Claims Investigation	30
Government Property Seized from Contractor Employee	31

## AUDITS

The following identifies all audit reports issued from October 1, 2020, through March 31, 2021.

DATE ISSUED	REPORT TITLE	NUMBER OF RECS	BETTER USE OF FUNDS	QUESTIONED COSTS	UNSUPPORTED COSTS	PAGE
Oct. 20, 2020	Respiratory Equipment Maintenance at the Portsmouth Site (DOE-OIG-21-01)	6				32
Nov. 16, 2020	Department of Energy Nuclear Waste Fund's Fiscal Year 2020 Financial Statement Audit (DOE-OIG-21-02)	0				32
Nov. 16, 2020	Department of Energy's Fiscal Year 2020 Consolidated Financial Statement Audit (DOE-OIG-21-03)	0				33
Nov. 18, 2020	Management Challenges at the Department of Energy – Fiscal Year 2021 (DOE-OIG-21-04)	0				34
Nov. 20, 2020	Federal Energy Regulatory Commission's Fiscal Year 2020 Financial Statement Audit (DOE-OIG-21-05)	0				34

DATE ISSUED	REPORT TITLE	NUMBER OF RECS	BETTER USE OF FUNDS	QUESTIONED COSTS	UNSUPPORTED COSTS	PAGE
Dec. 14, 2020	<p>Management of a Department of Energy Site Cybersecurity Program (DOE-OIG-21-07)</p> <p><i>This report is Official Use Only and not available for public viewing.</i></p>	55				35
Dec. 14, 2020	<p>Contingency Planning Efforts for Information Technology Mission Support Systems at Selected Department of Energy Locations (DOE-OIG-21-08)</p>	2				36
Dec. 21, 2020	<p>Management Letter on the Federal Energy Regulatory Commission's Fiscal Year 2020 Financial Statement Audit (DOE-OIG-21-09)</p> <p><i>This report is Official Use Only and not available for public viewing.</i></p>	2				37
Jan. 5, 2021	<p>Management Letter on the Department of Energy's Fiscal Year 2020 Consolidated Financial Statements (DOE-OIG-21-11)</p>	14				37

DATE ISSUED	REPORT TITLE	NUMBER OF RECS	BETTER USE OF FUNDS	QUESTIONED COSTS	UNSUPPORTED COSTS	PAGE
Jan. 19, 2021	Personnel Security Clearances and Badge Access Controls for Separated Employees (DOE-OIG-21-12)	8				37
Feb. 1, 2021	The Department of Energy's Wildland Fire Prevention Efforts at the Los Alamos National Laboratory (DOE-OIG-21-13)	5				38
Feb. 8, 2021	Management Letter on The Department of Energy's Unclassified Cybersecurity Program for Fiscal Year 2020 (DOE-OIG-21-14) <i>This report is Official Use Only and not available for public viewing.</i>	35				39
Feb. 19, 2021	Western Federal Power System's Fiscal Year 2020 Financial Statement Audit (DOE-OIG-21-15)	0				39
Feb. 22, 2021	The Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2020 (DOE-OIG-21-16)	2				40
Mar. 25, 2021	The Department of Energy's Unclassified Cybersecurity Program – 2020 (DOE-OIG-21-18)	0				40

## INSPECTIONS

This is a listing of all inspection reports issued from October 1, 2020, through March 31, 2021.

DATE ISSUED	REPORT TITLE	NUMBER OF RECS	BETTER USE OF FUNDS	QUESTIONED COSTS	UNSUPPORTED COSTS	PAGE
Dec. 9, 2020	Evaluation of the Aircraft Monitor and Control System's Nuclear Certification (DOE-OIG-21-06)	6				42
Dec. 29, 2020	Department of Energy's Compliance with Executive Order 12950, <i>Combating Race and Sex Stereotyping</i> (DOE-OIG-21-10)	0				42
Mar. 17, 2021	Followup on Conference Management at Selected Department Sites (DOE-OIG-20-56)	0				43

## **RESULTS**

### **LEGISLATIVE AND REGULATORY REVIEWS**

The Inspector General Act of 1978, as amended, requires the OIG to review and comment upon legislation and regulations relating to Department programs and to make recommendations concerning the impact of such legislation or regulations on Departmental economy and efficiency. During this reporting period, the OIG reviewed a number of legislative proposals in coordination with the CIGIE Legislative Committee.

### **INTERFERENCE WITH INSPECTOR GENERAL INDEPENDENCE**

During the reporting period from October 1, 2020, through March 31, 2021, the Department did not attempt to interfere with OIG independence, nor deny funding to OIG activities.

### **RESISTANCE TO OVERSIGHT ACTIVITIES OR RESTRICTED/SIGNIFICANTLY DELAYED ACCESS**

During the reporting period from October 1, 2020, through March 31, 2021, access to documents the OIG believed necessary to perform work was not restricted.

### **INVESTIGATIONS INVOLVING UNAUTHORIZED PUBLIC DISCLOSURE OF CLASSIFIED INFORMATION**

Pursuant to the requirement of Section 6718 of the National Defense Authorization Act, for the reporting period from October 1, 2020, through March 31, 2021, the Office of Investigations reports the following:

The number of investigations opened regarding an unauthorized public disclosure of classified information.	None
The number of investigations completed regarding an unauthorized public disclosure of classified information.	None
Of the number of such completed investigations identified under subparagraph (B), the number referred to the Attorney General for criminal investigation.	None

### **REVIEWS CLOSED AND NOT DISCLOSED TO THE PUBLIC**

The OIG had no reports undisclosed to the public for the reporting period from October 1, 2020, through March 31, 2021.



## INVESTIGATIONS INVOLVING SENIOR GOVERNMENT EMPLOYEES

During the reporting period from October 1, 2020, through March 31, 2021, the following investigations that involved a senior government employee at the GS-15 level or above were conducted by the Office of Investigations.

FACTS AND CIRCUMSTANCES	STATUS AND DISPOSITION	REFERRED TO DOJ	DOJ DECLINATION	DECLINATION REASON
Allegation senior political employees ordered a reversal of Department policy regarding the wearing of personal protective equipment during the COVID-19 pandemic.	Closed; Not substantiated	No	N/A	Allegation not substantiated
Allegation Senior Executive Service employee engaged in non-consensual sexual activity with a subordinate on government property.	Closed; Not substantiated	Yes	July 22, 2020	Lack of sufficient evidence

## WHISTLEBLOWER ACTIVITIES

Whistleblower matters open as of October 1, 2020	69
Whistleblower matters opened this period	5
Whistleblower matters closed this period	7
Whistleblower matters closed via Investigative Reports	0
Whistleblower matters closed via Letters	7
Whistleblower matters open as of March 31, 2021	67

## HOTLINE ACTIVITY

Total Hotline calls, emails, letters, and other complaints (contacts)	1,303 <sup>1</sup>
Hotline contacts resolved immediately/ redirected/no further action	1,167
Hotline contacts predicated for evaluation	136
Total Hotline predications processed this reporting period	134 <sup>2</sup>
Hotline predications transferred to OIG Program Office	35
Hotline predications referred to Department management or other entity for information/action	39
Hotline predications closed based upon preliminary OIG activity and review	60
Hotline predications open at the end of the reporting period	3

<sup>1</sup>This number refers to any contact that required Hotline staff review, including re-contacts for additional information and requests for disposition.

<sup>2</sup>This number includes one predication carried over from the last semiannual reporting period.

## COMMENTS NOT PROVIDED BY THE DEPARTMENT WITHIN 60 DAYS

For the reporting period from October 1, 2020, through March 31, 2021, there were no audit or inspection reports with comments not provided within 60 days.

## REPORTS LACKING MANAGEMENT DECISION

The Department has a system in place to track audit and inspection reports and management decisions. Its purpose is to ensure that recommendations and corrective actions indicated by audit agencies and agreed to by management are addressed as efficiently and expeditiously as possible. The following audit report is over 6 months old, and no management decision had been made by the end of the reporting period. An explanation for the lack of management decision is described in the table below.

DATE ISSUED	REPORT TITLE	STATUS OF MANAGEMENT DECISION
Apr. 10, 2002	Use of Noncompetitive Procurements to Obtain Services at the Savannah River Site (DOE/IG-0862)	The OIG has requested that the Department temporarily delay submitting a Management Decision on the recommendations in this report, pending the outcome of an ongoing related review.

## DISAGREEMENT WITH MANAGEMENT DECISION

For the reporting period from October 1, 2020, through March 31, 2021, there were no reports where the OIG disagreed with management decisions.

## RECOMMENDATIONS NOT IMPLEMENTED

The following table identifies 49 reports with a total of 124<sup>1</sup> recommendations which were agreed to by the Department but have not been implemented as of March 31, 2021. The total potential cost savings associated with these reports is \$1,176,273,623. The OIG is committed to working with management to expeditiously address the management decision and corrective action process, recognizing that certain initiatives will require long-term, sustained, and concerted efforts. [Non-hyperlinked reports are unavailable on the OIG website.]

DATE ISSUED	REPORT TITLE	TOTAL # OF OPEN RECS <sup>2</sup>	POTENTIAL MONETARY BENEFIT <sup>3</sup>
Dec. 17, 2007	<a href="#">Beryllium Surface Contamination at the Y-12 National Security Complex</a> (IG-0783)	1	
Nov. 13, 2009	<a href="#">Management Controls over Selected Aspects of the Department of Energy's Human Reliability Program</a> (OAS-M-10-01)	1	
June 24, 2013	<a href="#">Mitigation of Natural Disasters at Los Alamos National Laboratory</a> (OAS-M-13-04)	1	
Feb. 14, 2014	<a href="#">The Technology Transfer and Commercialization Efforts at the Department of Energy's National Laboratories</a> (OAS-M-14-02)	1	
Sept. 24, 2014	Assessment of Audit Coverage of Cost Allowability for Bechtel Jacobs Company, LLC under Department of Energy Contract No. DE-AC05-98OR22700 during Fiscal Year 2011 (OAS-V-14-17)	1	\$160,007,744
June 22, 2015	<a href="#">The Department of Energy's Implementation of the Pilot Program for Agreements for Commercializing Technology</a> (OAS-M-15-04)	1	
July 10, 2015	<a href="#">The National Nuclear Security Administration's Management of Support Service Contracts</a> (OAS-M-15-05)	1	
Sept. 3, 2015	<a href="#">The Department of Energy's Management of Electronic Mail Records</a> (DOE/IG-0945)	1	

<sup>1</sup>Those recommendations that are not agreed to by management are not tracked by the Department as open/unimplemented recommendations. Since 2007, the Department has only failed to agree on two recommendations issued by the OIG.

<sup>2</sup> A single recommendation in our reports may often be addressed to multiple program elements. The total number of open recommendations will include any recommendation that has not been corrected by at least one of the program elements.

<sup>3</sup> The Potential Monetary Benefits identified are representative of reports with open recommendations rather than individual recommendations. These amounts include funds that could be used more efficiently by implementing the recommended actions as well as other unresolved or questioned costs. Based on our experience, a significant portion of unresolved and questioned costs are ultimately determined to be allowable by contracting officials.

DATE ISSUED	REPORT TITLE	TOTAL # OF OPEN RECS <sup>2</sup>	POTENTIAL MONETARY BENEFIT <sup>3</sup>
Sept. 9, 2015	<a href="#">Assessment of Audit Coverage of Cost Allowability for Sandia Corporation During Fiscal Year 2013 Under Department of Energy Contract No. DE-AC04-94AL85000 (OAS-V-15-03)</a>	1	\$2,569,251
Apr. 1, 2016	<a href="#">Management and Oversight of Information Technology Contracts at the Department of Energy's Hanford Site (DOE-OIG-16-10)</a>	1	\$183,500,000
Sept. 29, 2016	<a href="#">Followup Audit of the Department's Continuity of Operations Planning (DOE-OIG-16-16)</a>	1	
Apr. 26, 2017	<a href="#">Department of Energy's West Valley Demonstration Project (DOE-OIG-17-05)</a>	2	
Sept. 10, 2018	<a href="#">Southwestern Power Administration's Asset Protection (DOE-OIG-18-47)</a>	1	
Oct. 31, 2018	<a href="#">The Department of Energy's Funds Distribution System 2.0 (DOE-OIG-19-03)</a>	1	
Feb. 14, 2019	<a href="#">Allegations Regarding Southwestern Power Administration's Procurement of the Pathways Core Training (DOE-OIG-19-16)</a>	1	\$17,349
Mar. 28, 2019	<a href="#">Preparedness for Firefighting Response at Los Alamos National Laboratory (DOE-OIG-19-23)</a>	1	
Mar. 29, 2019	<a href="#">Audit Coverage of Cost Allowability for Sandia Corporation During Fiscal Years 2014 and 2015 Under Department of Energy Contract No. DE-AC04-94AL85000 (DOE-OIG-19-24)</a>	1	\$5,583,067
Apr. 25, 2019	<a href="#">Allegations of Improper Contracting by Southwestern Power Administration (DOE-OIG-19-28)</a>	1	
May 20, 2019	<a href="#">Mitigation of Risks from Natural Disasters at Lawrence Berkeley National Laboratory (DOE-OIG-19-32)</a>	1	
June 7, 2019	<a href="#">Security over Industrial Control Systems at Select Department of Energy Locations (DOE-OIG-19-34)</a>	1	
June 10, 2019	<a href="#">The Department of Energy's Management of the ActioNet Information Technology Support Contract (DOE-OIG-19-35)</a>	1	\$294,000,000
June 25, 2019	<a href="#">Management of Consultant Services at Los Alamos National Laboratory (DOE-OIG-19-36)</a>	1	\$324,498
Sept. 27, 2019	<a href="#">Management of Cybersecurity over Selected Information Systems at Department of Energy Headquarters (DOE-OIG-19-52)</a>	1	

DATE ISSUED	REPORT TITLE	TOTAL # OF OPEN RECS <sup>2</sup>	POTENTIAL MONETARY BENEFIT <sup>3</sup>
Dec. 19, 2019	<a href="#">Audit Coverage of Cost Allowability for Honeywell Federal Manufacturing &amp; Technologies, LLC from October 1, 2014, to September 30, 2015, Under Department of Energy Contract No. DE-NA0000622, and from October 1, 2015, to September 30, 2017, Under Department of Energy Contract No. DE-NA0002839 (DOE-OIG-20-18)</a>	2	\$1,548,035
Dec. 26, 2019	<a href="#">Audit Coverage of Cost Allowability for Los Alamos National Laboratory from October 1, 2013, to September 30, 2016, Under the Department of Energy Contract No. DE-AC52-06NA25396 (DOE-OIG-20-20)</a>	1	\$8,458,966
Dec. 30, 2019	<a href="#">Followup on the Department of Energy's Unclassified Foreign Visits and Assignments Program (DOE-OIG-20-22)</a>	1	
Mar. 4, 2020	<a href="#">The Department of Energy's Wildland Fire Prevention Efforts at the Oak Ridge Reservation (DOE-OIG-20-32)</a>	2	
Mar 16, 2020	<a href="#">Audit Coverage of Cost Allowability for University of California from October 1, 2014, to September 30, 2017, Under Department of Energy Contract No. DE-AC02-05CH11231 (DOE-OIG-20-36)</a>	1	\$4,063,434
Mar. 23, 2020	<a href="#">The Department of Energy's Wildland Fire Prevention Efforts at the Nevada National Security Site (DOE-OIG-20-37)</a>	1	
June 1, 2020	<a href="#">The Strategic Petroleum Reserve's Modernization Program (DOE-OIG-20-43)</a>	2	
June 8, 2020	<a href="#">The Department of Energy's Management of Cleanup at the Paducah Site's C-400 Complex (DOE-OIG-20-44)</a>	2	
July 6, 2020	<a href="#">The Office of Science's Audit Resolution and Followup Process (DOE-OIG-20-45)</a>	1	
July 6, 2020	<a href="#">The Department of Energy's Federal Employee Substance Abuse Testing Program (DOE-OIG-20-46)</a>	2	
July 6, 2020	<a href="#">Security over Information Technology Peripheral Devices at Select Office of Science Locations (DOE-OIG-20-47)</a> <i>This report is Official Use Only and not available for public viewing.</i>	1	
July 13, 2020	<a href="#">Audit Coverage of Cost Allowability for Sandia Corporation, from October 1, 2015, through April 30, 2017, under the Department of Energy Contract No. DE-AC04-94AL85000 (DOE-OIG-20-48)</a>	3	\$420,640,865

DATE ISSUED	REPORT TITLE	TOTAL # OF OPEN RECS <sup>2</sup>	POTENTIAL MONETARY BENEFIT <sup>3</sup>
July 13, 2020	<a href="#">Audit Coverage of Cost Allowability for Nuclear Waste Partnership, LLC, from October 1, 2014, to September 30, 2017, under the Department of Energy Contract No. DE-EM0001971</a> (DOE-OIG-20-49)	1	\$31,760,414
July 20, 2020	<a href="#">The Department of Energy's Storage and Disposition of Explosives Material at Selected Sites</a> (DOE-OIG-20-50)	4	
July 20, 2020	<a href="#">Small Business Subcontracting Requirements for Prime Contractors at the Hanford Site</a> (DOE-OIG-20-51)	5	\$63,800,000
Sept. 16, 2020	<a href="#">Respiratory Equipment Maintenance at the Hanford Site</a> (DOE-OIG-20-55)	1	
Sept. 30, 2020	<a href="#">Followup on Conference Management at Selected Department Sites</a> (DOE-OIG-20-56)	1	
Sept. 30, 2020	<a href="#">Tank Waste Management at the Hanford Site</a> (DOE-OIG-20-57)	1	
Oct. 20, 2020	<a href="#">Respiratory Equipment Maintenance at the Portsmouth Site</a> (DOE-OIG-21-01)	6	
Dec. 9, 2020	<a href="#">Evaluation of the Aircraft Monitor and Control System's Nuclear Certification</a> (DOE-OIG-21-06)	5	
Dec. 14, 2020	<a href="#">Management of a Department of Energy Site Cybersecurity Program</a> (DOE-OIG-21-07)	18	
Dec. 14, 2020	<a href="#">Contingency Planning Efforts for Information Technology Mission Support Systems at Selected Department of Energy Locations</a> (DOE-OIG-21-08)	2	
Jan. 5, 2021	<a href="#">Management Letter on the Department of Energy's Fiscal Year 2020 Consolidated Financial Statements</a> (DOE-OIG-21-11)	10	
Jan. 19, 2021	<a href="#">Personnel Security Clearances and Badge Access Controls for Separated Employees</a> (DOE-OIG-21-12)	4	
Feb. 1, 2021	<a href="#">The Department of Energy's Wildland Fire Prevention Efforts at the Los Alamos National Laboratory</a> (DOE-OIG-21-13)	5	
Feb. 8, 2021	<a href="#">Management Letter on The Department of Energy's Unclassified Cybersecurity Program for Fiscal Year 2020</a> (DOE-OIG-21-14)	18	
<b>Total Open Recommendations</b>		<b>124</b>	<b>\$1,176,273,623</b>

## PEER REVIEWS

<b>PEER REVIEWS CONDUCTED BY ENERGY OIG</b> OCTOBER 1, 2020 – MARCH 31, 2021			
TYPE OF REVIEW	DATE OF PEER REVIEW	OIG REVIEWED	OUTSTANDING RECOMMENDATIONS
<b>Audits</b>	None this reporting period.		
<b>Inspections</b>	None this reporting period.		
<b>Investigations</b>	None this reporting period.		

<b>PEER REVIEWS CONDUCTED BY OTHER OIGS</b> OCTOBER 1, 2020 – MARCH 31, 2021				
TYPE OF REVIEW	DATE OF PEER REVIEW	REVIEWING OIG	FREQUENCY REQUIREMENT	OUTSTANDING RECOMMENDATIONS
<b>Audits</b>	None this reporting period.			
<b>Inspections</b>	None this reporting period.			
<b>Investigations</b>	None this reporting period.			

## INVESTIGATIVE OUTCOMES

### **Sentencing and Indictment in Procurement Integrity Act Investigation**

A subcontractor company for the Department's Strategic Petroleum Reserve (SPR) was sentenced in the U.S. District Court for the Eastern District of Louisiana to pay a \$400,000 criminal fine and a \$400 special assessment. As reported in the September 30, 2020, *Semiannual Report to Congress*, the subcontractor company previously pled guilty to Conspiracy to Defraud the Government and violating the Procurement Integrity Act. As previously reported, the Office of Inspector General (OIG) investigation determined that from February 2002 through October 2016 the subcontractor received subcontracts totaling approximately \$9 million for the provision of equipment and services at the various SPR facilities. To receive these subcontracts, the company conspired with a former subcontract management technical representative at the SPR and obtained non-public Government pricing information in advance of submitting its proposals. In addition, a former contractor employee who served as the management technical representative for the subcontract was indicted in the U.S. District Court for the Eastern District of Louisiana on one count of Conspiracy to Defraud the United States and one count of False Statements. The indictment alleged the former employee conspired with the subcontractor company by providing non-public pricing information to that company, and further lied to the OIG investigator regarding the matter. The investigation further determined that over 90% of the company's subcontract awards can be attributed to this scheme. The Department of Justice (DOJ) press release can be found [here](#).

### **Former Department Subcontractor Sentenced in Foreign Corrupt Practices Act Investigation**

A former Department subcontractor was sentenced in the U.S. District Court for the District of Maryland to 4 years in prison after being convicted at trial on four counts of violating the Foreign Corrupt Practices Act (FCPA), one count of conspiracy to violate the FCPA, and two counts of Wire Fraud. The subcontractor was also ordered to pay \$56,417 in asset forfeiture, and \$27,000 in fines and special assessments. As previously reported in the March 31, 2020, March 31, 2018, March 31, 2016, March 31, 2015, and September 30, 2015, *Semiannual Reports to Congress*, the former subcontractor, also the former co-president of a Maryland-based transportation company that provides services for the transportation of nuclear materials to customers in the U.S. and abroad, was indicted on 11 counts of Conspiracy, Wire Fraud, International Money Laundering, and violations of the FCPA. The transportation company entered into a deferred prosecution agreement with the DOJ to pay a \$2 million penalty to resolve charges of Conspiracy to Violate the Anti-Bribery provisions of the FCPA. The investigation determined the former co-president engaged with several co-conspirators in a scheme to bribe a Russian official to influence the awarding of contracts to the Russian State-owned nuclear energy corporation, TENEX. The former executive of a Russian company was sentenced to 48 months of incarceration and forfeiture of \$2,126,622 for Conspiracy to Commit Money Laundering. The investigation determined the executive violated the FCPA by participating in a kickback scheme with several American co-conspirators to direct the awarding of contracts for the shipment of uranium from Russia to the United States without competition under the



Megatons to Megawatts program. This is an ongoing joint investigation with the Federal Bureau of Investigation (FBI), and is being coordinated with the U.S. Attorney's Office for the District of Maryland. The DOJ press release can be found [here](#).

### **Sentencing in Grant Fraud Investigation**

A Department grantee was sentenced in the U.S. District Court for the District of Delaware to 2 years of supervised release, the first 12 months of which will be in a monitored home confinement, with a \$50,000 fine and a \$100 special assessment. As previously reported in the September 30, 2020, March 31, 2020, and September 30, 2017, *Semiannual Reports to Congress*, the grantee pleaded guilty to one count of wire fraud in connection with a Small Business Innovative Research (SBIR) grant fraud investigation. The investigation determined that from 2009 through 2018 the defendant obtained more than 30 SBIR awards from numerous Federal agencies, totaling over \$11 million, to include one Phase I SBIR award from the Department totaling approximately \$225,000. The investigation found numerous false statements in the award applications, as well as forged letters of support and collaboration. In addition to the guilty plea, the grantee entered into a civil settlement in which he will pay \$700,000 in damages to the Government for violations of the Civil False Claims Act. This is a joint investigation with the National Science Foundation (NSF) OIG, National Aeronautics and Space Administration (NASA) OIG, Defense Criminal Investigative Service (DCIS), Naval Criminal Investigative Service, and Air Force Office of Special Investigations, and is being concurrently prosecuted by the Criminal and Civil sections of the U.S. Attorney's Office for the District of Delaware.

### **Sentencing in Theft of Government Property Investigation**

Three former contractor employees were sentenced in the U.S. District Court for the Eastern District of Tennessee after pleading guilty to one charge each of Theft of Government Property. As previously reported in the March 31, 2020, *Semiannual Report to Congress*, an OIG investigation determined two former prime contractor construction superintendents conspired with a subcontractor electrician to steal over 4,400 pounds of copper wire from the Y-12 National Security Complex in Oak Ridge, Tennessee. The former subcontractor employee was sentenced to 5 years of probation and the former superintendents were each sentenced to 2 years of probation. All three were ordered to pay a \$100 special assessment fee and collective restitution of \$51,176.

### **Sentencings and Guilty Plea in Theft of Government Property Investigation**

Two owners of two separate businesses were sentenced in the U.S. District Court for the District of Colorado after previously pleading guilty to one count each of Theft of Government Property, pursuant to an Information. Each of the business owners were sentenced to 3 years of probation, a \$100 special assessment fee, and ordered to pay restitution in the amounts of \$165,004 and \$81,873. A former Department vendor was also sentenced in the U.S. District Court for the District of Colorado to 4 years of probation and ordered to pay a \$100 special assessment fee and restitution in the amount of \$194,210. An additional former Department vendor also pleaded guilty to one count of Theft of Government Property. Additionally, in response to an Investigative Report to Management (IRM) issued to the Department's Office of Acquisition Management, a letter of suspension and proposed debarment was issued to the former Department vendor. As previously

reported in the September 30, 2020, and March 31, 2020, *Semiannual Reports to Congress*, the OIG investigation determined the business owners and numerous other vendors participated in a fictitious billing scheme with a Department contractor employee tasked with inventory management duties at a Department-owned warehouse. The warehouse employee initiated fictitious purchase orders to the vendor companies to order goods for the warehouse. The goods ordered from the vendor companies were never received by the warehouse and the proceeds from the purchases were stolen by the warehouse employee and vendors involved in the scheme. This is an ongoing joint investigation with the FBI and General Services Administration OIG.

### **Guilty Plea and Sentencing for Attempted Burglary**

An individual with no affiliation to the Department pleaded guilty to one count of Attempted Burglary, in violation of Illinois State law, in the Eighteenth Judicial District Circuit Court, DuPage County, Illinois. The individual was sentenced to 30 months of probation, fined \$750, and ordered to pay \$800 in restitution to the Fermi National Accelerator Laboratory in Batavia, Illinois. As previously reported in the September 30, 2020, and March 31, 2020, *Semiannual Reports to Congress*, the OIG investigation found the individual and a co-conspirator were recorded on video trying to remove copper wiring from a storage building located at the Fermi National Accelerator Laboratory. This was a joint investigation with the DuPage County Sheriff's Department.

### **Superseding Indictment in Small Business Technology Transfer Fraud Investigation**

A Department grant recipient was charged by superseding indictment for two additional counts of wire fraud and one additional count of making false statements. As previously reported in the September 30, 2020, *Semiannual Report to Congress*, the grant recipient had previously been arrested and indicted for violations of 9 Federal statutes in a 13-count indictment, which included forfeiture of assets traceable to the offenses, including more than \$2 million which was seized when the grantee was arrested. The OIG investigation determined that the grant recipient and a co-conspirator, owners of a business which received Government funds under the Department's Small Business Technology Transfer (STTR) program, submitted numerous false statements and false business documents in proposals, reports, and other records submitted to the Department to obtain three STTR awards totaling \$2.1 million. The false statements submitted by the grant recipient were made regarding his contractual obligations under a foreign government talent recruitment plan, his receipt of research funding from a foreign government, and his international collaboration on U.S.-funded research. The grant recipients also converted Department STTR funds for personal use and were further engaged in a money laundering scheme to transfer the fraudulently obtained Department grant funds between multiple financial accounts. This is an ongoing joint investigation with the FBI and NSF OIG. The DOJ press release for the initial indictment can be found [here](#).

### **Arrest in Theft of Government Funds Investigation**

A former contractor employee was arrested pursuant to a warrant issued by the 9<sup>th</sup> Judicial District of Tennessee for violation of Theft of Property over \$10,000, according to the Criminal Code of Tennessee. The investigation determined that from January 2017 through

October 2017 the former contractor employee falsely claimed to have worked approximately 285 hours for an estimated amount of \$25,853. This is an ongoing investigation.

### **Indictment in Small Business Innovation Research Grant Fraud Investigation**

An owner of a scientific research company was indicted in the U.S. District Court for the Eastern District of Kentucky on 15 counts, including Conspiracy, Wire Fraud, Money Laundering, and False Claims. The grantees were also subject to criminal forfeiture. The investigation determined the grantees received approximately \$1.2 million in Department SBIR and STTR grant awards, in addition to funding from other Federal government agencies, and provided false information in their proposals and certifications to the Department. This is an ongoing investigation with the Environmental Protection Agency OIG and DCIS.

### **Research Professor Arrested for Grant Fraud**

A research professor was charged and arrested in the District of Massachusetts pursuant to a criminal complaint, and subsequently indicted on two counts of Wire Fraud and one count of Failing to Disclose Foreign Bank Accounts. The investigation determined that the professor failed to disclose contracts, appointments, and awards received from various foreign entities to the Department. This is an ongoing joint investigation involving multiple OIG field offices, FBI, DCIS, Homeland Security Investigations, and Internal Revenue Service Criminal Investigation. The DOJ press release can be found [here](#).

### **Indictment in Narcotics Possession Investigation**

A former subcontractor employee of the M&O contractor for the Savannah River Site (SRS) was indicted in the U.S. District Court for South Carolina on one count of Possession of a Controlled Substance with the Intent to Distribute. The investigation determined that the former employee was searched while exiting the site, which uncovered 73 grams of cocaine, packaged individually for potential sale, and \$4,382 in cash. The investigation further determined that the employee had prior knowledge that the cocaine was located in the vehicle, but no evidence revealed that the former employee sold any controlled substances onsite at SRS. This is an ongoing investigation.

### **Arrest in Offenses Against Children Investigation**

A contractor employee with the M&O contractor for the SRS was arrested on charges of third-degree Sexual Criminal Conduct with a minor, pursuant to an arrest warrant issued by the State of South Carolina. The investigation determined that the contractor employee admitted to the conduct during the administration of a polygraph examination. This is an ongoing joint investigation with the Aiken Department of Public Safety.

### **Criminal Complaint and Suspensions Filed in Grant Fraud Investigation**

A Department grantee was charged by Criminal Complaint in the U.S. District Court for the Western District of New York with False Statements and Wire Fraud in connection with SBIR awards from various Federal government agencies totaling approximately \$500,000, including one Department SBIR grant of approximately \$150,000. The investigation determined that the grantee paid Department invoices using funds originating from

another Federal agency, failed to pay research partners, and submitted false claims and certifications to the U.S. Government. The grantee and two affiliated companies related to the investigation were suspended from Federal Government contracting by the NSF. This is an ongoing joint investigation with the NSF OIG and NASA OIG.

### **Former Laboratory Employee Charged in Theft of Government Property Investigation**

A former employee at Princeton Plasma Physics Laboratory (PPPL) was charged by criminal complaint in the Middlesex County Superior Court, New Jersey, with three counts of New Jersey Statutes Annotated (NJS) Section 2C:20-3, Theft by Unauthorized Taking, a third-degree felony. A joint investigation with the Princeton University Police determined that from December 2020 through January 2021 the former employee stole large amounts of copper from PPPL. The OIG also pursued investigation of several similar thefts at PPPL and discovered that the former employee also stole a Department-owned camera and two Department-owned tool kits. The thefts of copper and additional items resulted in a total loss to PPPL of approximately \$35,500. Per Middlesex County COVID-19 protocols, a summons for the charges was issued in lieu of an arrest warrant. This is an ongoing investigation.

### **Civil Settlement in Grant Fraud Investigation**

A Department grantee, the owner of a company who received SBIR and STTR funds from various Federal agencies, including the Department, entered into a Civil Settlement Agreement with the DOJ in the amount of \$122,452. The Settlement Agreement resolved civil claims against the owner arising from the submission of false claims, materially false statements, and misrepresentations made in various applications for Federal funding. As previously reported in the September 30, 2020, March 31, 2019, and September 30, 2018, *Semiannual Reports to Congress*, this investigation determined that three grantees, through three separate companies, applied for and received SBIR and STTR grants for equivalent work, and concealed the existence of the grants and the relationships between the related grantees and companies from the awarding agencies. Additionally, during the application process, the grantees misrepresented to the awarding agencies the existence and use of company facilities, employees, and equipment. As also previously reported, two of the grantees reached Pretrial Diversion Agreements with the DOJ, and one grantee and all three corporations were sentenced in the U.S. District Court for the District of South Dakota after pleading guilty to Wire Fraud and Conspiracy to Commit Wire Fraud. One of the grantees received a sentence of 24 months of probation with 80 hours of community service and was ordered to pay restitution with the 3 corporations in the amount of \$1,084,819 with a \$100 special assessment fee. As also previously reported, the two remaining grantees each entered into \$250,000 Settlement Agreements. This is a joint investigation with the NASA OIG and NSF OIG.

### **Settlement Agreement in Grant Fraud Investigation**

A Department grantee, the former Chief Executive Officer (CEO) of a company, entered into a Civil Settlement Agreement with the DOJ in the amount of \$28,500 to resolve allegations of fraud related to the False Claims Act. The Department's share of the resolved amount was \$1,528. The investigation determined that the former CEO, whose company received

one Department and two NASA SBIR awards, executed, and submitted false certifications pursuant to these awards. As previously reported in the September 30, 2020, *Semiannual Report to Congress*, the former CEO's business partner also made false representations and certifications in order to receive the SBIR awards, which the company was otherwise ineligible to receive, and entered into a \$374,184 Civil Settlement Agreement. This case was investigated jointly with NASA OIG. The DOJ press release is available [here](#).

### **Settlement Agreement in False Claims Act Investigation**

As a result of an OIG investigation, the DOJ entered into a \$980,000 Civil Settlement Agreement with the Department's prime construction contractor for the Salt Waste Processing Facility (SWPF) at the SRS. The settlement resolves allegations that the contractor submitted false claims to the Department in connection with per diem monies paid to subcontractor employees working on the SWPF project from 2011 through 2017. As previously reported in the September 30, 2015, *Semiannual Report to Congress*, the contractor entered into a \$3.8 million Civil Settlement Agreement after an OIG investigation found the contractor paid its employees unallowable per diem and relocation monies after failing to take contractually required steps to verify employee eligibility. The subsequent OIG investigation showed that in addition to seeking reimbursement for unallowable per diem and relocation costs paid to its own employees, the contractor also sought reimbursement for unallowable costs paid to employees of its SWPF subcontractors.

### **Civil Settlement Agreement in Civil False Claims Investigation**

The Municipality of Ponce, Puerto Rico, entered into a Civil Settlement Agreement with the DOJ in the amount of \$100,000 to settle allegations of violations of the False Claims Act. The investigation determined that the Municipality of Ponce failed to solicit sealed public bids and to seek multiple bids or solicitations, as required under State and Federal procurement rules, when it awarded a contract for the procurement and installation of a solar photovoltaic system to provide power to the Municipality of Ponce's police station. The contract was paid for using Energy Efficiency and Conservation Block Grant funds from the Department under the American Recovery and Reinvestment Act.

### **Civil Settlement Agreement in Civil False Claims Investigation**

The Municipality of Cataño, Puerto Rico, entered into a Civil Settlement Agreement with the DOJ in the amount \$100,000 to settle allegations of violations of the False Claims Act. The investigation determined that the Municipality of Cataño failed to solicit sealed public bids, as required under State and Federal procurement rules, when it awarded a contract for the procurement and installation of air conditioner units for the Municipality of Cataño's coliseum. The contract was paid for using Energy Efficiency and Conservation Block Grant funds from the Department under the American Recovery and Reinvestment Act.

### **Notice of Termination and Debarment in Theft of Intellectual Property Investigation**

As a result of a referral issued to the U.S. Navy Acquisition Integrity Office, a Navy contractor employee, formerly a contractor employee at Argonne National Laboratory and a Federal employee at the U.S. Naval Research Laboratory, was terminated by a contractor to the Navy. The Navy also issued a letter of proposed debarment to the former contractor employee. The investigation determined that the former contractor employee downloaded

Department proprietary technology without authorization and started a corporation with the intent to commercialize and profit from the technology. Prior to this reporting period, the Navy had terminated the individual's employment with the U.S. Naval Research Laboratory after the OIG advised the Navy of the OIG's investigative findings. This was a joint investigation with the FBI and the Naval Criminal Investigative Service.

### **Debarment in False Statements Investigation**

As a result of an IRM, a former Los Alamos National Laboratory contractor employee was debarred from receiving Federal funds or contracts for a period of 5 years. As previously reported in the September 30, 2019, *Semiannual Report to Congress*, an investigation conducted by the FBI determined the former contractor employee provided false statements when questioned regarding involvement in a foreign government talent recruitment plan.

### **Restitution Paid by Former Contractor Employee**

A former contractor employee at Lawrence Livermore National Laboratory paid \$3,743 in restitution after having been charged with Embezzlement and Grand Theft in the Superior Court of California, County of Alameda. As a result of an IRM, the National Nuclear Security Administration's (NNSA) Office of Acquisition and Project Management suspended the former contractor employee and proposed a debarment from Federal contracting for a period of 1 year. As previously reported in the March 31, 2020, *Semiannual Report to Congress*, the investigation determined that the former contractor employee admitted to committing timecard fraud by charging regular hours to the contract while spending hours in a personal vehicle and not working. The former contractor employee was also terminated as a result of the investigation.

### **Employee Terminated in Theft of Government Property Investigation**

As a result of an OIG investigation, a contractor employee at NNSA's Albuquerque Complex was terminated. Also, as a result of the investigation, prior to termination the employee had been placed on unpaid administrative leave and reprimanded. The former contractor employee admitted to stealing several drones and accessory items from the Albuquerque Complex. The OIG recovered the stolen property, valued at approximately \$100,000. This is an ongoing joint investigation with the FBI.

### **Debarment in Federal Program Fraud Investigation**

As a result of an OIG investigation, a former West Virginia University Professor was debarred from receiving Federal funds or contracts for a period of 3 years. An investigation conducted by the FBI found the former professor falsely requested and received a leave of absence from his West Virginia University teaching responsibilities to care for his family when in fact he was working overseas to meet the requirements of his foreign government talent recruitment plan. The former professor pleaded guilty to one count of Federal Program Fraud and was sentenced to 3 months of imprisonment, 1 year of supervised release, and ordered to pay restitution in the amount of \$20,189 and a fine of \$9,363. An FBI investigation and the subject's guilty plea led to an OIG finding that the former professor was the Principal Investigator on two Department Office of Science awards during the time period of the charged fraudulent activity.

### **Notice of Suspension in Per Diem Claims Investigation**

As a result of an OIG investigation, NNSA suspended a former employee of a parent company of the SRS M&O contractor from Federal Government contracting and proposed a debarment of 1 year. The proposed debarment includes a company owned by the former employee and would also prevent the former employee's company from contracting and receiving award of Federal Government contracts for 1 year. As previously reported in the September 30, 2020, *Semiannual Report to Congress*, the investigation determined that while on a long-term assignment to SRS, the former employee knowingly sought improper reimbursement for a less-than-arms-length rental agreement with an entity he controlled. He then concealed this obvious conflict of interest from both the SRS M&O contractor and its parent company.

### **Notice of Termination in Timecard Fraud Investigation**

During an OIG investigation, a Senior Leadership Team employee of the Idaho National Laboratory's prime contractor was terminated while under investigation for timecard fraud. To date, the investigation has determined the Senior Leadership Team employee was compensated for numerous hours that the employee did not work. The contractor also reimbursed the Department a total of \$148,554 for the hours that the former employee did not work. This is an ongoing investigation.

### **Contractor Employee Terminated in Theft of Government Property Investigation**

A contractor employee at the Portsmouth Gaseous Diffusion Plant in Piketon, Ohio, was terminated for theft of Government property. The former contractor employee was observed by Protective Force personnel placing government property into the trunk of a personal vehicle and attempting to exit the protected area of the Portsmouth Gaseous Diffusion Plant. Protective Force personnel stopped the former employee and recovered the stolen property, amounting to \$4,629. Pike County Sheriff's Office responded to the scene and arrested the former employee for theft. The former employee admitted to removing the property without permission and further admitted to a continuing pattern of theft spanning the last 9 years. This is an ongoing investigation.

### **Contractor Employee Resigns in Lieu of Termination**

As a result of an OIG investigation, a contractor employee at the Pacific Northwest National Laboratory resigned in lieu of termination by the contractor. During an OIG interview, the former contractor employee admitted to intentionally falsifying timecards, leaving work early without taking leave, arriving to work late, and teleworking without evidence of completing work activities. The former contractor employee's timecards included hours charged to a project on which no work had been completed. The former contractor employee had approximately 500 hours that were unaccounted for in a 6-month period. This is an ongoing investigation.

### **Recovery of Funds in False Claims Investigation**

In response to an IRM, the M&O contractor at the Waste Isolation Pilot Plant identified \$12,866 in unallowable and questioned costs related to lodging expenses reimbursable to a

former subcontractor employee, and the entire amount was recovered from the subcontractor. An OIG investigation had determined the former subcontractor employee submitted false lodging expenses for reimbursement to the M&O.

**Government Property Seized from Contractor Employee**

The OIG seized \$1,964 worth of computer-related equipment from the personal residence of a contractor employee of the Lawrence Berkeley National Laboratory. The OIG investigation determined the laboratory employee used Government funds to purchase items for personal use, utilizing the laboratory procurement system. The contractor employee admitted to the purchases when interviewed by the OIG. This is an ongoing investigation.



## AUDIT REPORTS

### **Respiratory Equipment Maintenance at the Portsmouth Site**

The Department's Portsmouth Site (Portsmouth) includes one of three large gaseous diffusion plants in the United States initially constructed to produce enriched uranium to support the Nation's nuclear weapons program and, in later years, enriched uranium used by commercial nuclear reactors. In 2001, enrichment operations were discontinued at Portsmouth. In 2011, decontamination and decommissioning of Portsmouth's gaseous diffusion plant commenced. Fluor-BWXT Portsmouth LLC (FBP) is the Department's contractor responsible for the decontamination and decommissioning of Portsmouth's gaseous diffusion plant.

We initiated this audit to determine whether Portsmouth was adequately maintaining respiratory protection equipment to protect workers from exposure to hazardous materials. This report is one in a series of reports at select Office of Environmental Management sites.

During our audit we identified significant weaknesses in the decontamination of radiologically contaminated respirators that could increase the risk that workers would be exposed to radioactive contamination and potentially inhale radioactive particles. Specifically, we identified that (1) FBP's cleaning contractor, UniTech, was not in compliance with its contract requirement to ensure respiratory protection equipment did not contain radioactive contamination, and (2) FBP's mitigating controls were inadequate to ensure respiratory equipment returned from UniTech was not radiologically contaminated. In addition, FBP did not always ensure respiratory protection equipment was safeguarded from loss.

The issues with the UniTech contract occurred because FBP's corrective actions were inadequate to address the root cause of contaminated respirators being shipped to FBP, recurring issues were not reported to the Department's Occurrence Reporting and Processing System, FBP's oversight of UniTech did not ensure all contractual requirements were being met, and the Department did not hold FBP accountable for the UniTech contract issues. In addition, respiratory protection equipment was not always safeguarded from loss because FBP had not established an adequate inventory system that could track respirators from purchase to disposal. Management generally concurred with our recommendations and its proposed corrective actions are consistent with our recommendations. (DOE-OIG-21-01)

### **Department of Energy Nuclear Waste Fund's Fiscal Year 2020 Financial Statement Audit**

The report presents the results of the independent certified public accountants' audit of the balance sheets of the Department's Nuclear Waste Fund, as of September 30, 2020, and 2019, and the related statements of net cost, changes in net position, and statements of budgetary resources for the years then ended.

To fulfill the OIG's audit responsibilities, we contracted with the independent public accounting firm of KPMG LLP (KPMG) to conduct the audit, subject to our review. KPMG is responsible for expressing an opinion on the Nuclear Waste Fund's financial statements and reporting on applicable internal controls and compliance with laws and regulations. The OIG monitored audit progress and reviewed the audit report and related documentation. This review disclosed no instances where KPMG did not comply, in all material respects, with generally accepted Government auditing standards. The OIG did not express an independent opinion on the Nuclear Waste Fund's financial statements.

KPMG concluded that the combined financial statements present fairly, in all material respects, the respective financial position of the Nuclear Waste Fund as of September 30, 2020, and 2019, and its net costs, changes in net position, and budgetary resources for the years then ended, in accordance with United States generally accepted accounting principles.

As part of this review, auditors also considered the Nuclear Waste Fund's internal controls over financial reporting and tested for compliance with certain provisions of laws, regulations, contracts, and grant agreements that could have a direct and material effect on the determination of financial statement amounts. The audit did not identify any deficiency in internal control over financial reporting that is considered a material weakness. Additionally, the results of the auditors' review disclosed no instances of noncompliance or other matters required to be reported under Government Auditing Standards or applicable Office of Management and Budget (OMB) guidance. (DOE-OIG-21-02)

**Department of Energy's Fiscal Year 2020 Consolidated Financial Statement Audit**  
Pursuant to requirements established by the Government Management Reform Act of 1994, the OIG engaged the independent public accounting firm of KPMG to perform the audit of the Department's FY 2020 Consolidated Financial Statements.

KPMG audited the consolidated financial statements of the Department as of September 30, 2020, and 2019, and the related consolidated statements of net cost, changes in net position, custodial activity, and combined statements of budgetary resources for the years then ended. KPMG concluded that these consolidated financial statements are presented fairly, in all material respects, in conformity with United States generally accepted accounting principles and has issued an unmodified opinion based on its audits and the reports of other auditors for the years ended September 30, 2020, and 2019.

The OIG issued notices of findings and recommendations to management throughout the audit. In nearly all instances, management concurred with the findings and recommendations. All findings will be detailed in management letters. The audit disclosed no instances of noncompliance or other matters required to be reported under applicable audit standards and requirements.

KPMG is responsible for the auditors' report and the opinions and conclusions expressed therein. The OIG is responsible for technical and administrative oversight regarding

KPMG’s performance under the terms of the contract. Our review was not intended to enable us to express, and accordingly, we do not express an opinion on the Department’s financial statements, management’s assertions about the effectiveness of its internal controls over financial reporting, or the Department’s compliance with laws and regulations. Our monitoring review disclosed no instances where KPMG did not comply with applicable auditing standards. (DOE-OIG-21-03)

### **Management Challenges at the Department of Energy – Fiscal Year 2021**

In compliance with the Reports Consolidation Act of 2000, the OIG annually identifies what it considers to be the most significant management challenges facing the Department. The OIG’s goal is to focus attention on significant issues with the objective of working with Department officials to enhance the effectiveness of agency programs. The Management Challenges Report should be a valuable tool to assist the Department to successfully fulfill its mission of ensuring America’s security and prosperity by addressing its energy, environmental, and nuclear challenges through transformative science and technology solutions.

Historically, our Management Challenges Report identified broad areas of concern for the Department. This year, the OIG significantly revised how the Management Challenges Report was compiled and presented to focus on more specific goals and challenges that the Department is facing. We coordinated with Department mission elements to identify the most pressing challenges, with an eye toward better focusing on practical issues where near-term progress is achievable. Our intent is to provide the Secretary and other policymakers with a more useful document containing specific and actionable challenge areas where meaningful improvements may be realized in the near term.

We hope that the new methodology used to identify management challenges within this report will prove more useful to senior Department officials and will enable action to address the issues they are facing. (DOE-OIG-21-04)

### **Federal Energy Regulatory Commission’s Fiscal Year 2020 Financial Statement Audit**

The report presents the results of the independent certified public accountants’ audit of the Federal Energy Regulatory Commission’s (FERC) balance sheets as of September 30, 2020, and 2019, and the related statements of net cost, changes in net position, and statements of budgetary resources for the years then ended.

To fulfill the OIG’s audit responsibilities, we contracted with the independent public accounting firm of KPMG to conduct the audit, subject to our review. KPMG is responsible for expressing an opinion on FERC’s financial statements and reporting on applicable internal controls and compliance with laws and regulations. The OIG monitored audit progress and reviewed the audit report and related documentation. This review disclosed no instances where KPMG did not comply, in all material respects, with generally accepted Government auditing standards. The OIG did not express an independent opinion on FERC’s financial statements.

KPMG concluded that the combined financial statements present fairly, in all material respects, the respective financial position of FERC as of September 30, 2020, and 2019, and its net costs, changes in net position, and budgetary resources, and custodial activity for the years then ended, in accordance with United States generally accepted accounting principles.

As part of this review, auditors also considered FERC's internal controls over financial reporting and tested for compliance with certain provisions of laws, regulations, contracts, and grant agreements that could have a direct and material effect on the determination of financial statement amounts. The audit did not identify any deficiency in internal control over financial reporting that is considered a material weakness.

The results of the auditors' review of FERC's compliance with certain laws and regulations disclosed no instances of noncompliance or other matters required to be reported under Government Auditing Standards or applicable OMB guidance. (DOE-OIG-21-05)

### **Management of a Department of Energy Site Cybersecurity Program**

The Department operates many facilities across the Nation that depend on information technology systems and networks for essential operations required to accomplish its national security, research and development, and environmental management missions. To support its mission, the site reviewed uses various types of information systems that includes several key systems and applications. The Federal Information Security Modernization Act of 2014 requires each Federal agency to develop, document, and implement an enterprise-wide cybersecurity program to protect systems and data that support the operations and assets of an agency, including those provided or managed by contractors. We initiated this audit to determine whether the site effectively managed its cybersecurity program.

During our test work, we noted several areas of immediate concern related to vulnerability management and the authorization of information system operations at the site. In August 2019, we issued a management alert to ensure that management was provided with the opportunity to initiate immediate actions to address certain issues identified during our audit. Subsequent to the issuance of the management alert, we continued our test work, and this report addresses additional risk areas and recommendations.

The site had not implemented an effective cybersecurity program in accordance with Federal and Department requirements. Our review identified control weaknesses in each of the 14 control families tested as described in National Institute of Standards and Technology Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. The weaknesses identified occurred, in part, due to an inadequate cybersecurity governance structure, a lack of cybersecurity performance metrics, and the existence of limited resources available for cybersecurity activities. For instance, the site's cybersecurity governance structure relied on program-level policy, and it had not adequately developed and/or implemented many site-specific policies and procedures. In addition, we determined that performance metrics had not been established to incentivize the site's operating contractor to ensure that fully effective

cybersecurity practices were implemented. Furthermore, a lack of resources dedicated to cybersecurity activities contributed to many of the weaknesses identified, including those related to security assessment and authorization, risk assessment, and audit and accountability. To their credit, officials had initiated actions to address a number of weaknesses identified during our review. However, absent a fully effective cybersecurity program, the site's information systems and data will continue to be at a higher-than-necessary risk of compromise, loss, or modification.

To help improve the management of the site's cybersecurity program, we issued a detailed report to Department management that included a total of 55 recommendations. Management concurred with the recommendations and indicated that corrective actions were taken or planned to mitigate the findings identified in the report. Due to the sensitive nature of the vulnerabilities identified during our audit, the report issued to the Department was for Official Use Only. We provided site and program officials with detailed information regarding vulnerabilities that we identified. (DOE-OIG-21-07)

### **Contingency Planning Efforts for Information Technology Mission Support Systems at Selected Department of Energy Locations**

Information technology (IT) mission support systems and their related functions play a paramount role in the Department's ability to accomplish its day-to-day missions. However, information systems are vulnerable to a variety of disruptions ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire). Ensuring that IT support systems are available at critical moments can impact the Department's ability to withstand or recover from disruptions. Contingency planning supports this requirement through the establishment of thorough plans, procedures, and technical measures that enable a system to be recovered as quickly and effectively as possible following a service disruption.

Because of the importance of the Department's missions, it is imperative that the Department understands the impact of potential disruptions on its computing environment and be able to maintain or restore its information systems and maintain operations, as appropriate. As such, we initiated this audit to determine whether the Department had adequately planned for the restoration of IT mission support systems and functions in accordance with established requirements to ensure functionality in the event of a disruption.

We found that the Department had not always adequately planned for the restoration of information systems in accordance with established requirements to ensure availability and functionality in the event of a disruption. Specifically, we found that three of the four sites reviewed had not fully implemented contingency planning requirements related to development of a Business Impact Analysis as identified in Federal requirements. In addition, sites had not fully developed Information System Contingency Plans in accordance with Federal guidance for 10 of the 17 systems reviewed.

The weaknesses identified were due primarily to inappropriate interpretations of contingency planning requirements by Federal and contractor officials. Management

concurring with the recommendations and stated that corrective actions were planned to address the issues identified in the report. (DOE-OIG-21-08)

### **Management Letter on the Federal Energy Regulatory Commission’s Fiscal Year 2020 Financial Statement Audit**

This report is Official Use Only (OUO) and not available for public viewing.  
(DOE-OIG-21-09)

### **Management Letter on the Department of Energy’s Fiscal Year 2020 Consolidated Financial Statements**

Pursuant to requirements established by the Government Management Reform Act of 1994, the OIG engaged the independent public accounting firm of KPMG to perform the audit of the Department’s FY 2020 Consolidated Financial Statements. During the audit, KPMG considered the Department’s internal controls over financial reporting and tested for compliance with certain provisions of laws, regulations, contracts, and grant agreements that could have a direct and material effect on the consolidated financial statements.

During the course of the audit, KPMG identified deficiencies in internal control that were included in the attached management letter. Specifically, the issued letter contains 10 new findings and a total of 14 recommendations that were issued during the FY 2020 Audit of the Department’s Consolidated Financial Statements. Management fully concurred with all but one recommendation included in the management letter and took or planned to take corrective actions. Management’s responses are included with each finding. The audit did not identify any deficiency in internal control over financial reporting that is considered a material weakness. (DOE-OIG-21-11)

### **Personnel Security Clearances and Badge Access Controls for Separated Employees**

The Department uses security clearances and badges to control access to its sites and facilities. In 2004, the Homeland Security Presidential Directive-12 (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors directed Federal agencies to adopt a common identification standard for all employees and contractors. In an effort to comply with the mandate in HSPD-12, the Department provides its Federal and contractor employees with Personal Identity Verification (PIV) cards, which serve as access authorization badges. PIV cards indicate the level of access to classified matter or Special Nuclear Material for which the holder may be eligible, hereinafter referred to as a “security clearance.” PIV cards also allow employees to enter, occupy, or leave Departmental sites and facilities. From October 2015 through May 2018, more than 10,000 Federal and contractor employees separated their employment association with the Department through retirement, resignation, removal, or death. This included over 2,000 individuals with security clearances.

The OIG has issued several reports that identified weaknesses in the Department’s controls over security clearance terminations and badge retrievals for separated employees. These reports found that unauthorized individuals could gain access to Department facilities due to problems with the Department’s clearance and badging controls, such as not retrieving

security badges from separated employees or not removing security clearances of separated employees in a timely manner. Because establishing and maintaining adequate access controls is important, we initiated this audit to determine whether the Department terminated security clearance and PIV card access for separated employees in accordance with Federal regulations and Department policies.

We found that the Department had not always terminated security clearance and PIV card access for separated Federal and contractor employees, as required. Federal regulations, Departmental orders, and other guidance documents establish several required control procedures that are designed to prevent access to Department sites and facilities when Federal and contractor employees separate their association with the Department. These controls include updating the Department's PIV card database in USAccess to reflect employee separations; recovering and destroying access PIV cards; and, where applicable, terminating separated employees' security clearances.

The problems identified with updating USAccess, destroying badges, and terminating security clearances for separated employees can be attributed to the fact that current requirements do not clearly delineate responsibility and accountability for access authorization termination actions. In addition, current directives do not require a formal security out-processing procedure or outline enforcement measures. According to a Headquarters security official, the current structure of the overall process is not producing the results needed to ensure that necessary safeguards are in place for the notification, retrieval, and destruction of PIV cards for separated employees. For example, the program offices are not meeting a requirement to terminate the Department's interest in an employee's security clearance and to complete the security termination form within 4 working days of separation. While some of the data issues identified can be attributed to the deficiency in assignment of responsibility and authority, program officials also indicated that the information contained in identity management systems lacks standardization, which negatively affects access eliminations and other Department operations involving personnel information.

If clearances and PIV cards are not properly terminated, recovered, and destroyed, former employees may gain unauthorized access to Department buildings or information. Given the important role the Department plays in the Nation's security posture, we made recommendations designed to improve the Department's controls for terminating a security clearance and PIV card access for separated employees. Management generally concurred with our recommendations and identified actions it would take to address them. (DOE-OIG-21-12)

### **The Department of Energy's Wildland Fire Prevention Efforts at the Los Alamos National Laboratory**

We initiated this audit to determine whether the Los Alamos Field Office and the contractor were taking necessary actions to identify possible hazards associated with and mitigate the impacts of wildland fire.

We found that the contractor had not fully implemented activities designed to reduce the impact from wildland fire. Specifically, we found that mitigation measures such as tree thinning, which are necessary to reducing the risk of crown fires, were not always performed, resulting in an increased potential for a wildland fire to spread. In addition, not all fire roads were maintained in a state to ensure safe passage for firefighters and equipment responding to wildland fires in undeveloped areas, which could create dangerous conditions for emergency responders and delay response times. Further, contractor officials could not demonstrate that annual planning and preparedness activities were completed as prescribed in the Wildland Fire Management Plan. Without documenting planning and preparedness activities, there was no assurance that all prevention and mitigation options were considered and that the site was fully prepared for wildland fire events.

These issues occurred, in part, because the contractor had not developed a comprehensive, risk-based approach to wildland fire management in accordance with the Federal Wildland Fire Management Policy. In addition, the issues also occurred due to a lack of formality in the implementation of the Wildland Fire Management Plan. Further, a lack of Federal oversight of the contractor's wildland fire management activities contributed to the issues we identified.

Management concurred with our recommendations and proposed corrective actions that are consistent with our recommendations. The recommendations remain open and will be tracked in the Departmental Audit Report Tracking System. (DOE-OIG-21-13)

### **Management Letter on the Department of Energy's Unclassified Cybersecurity Program for Fiscal Year 2020**

This report is Official Use Only (OUO) and not available for public viewing.  
(DOE-OIG-21-14)

### **Western Federal Power System's Fiscal Year 2020 Financial Statement Audit**

The report presents the results of the independent certified public accountants' audit of the Western Federal Power System's combined balance sheets, as of September 30, 2020, and 2019, and the related statements of revenues and expenses, changes in capitalization, and cash flows for the years then ended.

To fulfill the OIG's audit responsibilities, we contracted with the independent public accounting firm of KPMG to conduct the audit, subject to our review. KPMG is responsible for expressing an opinion on the Western Federal Power System's financial statements and reporting on applicable internal controls and compliance with laws and regulations. The OIG monitored audit progress and reviewed the audit report and related documentation. This review disclosed no instances where KPMG did not comply, in all material respects, with generally accepted Government auditing standards. The OIG did not express an independent opinion on the Western Federal Power System's financial statements.



KPMG concluded that the combined financial statements present fairly, in all material respects, the respective financial position of the Western Federal Power System as of September 30, 2020, and 2019, and the results of its operations and its cash flow for the years then ended, in accordance with United States generally accepted accounting principles.

As part of this review, the auditors also considered the Western Federal Power System's internal controls over financial reporting and tested for compliance with certain provisions of laws, regulations, contracts, and grant agreements that could have a direct and material effect on the determination of financial statement amounts. The audit did not identify any deficiency in internal control over financial reporting that is considered a material weakness. (DOE-OIG-21-15)

### **The Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2020**

We initiated this evaluation to determine whether the FERC unclassified cybersecurity program adequately protected data and information systems.

Based on FY 2020 test work performed by KPMG, nothing came to our attention to indicate that attributes required by OMB and the National Institute of Standards and Technology were not incorporated into FERC's unclassified cybersecurity program for each of the major topic areas tested. In particular, FERC had implemented information technology security controls for various areas such as risk management, data protection and privacy, and security training, among others.

While FERC's cybersecurity program was effective overall, we identified a segregation of duties issue in a FERC application. Specifically, we found a user was granted conflicting privileges in the system that created an internal control weakness. Although FERC had designed a control to prevent such an issue from occurring, it had not been effectively implemented. This issue was concerning because the conflicting roles could have potentially allowed the user to both create and approve certain items in the system. Given the segregation of duties weakness, we issued a notice of finding and recommendations to FERC. Management provided corrective actions that are responsive to our recommendations; therefore, a management decision is not required. (DOE-OIG-21-16)

### **The Department of Energy's Unclassified Cybersecurity Program - 2020**

The Department operates many facilities across the Nation that depend on information technology systems and networks for essential operations required to accomplish its national security, research and development, and environmental management missions. As information technology continues to evolve, there are greater opportunities for efficiencies and accessibility to information but also increased cybersecurity threats. In its *Federal Information Security Modernization Act of 2014 Fiscal Year 2019 Report to Congress*, OMB reported that the number of agency-reported incidents across the Federal Government decreased by 8 percent between FY 2018 and FY 2019. However, this decline in incidents did not at all indicate a reduction in the cybersecurity threat posed to the Federal Government. In fact, the systems used to support the Department's various missions

continue to face millions of cybersecurity threats each year, ranging from unsophisticated hackers to advanced persistent threats using state-of-the-art intrusion tools and techniques. In addition, during FY 2020, the Department faced the unprecedented challenge of maintaining security over its information and systems even as a large component of its workforce worked remotely in response to COVID-19.

The *Federal Information Security Modernization Act of 2014* requires Federal agencies to develop, implement, and manage agency-wide information security programs. In addition, Federal agencies are required to provide acceptable levels of security for the information and systems that support their operations and assets. As required by the *Federal Information Security Modernization Act of 2014*, the OIG conducted an independent evaluation to determine whether the Department's unclassified cybersecurity program adequately protected its data and information systems. This report documents the results of our evaluation of the Department's cybersecurity program for FY 2020.

We determined that opportunities existed for the Department, including NNSA, to improve the protection of unclassified information systems and data. The Department had taken actions over the past year to address previously identified weaknesses related to its cybersecurity program. In particular, programs and sites made progress remediating weaknesses identified in our FY 2019 evaluation, which resulted in the closure of 42 of 54 (78 percent) prior year recommendations. Although these actions were positive, our current evaluation identified weaknesses in areas including system integrity of web applications, configuration management, vulnerability management, access controls, and contingency planning, many of which were consistent with our prior reports.

The weaknesses identified throughout our evaluation of the Department's unclassified cybersecurity program occurred for a variety of reasons. For instance, the identified weaknesses related to system integrity of web applications generally occurred because those applications were configured without implementing adequate security controls designed to reject malicious input. In addition, vulnerability management programs at the sites reviewed did not always include testing processes and procedures to identify vulnerabilities related to attacks against web application functionality. We also noted that vulnerability management weaknesses existed at one location because the vulnerability management process was not fully effective in addressing known vulnerabilities, including those related to unsupported software and missing patches.

To correct the cybersecurity weaknesses identified throughout the Department, we made 83 recommendations to programs and sites during FY 2020 to include those identified during this evaluation and in other issued reports. Corrective actions to address each of the recommendations, if fully implemented, should help to enhance the Department's unclassified cybersecurity program. In some instances, we also provided opportunities for improvement at locations reviewed but did not issue them as formal findings and recommendations. Because there are no recommendations included in this report, a management decision is not required. (DOE-OIG-21-18)

## INSPECTION REPORTS

### **Evaluation of the Aircraft Monitor and Control System’s Nuclear Certification**

The National Nuclear Security Administration (NNSA) and the Department of Defense (DoD) have a long-standing agreement of joint responsibilities for design and testing requirements of the Aircraft Monitor and Control (AMAC) system. In November 2019, the Department of Energy and DoD Offices of Inspector General announced a joint evaluation of the AMAC system’s nuclear certification. The DoD OIG’s objective was to determine whether testing conducted on the AMAC system for DoD nuclear weapon capable delivery aircraft meets the DoD and Department of Energy nuclear certification requirements. Our objective was to determine the extent to which the Department of Energy provided oversight of the AMAC system testing requirements for nuclear weapons delivery.

While NNSA was aware of and engaged in addressing the challenges posed with AMAC system testing requirements for nuclear delivery, we found opportunities to strengthen NNSA’s oversight. Specifically, NNSA’s oversight was impacted by disagreements with the Air Force. There was discord between the two Federal agencies on the number of aircraft to test, as well as changes to the test requirements made by the Air Force outside of the AMAC Project Officers Group. Disagreements between NNSA and the Air Force on AMAC tests to establish compatibility between the delivery aircraft and the nuclear weapon have occurred since at least 2008. These disagreements resulted in NNSA and the Air Force engaging in prolonged exchanges that delayed aircraft tests needed to establish or reaffirm compatibility, weapon reliability, and nuclear safety.

These challenges to NNSA’s oversight of the AMAC system testing requirements for nuclear weapons delivery occurred because NNSA’s process for resolving interagency differences did not have specified timeframes, which resulted in some delays for resolution of issues between the two Federal agencies where agreement could not be reached. In addition, NNSA and Sandia National Laboratories accepted the final versions of the Certification Requirements Plans in good faith and did not always perform followup reviews. Finally, there are fundamental inconsistencies between the Memorandum of Understanding between NNSA and the Air Force, the AMAC Project Officers Group Charter, and the DoD/Air Force Manual.

Management generally concurred with the recommendations and provided corrective actions that are responsive to our recommendations; therefore, a management decision is not required. (DOE-OIG-21-06)

### **Department of Energy’s Compliance with Executive Order 13950, Combating Race and Sex Stereotyping**

On September 22, 2020, President Donald J. Trump issued *Executive Order 13950, Combating Race and Sex Stereotyping*. The Executive Order required that Federal agencies, Federal grantees, Federal contractors, and the Uniformed Services take action to combat divisive concepts, race or sex stereotyping, and race or sex scapegoating. Additionally, the Executive Order required each agency head to request that the agency’s OIG thoroughly review and assess compliance with the Executive Order no later than December 31, 2020,

and annually thereafter, and report to OMB. The Department requested the OIG to perform this review. As such, we initiated this inspection to review and assess the Department's compliance with the requirements of Executive Order 13950.

We found that the Department's Office of Economic Impact and Diversity, working in conjunction with the Office of Management, and NNSA, had made progress implementing the Executive Order. Specifically, the Department had complied with Executive Order agency requirements by assigning a senior political appointee in Economic Impact to be responsible for ensuring compliance with the requirements of the Executive Order. Also, the senior political appointee appropriately requested that the OIG review the Department's compliance with the Executive Order. Finally, on November 24, 2020, the Department's Deputy Secretary issued a memorandum to the Heads of Departmental elements stating that the Department must comply with the Executive Order. We further noted that the Department had taken steps to comply with the Executive Order in the areas of contracts and grants, spending, and training. (DOE-OIG-21-10)

### **Allegation on Weapons Quality Assurance at the Kansas City National Security Campus**

Established by Congress in 2000, NNSA is a semi-autonomous agency within the Department responsible for enhancing national security through the military application of nuclear science. One of NNSA's core missions is to ensure that the U.S. maintains a safe, secure, and reliable nuclear stockpile through the application of science, technology, engineering, and manufacturing.

One of the eight sites that comprise NNSA is the Kansas City National Security Campus (KCNSC) located near Kansas City, Missouri. KCNSC is responsible for manufacturing and procuring non-nuclear components for nuclear weapons, including electronic, mechanical, quality assurance and engineered material components.

In September 2019, the OIG received two serious allegations of non-compliance with nuclear weapon product designs that, if true, could have had a detrimental effect on the safety and reliability of the nuclear stockpile. Specifically the allegations stated that KCNSC accepted: (1) parts 2A3555 and 2A3557 flex cables despite those flex cables failing continuity testing; and (2) part 3A3917 rigid-flex cables that did not conform to their design's specifications; and that KCNSC did not consult the design agency, Sandia National Laboratories, regarding the actual methods used to produce these rigid-flex cables.

We partially substantiated the allegations. Specifically, we substantiated that the KCNSC incorrectly accepted a limited number of parts 2A3555 and 2A3557 flex cables that were erroneously reported to have passed continuity testing but had, in fact, failed the continuity testing. We attributed this to the continuity testing subcontractor's failure to update its testing requirements. Based on our work, KCNSC either scrapped the flex cables or determined that they were acceptable for use through the Specification Exception Release Process.

We substantiated that the KCNSC had part 3A3917 rigid-flex cables manufactured in a manner that did not conform to the design's specification. We attributed this to the poor communication between the design and production agency regarding the change to a copper foil construction. However, we were unable to substantiate that the KCNSC had not consulted with the design agency regarding the actual method used to produce Part 3A3917. According to both the Department and contractor officials, the manufactured 3A3917 rigid-flex cables were reviewed and determined to be acceptable for use. In addition, NNSA completed a root-cause analysis designed to prevent issues in other product lines.

Because of the quick action taken by NNSA in response to our management notification memos and inspection findings, there is no expected impact as a result of these allegations. Therefore, we have no additional recommendations. (DOE-OIG-21-17)

## SEMIANNUAL REPORTING REQUIREMENTS INDEX

This table identifies the report sections that meet each reporting requirement prescribed by the Inspector General Empowerment Act of 2016.

REPORTING REQUIREMENT	SECTION	PAGE
Review of Legislation and Regulations	4(a)(2)	15
Total Number of Issued Investigative Reports	5(a)(17)(A)	4
Referrals to the Department of Justice for Criminal Prosecution	5(a)(17)(B)	4
Total Number of Persons Referred to the State/Local Prosecuting Authorities for Criminal Prosecution	5(a)(17)(C)	4
Total Number of Indictments and Criminal Informations During the Reporting Period That Resulted from Any Prior Referral to Prosecuting Authorities	5(a)(17)(D)	4
Description of the Metrics Used for Developing the Data for the 5(a)(17) Statistical Tables	5(a)(18)	4–5
Investigations Involving Senior Government Employees	5(a)(19)	16
Instances of Whistleblower Retaliation	5(a)(20)	16
Detailed Description of Any Attempt by the Department to Interfere with the Independence of the OIG	5(a)(21)	15
Reviews Closed and Not Disclosed to the Public	5(a)(22)	15
Recommendations for Corrective Action to Significant Problems	5(a)(2)	32–41
Previous Reports' Recommendations for Which Corrective Action Has Not Been Implemented	5(a)(3)	18–21
Matters Referred to Prosecutive Authorities	5(a)(4)	23–31
Audit Reports Issued in This Reporting Period	5(a)(6)	11–13
Summary of Significant Reports	5(a)(7)	32–41
Reports with Questioned Costs	5(a)(8)	5
Reports with Recommendations That Funds Be Put to Better Use	5(a)(9)	5
Previous Audit Reports Issued with No Management Decision Made by End of This Reporting Period	5(a)(10)	17
Significant Revised Management Decisions	5(a)(11)	17
Significant Management Decisions with Which the OIG Is in Disagreement	5(a)(12)	17
Federal Financial Management Improvement Act-related Reporting	5(a)(13)	N/A
Peer Review Results	5(a)(14–16)	22

## ABOUT THE DEPARTMENT AND OIG

**The U.S. Department of Energy** is headquartered in Washington, DC and is responsible for the Energy Information Administration, the National Nuclear Security Administration, 21 preeminent research laboratories and facilities, 4 power marketing administrations, 9 field offices, and 10 program offices which help manage the Department's mission with more than 15,000 Federal employees and a host of contract employees. The Department is the Nation's top sponsor of research and development and has won more Nobel Prizes and research and development awards than any other private sector organization, and twice as many as all other Federal agencies combined. The mission of the Department is to ensure America's security and prosperity by addressing its energy, environmental, and nuclear challenges through transformative science and technology solutions.

**The OIG's** mission is to strengthen the integrity, economy, and efficiency of the Department's programs and operations. The OIG has the authority to inquire into all Department programs and activities as well as the related activities of persons or parties associated with Department grants, contracts, or other agreements. As part of its independent status, the OIG provides the Secretary with an impartial set of "eyes and ears" to evaluate management practices. With approximately 293 employees, the organization strives to be a highly effective organization that promotes positive change.

## OIG HOTLINE CONTACT INFORMATION

Contact the OIG Hotline if you suspect fraud, waste, or abuse involving Department programs, or by a Department employee, contractor, or grant recipient.

<b>Complaint Form</b>	<a href="https://www.energy.gov/ig/complaint-form">https://www.energy.gov/ig/complaint-form</a>
<b>Toll Free Telephone Number</b>	1-800-541-1625
<b>Washington DC Metro Telephone Number</b>	202-586-4073
<b>Fax</b>	202-586-4902
<b>Email Address</b>	<a href="mailto:ighotline@hq.doe.gov">ighotline@hq.doe.gov</a>
<b>Physical Address</b>	U.S. Department of Energy 1000 Independence Ave, SW Washington, DC 20585

## FEEDBACK AND MEDIA INQUIRIES

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](mailto:OIG.Reports@hq.doe.gov) and include your name, contact information, and the report number.

For media inquiries, please email [OIGPublicAffairs@hq.doe.gov](mailto:OIGPublicAffairs@hq.doe.gov).