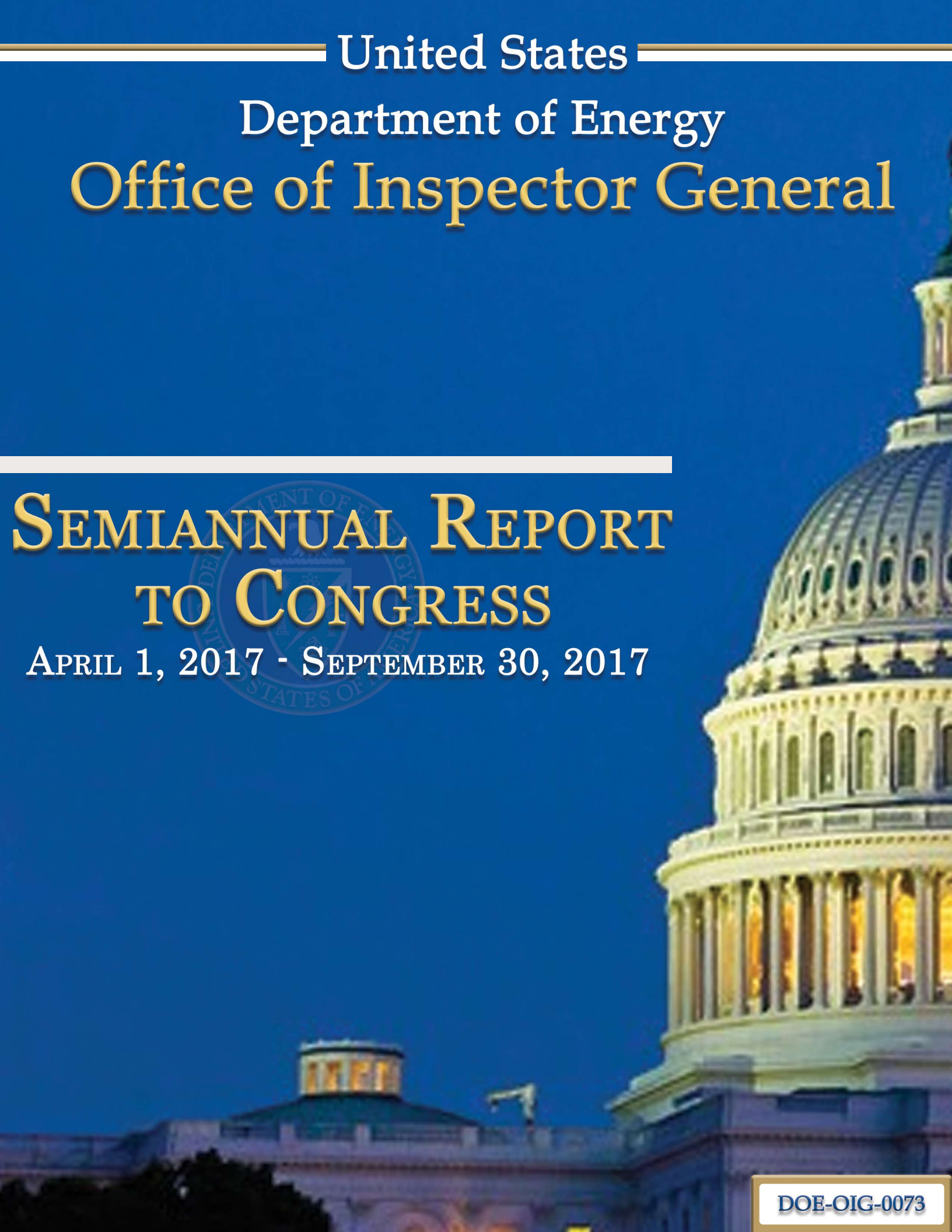
United States

Department of Energy

Office of Inspector General

Semiannual Report to Congress

April 1, 2017 - September 30, 2017



DOE-OIG-0073

Table of Contents

Message from Acting Inspector General

It is with pleasure that I present the Semiannual Report to Congress for the period ending September 30, 2017. This report highlights the work of the Office of the Inspector General (OIG) within the U.S. Department of Energy complex.

Over the past 6 months, much of our efforts were dedicated to mitigating cyber-security vulnerabilities. The Department of Energy operates nearly 100 entities across the Nation and depends on information technology (IT) systems and networks for essential operations required to accomplish its national security, research and development, and environmental management missions. The systems used to support the Department's various missions face millions of cyber threats each year ranging from unsophisticated hackers to advanced persistent threats using state-of-the-art intrusion tools and techniques. For instance, the Department responded to more than 18,000 potential incidents in FY 2017 related to areas such as malicious code, information and system compromise and unauthorized use. Many of these malicious attacks were designed to steal information and disrupt, deny access, degrade, or destroy the Department's information systems.

Our audit and inspection staff has been instrumental in detecting potential cyber-security risks within the Department. Of the 19 reports issued during this reporting period, several focused on cyber-security related activities within Energy operations and programs. For example, our review on The Office of Enterprise Assessments Testing Incident at the 2016 Department of Energy Cyber Conference, OIG-SR-17-05, raised concerns about the lack of coordination among Department elements in addressing a specific cyber-security assessment. Our report on The Department of Energy's Implementation of Multifactor Authentication Capabilities, DOE-OIG-17-08, found the Department made progress towards fully implementing multi-factor authentication, but weaknesses related to ensuring adequate protections over access to network and application resources continued to exist. Furthermore, followup reporting on Bonneville Power Administration's Cybersecurity Program, DOE-OIG-17-06 showed that Bonneville made efforts to improve its cybersecurity program since our previous review. However, our report disclosed that Bonneville had not implemented a fully effective cybersecurity program and we continued to identify weaknesses in the areas of access controls, vulnerability and configuration management, and contingency planning. We also noted officials had not ensured all systems contained up-to-date security controls.

Also during this period, our criminal investigators engaged in joint efforts with other law enforcement organizations to combat cybersecurity threats targeting the Department's operational, programmatic, and financial well-being. For example, our investigators uncovered that a former technician utilized a Lawrence Livermore National Laboratory computer and network to view and obtain unlawful images. As a result of the work of our office, this individual was sentenced to 135 months incarceration. Another investigation by our office revealed that a former contractor employee purchased unauthorized and unnecessary items through the Kansas City National Security Campus procurement system which were subsequently sold for personal gain on eBay. This individual was sentenced to 12 months and 1 day incarceration, 3 years of supervised release, and ordered to pay over $50,000 in restitution. It is also worth noting that in FY 2017, our criminal investigators are seeing more instances of impersonation of procurement officials and impersonation of legitimate vendors. One instance noted this year resulted in a payment by Pacific Northwest National Laboratory (PNNL) of approximately $530,000 to a fictitious vendor who, via email correspondence, requested a change in bank routing number by impersonating a current legitimate PNNL subcontractor. We are actively investigating this instance and are closely monitoring other phishing attacks throughout the Department.

The Office of Inspector General recognizes the benefit of continued collaboration with Department officials that is designed to diminish cyber-security threats presented throughout the agency. We will continue to foster these relationships to achieve our mission to prevent fraud, waste, and abuse.

April G. Stephenson

INVESTIGATIONS

INVESTIGATIVE ACTIVITIES

Cases Open as of April 1, 2017	199
Cases opened	36
Cases closed	41
Cases Open as of September 30, 2017	194
Multi-Agency Task Force Cases Opened During Period	6
Qui Tam[1] Investigations Opened During Period	1
Total Open Qui Tam Investigations as of September 30, 2017	12
Total Investigative Reports[2] Issued During Period	13
Recommendations to management for positive change and other actions	38
Administrative discipline and other management actions	7
Suspensions/Debarments	23
Total Persons[3] Referred to a Prosecuting Authority	36
Department of Justice Referrals	31
State/Local Referrals	5
Referrals accepted for prosecution[4]	27
Total Indictments[5]/Criminal Informations	13
Indictments/Criminal Informations Resulting from Prior Period Referrals	13
Criminal convictions	10
Pre-trial diversions	3
Civil actions	9
Dollars Recovered[6] (Fines, Settlements, Recoveries)	$9,950,880.67

HOTLINE RESULTS

Total Hotline calls, emails, letters, and other complaints (contacts)[7]	871
Hotline contacts resolved immediately/redirected/no further action	654
Hotline contacts predicated for evaluation	217
Total Hotline predications processed this reporting period[8]	227
Hotline predications transferred to OIG Program Office	17
Hotline predications referred to Department management or other entity for information/action	81
Hotline predications closed based upon preliminary OIG activity and review	122
Hotline predications open at the end of the reporting period	7

[1]For more information on Qui Tams, go to: http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00932.htm
[2]Investigative Reports issued by the Office of Investigations include Reports of Investigation and Investigative Reports to Management.
[3]Persons is defined as an individual or an entity. For example, two co-owners and their business entity would be counted as three persons.
[4]Some referrals accepted during the 6-month period were referred for prosecution during a previous reporting period.
[5]Sealed Indictments are included.
[6]Some of the money collected was the result of investigations involving multiple agencies.
[7]This number includes any contact that required Hotline staff review including re-contacts for additional information and requests for disposition.
[8]This includes 10 predications carried over from the last semiannual reporting period.

AUDITS AND INSPECTIONS

AUDITS AND INSPECTIONS ACTIVITIES

Total Reports Issued	**19**
Audit Reports Issued	15
Inspection Reports Issued	4

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 March 31, 2017:[1]	8	$49,078,867
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: [2]	1	$674,774
(i) Agreed to by management:		$674,774
(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:	7	$48,404,093

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 March 31, 2017:[1]	31	$943,013,389	$5,172,560	$948,185,949
Reports issued during the reporting period that include questioned or unsupported costs (regardless of whether a decision on dollars has been made):	2	$4,012,957	$46,050	$4,059,007
Reports that include questioned and/or unsupported costs for which a decision on dollars was made during the reporting period:[2]	11	$233,665,006	$0	$233,665,006
(i) Value of disallowed costs:		$5,685,626	$0	$5,685,626
(ii) Value of costs not disallowed:		$227,979,380	$0	$227,979,380
Reports that include questioned and/or unsupported costs for which decisions on dollars have not been made at the end of the reporting period:	22	$713,361,340	$5,218,610	$718,579,950

Definitions:

Better Use of Funds: *Funds that could be used more efficiently by implementing recommended actions.*

Management decision: *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: *A cost that is (1) unnecessary; (2) unreasonable; or (3) an alleged violation of law, regulation, contract, etc.*

Unsupported costs: *A cost that is not supported by adequate documentation.*

[1]Includes reports for which the Department may have made some decisions on dollars but not all issues within the report have been resolved.

[2]Does not include reports for which the Department has made decisions on some aspects of the report but not all.

During this reporting period, the following positive outcomes resulted from OIG work conducted during the current or previous reporting periods.

INVESTIGATIVE OUTCOMES

Settlement Reached in Savannah River Site Qui Tam Investigation
The U.S. Department of Justice entered into a $4.6 million civil settlement agreement with a subcontractor on the Mixed Oxide Fuel Fabrication project at the Savannah River Site to resolve allegations made under the Civil False Claims Act. The qui tam investigation determined the subcontractor certified and billed the Government for reinforcing steel bars that met the Nuclear Quality Assurance-1 standard when the steel bars did not meet the standard. This investigation was coordinated with the U.S. Attorney's Office, Northern District of Georgia, and the U.S. Department of Justice's Civil Fraud Section, Washington, D.C.

Sentencing in Transportation of Child Pornography Investigation
A former technician at the Lawrence Livermore National Laboratory, was sentenced to 135 months incarceration in the U.S. District Court for the Eastern District of California on Transportation of Child Pornography charges. The investigation was successful in removing a serious threat from the community. The filing of the Information and plea agreement were reported in the March 31, 2017, Semiannual Report to Congress. This was a joint investigation with the Federal Bureau of Investigation.

Sentencings in Bribery Investigation
A former senior Department employee pleaded guilty to Conspiracy and Bribery violations and was sentenced in the U.S. District Court for the District of Maryland to 18 months incarceration, 3 years of probation and ordered to pay $469,287 in restitution, a $200 special assessment fee and a $75,000 fine. A prospective Department contractor employee was sentenced in U.S. District Court for the District of Maryland to 1 year and 1 day incarceration, 1 year of probation, ordered to pay $15,000 in fines with a $100 special assessment fee, and directed to forfeit $7,000 that was paid in bribe money. A former Department contractor employee was sentenced in U.S. District Court for the District of Maryland to 18 months incarceration to be followed by 1 year of supervised release and ordered to pay $70,000 in restitution with a $25,000 fine and a $200 special assessment fee. Additionally, a co-conspirator was sentenced in U.S. District Court for the District of Columbia to 2 years of probation. As reported in the March 31, 2017, Semiannual Report to Congress, a two-count Information was filed against the former senior Department employee, the prospective Department contractor employee pleaded guilty to one count of Bribery, and the co-conspirator pleaded guilty to one count of False Statements. The investigation determined the former senior Department employee solicited and was paid bribes to secure Department contracts for various companies and individuals, the prospective Department contractor employee paid bribes to secure a contract with the Department, the former Department contractor paid bribes to secure and maintain its contract with the Department, and the co-conspirator made false statements to federal agents related to bribery payments made to the senior Department employee. This is an ongoing, joint investigation with the Federal Bureau of Investigation.

Sentencing in Grant Fraud Investigation

The former Chief Executive Officer (CEO) of a non-profit organization receiving Department funds was sentenced in the U.S. District Court of Minnesota to 48 months of incarceration, 2 years supervised release and ordered to pay $387,063 in restitution with a special assessment fee of $1,600. As reported in the March 31, 2017, Semiannual Report to Congress, the CEO pleaded guilty to charges of Conspiracy to Commit Theft Concerning Programs Receiving Federal Funds, Mail Fraud, Wire Fraud, and Theft Concerning Programs Receiving Federal Funds. The investigation determined the former CEO diverted at least $250,000 in grant funds to pay personal expenses, including the purchase of automobiles, airline tickets, hotel expenses, rental cars, a Caribbean cruise, and paying his son $140,000 for work not performed. This is a joint investigation with the Federal Bureau of Investigation, Internal Revenue Service Criminal Investigation Division, and Department of Health and Human Services OIG.

Guilty Plea by Former National Nuclear Security Administration Contractor

A former National Nuclear Security Administration (NNSA) contractor pleaded guilty in the District of South Carolina to Conspiracy. As previously reported, two NNSA contractors were indicted on thirteen counts of Wire Fraud, one count of Conspiracy, and one count of Theft of Government Funds. As reported in the March 31, 2017, Semiannual Report to Congress, the other contractor pleaded guilty to Conspiracy. The investigation determined that from 2009 to 2015 the indicted subjects stole over $6.5 million of Department funds by submitting fictitious invoices to NNSA's contractors for materials supposedly used to build the Mixed-Oxide (MOX) Fuel Fabrication Facility located at the Savannah River Site. A portion of the stolen Department funds were used to purchase gratuities for other contractors at the MOX Project. In addition to these defendants, four other former contractors were charged with violations of Gratuities and False Statements. This is an ongoing joint investigation with the Federal Bureau of Investigation.

HOTLINE OUTCOMES

In response to a Hotline referral regarding an allegation of blocked emergency exit doors in a building at the Y-12 National Security Complex, the National Nuclear Security Administration (NNSA) performed a focused inspection and determined three egress paths were blocked. NNSA cleared one of the pathways immediately and required Consolidated Nuclear Security, the contractor which operates the Y-12 National Security Complex, to prepare a formal corrective action plan with causal analysis that detailed actions taken for any performance problem.

After receiving a Hotline referral, the Office of the Chief Human Capital Officer conducted a review into allegations of prohibited personnel practices within the Office of the Chief Financial Officer (CFO). A former CFO employee alleged that while assigned to the program office, rating officials failed to provide an annual performance review and associated performance award payment in a timely manner. CFO management acknowledged their failure and took corrective action.

Based on a Hotline referral, the Office of Environmental, Health, Safety and

Security (EHSS) conducted a review into an allegation regarding restricted area access protocols. The complainant contacted the Hotline alleging a security violation after witnessing another individual enter a room being used for a restricted briefing that was not adequately secured or labeled as restricted access. Subsequent to a review by EHSS, which determined while no security violation had occurred, Chapter 2 of the Headquarters Facilities Master Security Plan was rewritten. Additionally, a requirement to memorialize security protocols via a written Security Plan was implemented.

AUDIT AND INSPECTION OUTCOMES

In response to our report on The Department of Energy's $12.3 Billion Waste Treatment and Immobilization Plant – Quality Assurance Issues – Black Cells, DOE/IG-0863, the Department completed a vertical slice audit on the procurement of a safety-related vessel, the Low Activity Waste Caustic Scrubber, in May 2017. The Department concluded that, with one exception, the Low Activity Waste Caustic Scrubber Vessel was received and accepted satisfactorily. The Department will continue to followup on actions taken by the responsible contractor to correct quality assurance program issues. Our report revealed a number of instances where quality assurance requirements were not completely followed for processing vessels installed in black cell and/or hard to reach areas. Specifically, we found that Bechtel had not obtained or maintained documentation related to welds or radiographs, which were required by contract.

In response to findings identified in this annual evaluation of the Department's unclassified cybersecurity program (The Department of Energy's Unclassified Cybersecurity Program – 2016, DOE-OIG-17-01), we determined that actions were taken to correct issues related to access controls, system integrity of Web applications, and configuration and vulnerability management of desktop and network systems and devices. These actions resulted in the closure of numerous prior year weaknesses at programs and sites across the Department.

In response to our 2016 audit on Bonneville Power Administration's Contractor Workforce, DOE-OIG-17-03, Bonneville Power Administration reported that it had completed multiple actions to address concerns we raised regarding the risk of personal services contracts. For example, Bonneville updated classroom training and manager handbooks to more clearly explain personal services relationships. Additionally, it created a new compliance function within its Supplemental Labor Management Office to assess and monitor adherence to procurement policy, including policies prohibiting personal services contracts.

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 during the period April 1, 2017, through September 30, 2017.

AUDITS

The following identifies all audit reports issued between April 1, 2017, and September 30, 2017.

DATE ISSUED	REPORT TITLE	NUMBER OF RECS	BETTER USE OF FUNDS	QUESTIONED COSTS	UNSUPPORTED COSTS	PAGE
Apr 11, 2017	Followup on the Small Business Innovation Research and Small Business Technology Transfer Programs (OAI-M-17-06)	7			$46, 050	34
Apr 13, 2017	Followup on the K Basin Sludge Removal Project (OAI-L-17-04)	0				35
Apr 21, 2017	The Department of Energy's Improper Payment Reporting in the Fiscal Year 2016 Agency Financial Report (OAI-FS-17-09)	0				35
Apr 26, 2017	Department of Energy's West Valley Demonstration Project (DOE-OIG-17-05)	8				35
May 11, 2017	Audit Coverage of Cost Allowability for Princeton University During Fiscal Years 2013 Through 2015 Under Department of Energy Contract No. DE-AC02-09CH11466 (OAI-V-17-03)	0				36
May 17, 2017	Audit Coverage of Cost Allowability for Battelle Memorial Institute Under its Contract to Manage the Pacific Northwest National Laboratory During Fiscal Years 2013 and 2014 Under Department of Energy Contract No. DE-AC05-76RL01830 (OAI-V-17-04)	3				38
May 31, 2017	Maintenance and Testing of Intrusion Detection and Alarm Systems (OAI-L-17-06)	0				39
Jun 15, 2017	The Office of Enterprise Assessments Testing Incident at the 2016 Department of Energy Cyber Conference (OIG-SR-17-05)	4				40
Jul 10, 2017	Review of Training Expenses at the Department of Energy's Office of Fossil Energy (OAI-M-17-08)	2				41

DATE ISSUED	REPORT TITLE	NUMBER OF RECS	BETTER USE OF FUNDS	QUESTIONED COSTS	UNSUPPORTED COSTS	PAGE
Jul 20, 2017	Audit Coverage of Cost Allowability for Consolidated Nuclear Security LLC during July 1, 2014, through September 30, 2015, under Department of Energy Contract No. DE-NA-0001942 (OAI-V-17-05)	1		$4,012,957		42
Aug 16, 2017	Followup on Bonneville Power Administration's Cybersecurity Program (DOE-OIG-17-06)	5				43
Sep 12, 2017	Interim Storage of Transuranic Waste at the Department of Energy (OAI-L-17-07)	0				45
Sep 14, 2017	Quality Assurance Management at the Waste Isolation Pilot Plant (DOE-OIG-17-07)	3				46
Sep 21, 2017	The Department of Energy's Implementation of Multifactor Authentication Capabilities (DOE-OIG-17-08)	5				47
Sep 22, 2017	Allegation of Nepotism and Misuse of Position within the Office of Management (DOE-OIG-17-09)	4				48

INSPECTIONS

The following identifies all inspection reports issued between April 1, 2017, and September 30, 2017. [1]

DATE ISSUED	REPORT TITLE	NUMBER OF RECS	BETTER USE OF FUNDS	QUESTIONED COSTS	UNSUPPORTED COSTS	PAGE
Apr 20, 2017	Alleged Security and Safety Concerns at the Oak Ridge National Laboratory (OAI-L-17-05)	0				51
May 24, 2017	Construction Rework at the Mixed Oxide Fuel Fabrication Facility (OAI-M-17-07)	2				51
Jul 21, 2017	Alleged Tesa Access Issues At Lawrence Livermore National Laboratory (OAI-M-17-09)	4				52
Jul 25, 2017	Allegations of Mismanagement of the Human Reliability Program at the Oak Ridge National Laboratory (OAI-M-17-10)	1				53

[1]On September 15, 2017, Followup Review of Controls Over the Department's Classification of National Security Information, was revised to amend the section on classification self-assessment and decision reviews completed by the Department. We corrected the review period and percentages of the annual classification decision reviews and biennial classification program self-assessments the Office of Intelligence and Counterintelligence has completed.

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. We reviewed eight proposed regulations, bills, and/or letters during this reporting period.

Interference With IG Independence

The Department did not interfere or restrict communications between our office and Congress nor put in place any budgetary constraints designed to limit the capabilities of our office.

Resistance to Oversight Activities or Restricted/Significantly Delayed Access

Access to documents the OIG believed necessary to perform work was not restricted during this period.

Investigations Involving Senior Level Employees

During the reporting period April 1, 2017 through September 30, 2017, the following investigations that involved an 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 SES employee asked subordinates to lie to Equal Employment Opportunity investigator.	Closed; unsubstantiated	Yes	Oct 3, 2016	Lack of sufficient evidence for a criminal indictment
Allegation retired SES had conflict of interest with contractor prior to retirement.	Closed; unsubstantiated	No	N/A	N/A
Allegation former SES obstructed investigation and provided false statements to federal agents.	Open	Yes	Apr 18, 2017	Lack of sufficient evidence for a criminal indictment

FACTS AND CIRCUMSTANCES	STATUS AND DISPOSITION	REFERRED TO DOJ	DOJ DECLINATION	DECLINATION REASON
Allegation GS-15 employee solicited and accepted bribery payments	Open; pled guilty to Conspiracy and Bribery; sentenced to 18 months incarceration, 3 years of probation, $469,287 restitution, $75,000 fine	Yes	N/A	N/A

WHISTLEBLOWER RETALIATION COMPLAINTS

During the reporting period April 1, 2017 through September 30, 2017, there were no instances of confirmed whistleblower retaliation. However, during this period, the OIG received the following complaints under 41 USC Section 4712 and/or under the Presidential Policy Directive 19:

Complaints Received	5
Complaints Accepted for Investigation	3
Complaints Not Accepted for Investigation	2

COMMENTS NOT PROVIDED WITHIN 60 DAYS

For the reporting period April 1, 2017, through September 30, 2017, the Department failed to provide comments on the following report within 60 days.

DATE ISSUED	REPORT TITLE	LENGTH OF TIME TO RECEIVE COMMENTS
Ongoing	NNSA's Energy Savings Performance Contracts	151
Ongoing	National Ignition Facility	120
Ongoing	(KPMG) FY 2014 Savannah River Nuclear Solutions Incurred Costs	95
Sep 12, 2017	Interim Storage of Transuranic Waste at the Department of Energy (OAI-L-17-07)	64

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 six 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, 2012	Use of Noncompetitive Procurements to Obtain Services at the Savannah River Site (DOE/IG-0862)	The OIG has requested the Department temporarily delay submitting a management decision on the recommendations in this report, pending the outcome of an ongoing related review.

Recommendations Not Implemented

The following table identifies 68 reports with a total of 139[1] recommendations which were agreed to by the Department but have not been implemented as of September 30, 2017. The total potential cost savings associated with these reports is $378,063,386. 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 not available on the OIG website.]

DATE ISSUED	REPORT TITLE	TOTAL # OF OPEN RECS[2]	POTENTIAL MONETARY BENEFIT[3]
Dec 20, 2005	Assessment of Changes to the Internal Control Structure and Their Impact on the Allowability of Costs Claimed by and Reimbursed to Sandia Corporation Under Department of Energy Contract No. DE-AC04-94AL85000 (OAS-V-06-06)	1	$2,032,805

[1]Those recommendations that are not agreed to by management are not tracked by the Department as open/unimplemented recommendations. Since 2005, the Department has only failed to agree on 3 recommendations issued by the OIG.

[2] 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.

[3]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[2]	POTENTIAL MONETARY BENEFIT[3]
Jan 16, 2007	Assessment of Changes to the Internal Control Structure and their Impact on the Allowability of Costs Claimed by and Reimbursed to Sandia Corporation under Department of Energy Contract No.DE-AC04-94AL85000 (OAS-V-07-05)	1	$2,836,181
Dec 17, 2007	Beryllium Surface Contamination at the Y-12 National Security Complex (IG-0783)	1	
May 7, 2008	Assessment of Changes to the Internal Control Structure and Their Impact on the Allowability of Costs Claimed by and Reimbursed to Sandia Corporation, under the Department of Energy Contract, DE-AC04-94AL85000 for Fiscal Year 2006 (OAS-V-08-09)	1	$3,393,317
Nov 13, 2009	Management Controls over Selected Aspects of the Department of Energy's Human Reliability Program (OAS-M-10-01)	2	
Sep 22, 2010	The Department of Energy's Audit Resolution and Follow-up Process (IG-0840)	2	
Oct 5, 2010	Audit Coverage of Cost Allowability for Sandia Corporation During Fiscal Years 2007 AND 2008 under Department of Energy Contract NO. DE-AC04-94AL85000 (OAS-V-11-01)	1	
Feb 20, 2013	Assessment of Audit Coverage of Cost Allowability Sandia Corporation during Fiscal Years 2009 and 2010 under Department of Energy Contract No. DE-AC04-94AL85000 (OAS-V-13-07)	2	$12,760,295
Jun 24, 2013	Mitigation of Natural Disasters at Los Alamos National Laboratory (OAS-M-13-04)	1	
Sep 30, 2013	Department of Energy Quality Assurance: Design Control for the Waste Treatment and Immobilization Plant at the Hanford Site (IG-0894)	1	
Oct 24, 2013	The Department's Fleet Vehicles Sustainability Initiatives at Selected Locations (IG-0896)	3	
Jan 2, 2014	NNSA's Management of the $245 Million Nuclear Materials Safeguards and Security Upgrades Project Phase II (IG-0901)	2	
Feb 14, 2014	The Technology Transfer and Commercialization Efforts at the Department of Energy's National Laboratories (OAS-M-14-02)	1	
Apr 15, 2014	The Department of Energy's Management and Use of Mobile Computing Devices and Services (IG-0908)	1	
Apr 23, 2014	Assessment of Audit Coverage of the Cost Allowability for Sandia Corporation under Department of Energy Contract DE-AC04-94-AL-85000, for Fiscal Years 2011 and 2012 (OAS-V-14-10)	1	5,741,818

DATE ISSUED	REPORT TITLE	TOTAL # OF OPEN RECS[2]	POTENTIAL MONETARY BENEFIT[3]
Jun 26, 2014	The Department of Energy's Implementation of Voice over Internet Protocol Telecommunications Networks (IG-0915)	1	
Aug 6, 2014	Management of the National Nuclear Security Administration's Biosafety Laboratories (IG-0917)	1	
Sep 19, 2014	The Department of Energy's Management of Cloud Computing Activities (IG-0918)	1	
Sep 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
Oct 22, 2014	The Department of Energy's Unclassified Cybersecurity Program – 2014 (IG-0925)	2	
Nov 12, 2014	Follow-up Audit of Contractor Intergovernmental Personnel Act Assignments (IG-0928)	2	$3,000,000
Feb 26, 2015	Argonne National Laboratory Infrastructure Projects (OAS-M-15-02)	1	
Jun 10, 2015	Allegations Related to the Energy Information Administration's Reporting Process (DOE/IG-0940)	1	
Jun 12, 2015	Southwestern Federal Power System's Fiscal Year 2014 Financial Statement Audit (OAS-FS-15-11)	2	
Jun 22, 2015	The Department of Energy's Implementation of the Pilot Program for Agreements for Commercializing Technology (OAS-M-15-04)	1	
Jul 10, 2015	The National Nuclear Security Administration's Management of Support Service Contracts (OAS-M-15-05)	1	
Jul 16, 2015	Follow-up on Nuclear Safety: Safety Basis and Quality Assurance at the Los Alamos National Laboratory (DOE/IG-0941)	1	
Sep 3, 2015	The Department of Energy's Management of Electronic Mail Records (DOE/IG-0945)	3	
Sep 9, 2015	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)	1	$2,569,251
Nov 3, 2015	The Department of Energy's Unclassified Cybersecurity Program – 2015 (DOE-OIG-16-01)	1	
Nov 4, 2015	The Department of Energy's Cybersecurity Risk Management Framework (DOE-OIG-16-02)	2	

DATE ISSUED	REPORT TITLE	TOTAL # OF OPEN RECS[2]	POTENTIAL MONETARY BENEFIT[3]
Nov 17, 2015	Procurement of Parts and Materials for the Waste Treatment and Immobilization Plant at the Hanford Site (DOE-OIG-16-03)	2	
Dec 7, 2015	Issues Management at the Los Alamos Field Office (OAI-M-16-02)	2	
Jan 7, 2016	Information Technology Management Letter on the Audit of the Department of Energy's Consolidated Balance Sheet for Fiscal Year 2015 (OAI-FS-16-05) *Full Report Not Publically Available – Official Use Only*	1	
Jan 15, 2016	Management Letter on the Audit of the Department of Energy's Consolidated Financial Statements for Fiscal Year 2015 (OAI-FS-16-06)	2	
Feb 1, 2016	Corrective Action Program at the Waste Treatment and Immobilization Plant (OAI-M-16-06)	1	
Feb 25, 2016	Issues Management at the Los Alamos National Laboratory (DOE-OIG-16-07)	4	
Mar 1, 2016	The Department of Energy's Audit Resolution and Followup Process (DOE-OIG-16-08)	3	
Mar 21, 2016	Procurement Administration and Human Reliability Program Revocations Within the Office of Secure Transportation (OAI-M-16-07)	1	
Apr 1, 2016	Management and Oversight of Information Technology Contracts at the Department of Energy's Hanford Site (DOE-OIG-16-10)	1	$183,500,000
Apr 4, 2016	Followup on Western Area Power Administration's Critical Asset Production (DOE-OIG-16-11)	1	
Apr 26, 2016	The Department of Energy's Continued Support of the Texas Clean Energy Project Under the Clean Coal Power Initiative (OIG-SR-16-02)	3	
May 2, 2016	The Department of Energy's Energy Information Technology Services Federal Support Costs (DOE-OIG-16-12)	3	
Jul 7, 2016	Lawrence Livermore National Laboratory's Laser Inertial Fusion Energy Endeavor (OAI-M-16-13)	3	
Jul 14, 2016	Enriched Uranium Operations at the Y-12 National Security Complex (DOE-OIG-16-13)	1	
Jul 27, 2016	Battelle's Pacific Northwest National Laboratory Procurement Activities (OAI-M-16-14)	4	
Sep 29, 2016	Followup Audit of the Department's Continuity of Operations Planning (DOE-OIG-16-16)	2	
Oct 14, 2016	The Department of Energy's Unclassified Cybersecurity Program – 2016 (DOE-OIG-17-01)	1	

DATE ISSUED	REPORT TITLE	TOTAL # OF OPEN RECS[2]	POTENTIAL MONETARY BENEFIT[3]
Oct 31, 2016	Management Letter on the Southwestern Federal Power System's Fiscal Year 2015 Financial Statement Audit (OAI-FS-17-01)	2	
Nov 15, 2016	Management Letter on the Southwestern Federal Power System's Fiscal Year 2015 Financial Statement Audit (OAI-FS-17-01)	2	
Dec 29, 2016	Bonneville Power Administration's Contractor Workforce (DOE-OIG-17-03)	2	
Jan 3, 2017	Audit Coverage of Cost Allowability for Jefferson Science Associates LLC During Fiscal Years 2011 – 2014 Under Department of Energy Contract No. DE-AC05-06OR23177 (OAI-V-17-01)	1	$5,031
Jan 10, 2017	Management Letter on the Audit of the Department of Energy's Consolidated Financial Statements for Fiscal Year 2016 (OAI-FS-17-05)	9	
Jan 12, 2017	Information Technology Management Letter on the Audit of the Department of Energy's Consolidated Financial Statements for Fiscal Year 2016 (OAI-FS-17-07) *Full Report Not Publically Available – Official Use Only*	2	
Jan 17, 2017	Followup Review of Controls Over the Department's Classification of National Security Information (DOE-OIG-17-04)	2	
Feb 15, 2017	Quality Assurance for River Corridor Closure Contract Procurements (OAI-M-17-05)	3	$270,894
Feb 23, 2017	Management of Suspended Procurements at the Waste Treatment and Immobilization Plant Project (OIG-SR-17-04)	3	$1,900,000
Apr 11, 2017	Followup on the Small Business Innovation Research and Small Business Technology Transfer Programs (OAI-M-17-06)	4	$46,050
Apr 26, 2017	Department of Energy's West Valley Demonstration Project (DOE-OIG-17-05)	8	
May 17, 2017	Audit Coverage of Cost Allowability for Battelle Memorial Institute Under its Contract to Manage the Pacific Northwest National Laboratory During Fiscal Years 2013 and 2014 Under Department of Energy Contract No. DE-AC05-76RL01830 (OAI-V-17-04)	3	
May 19, 2017	Construction Rework at the Mixed Oxide Fuel Fabrication Facility (OAI-M-17-07)	1	
Jun 15, 2017	The Office of Enterprise Assessments Testing Incident at the 2016 Department of Energy Cyber Conference (OIG-SR-17-05)	1	
Jul 10, 2017	Review of Training Expenses at the Department of Energy's Office of Fossil Energy (OAI-M-17-08)	1	

DATE ISSUED	REPORT TITLE	TOTAL # OF OPEN RECS[2]	POTENTIAL MONETARY BENEFIT[3]
Jul 21, 2017	Alleged Tesa Access Issues at Lawrence Livermore National Laboratory (OAI-M-17-09)	4	
Jul 25, 2017	Allegations of Mismanagement of the Human Reliability Program at the Oak Ridge National Laboratory (OAI-M-17-10)	1	
Sep 14, 2017	Quality Assurance Management at the Waste Isolation Pilot Plant (DOE-OIG-17-07)	3	
Sep 21, 2017	The Department of Energy's Implementation of Multifactor Authentication Capabilities (DOE-OIG-17-08)	5	
Sep 22, 2017	Allegation of Nepotism and Misuse of Position within the Office of Management (DOE-OIG-17-09)	4	
Total Open Recommendations		**139**	**$378,063,386**

Reviews Closed and Not Disclosed to the Public

The Office of Inspector General had no undisclosed reports from the public for this reporting period April 1, 2017, through September 30, 2017.

Peer Reviews

PEER REVIEWS CONDUCTED BY ENERGY OIG APRIL 1, 2017 – SEPTEMBER 30, 2017			
TYPE OF REVIEW	**DATE OF PEER REVIEW**	**OIG REVIEWED**	**OUTSTANDING RECOMMENDATIONS**
Audits	None this reporting period		
Inspections	None this reporting period		
Investigations	None this reporting period		

PEER REVIEWS CONDUCTED OF ENERGY OIG APRIL 1, 2017 – SEPTEMBER 30, 2017			
TYPE OF REVIEW	**DATE OF PEER REVIEW**	**REVIEWING OIG**	**OUTSTANDING RECOMMENDATIONS**
Audits	None this reporting period		
Inspections	None this reporting period		
Investigations	July 13, 2017	U.S. Department of Transportation	None

INVESTIGATIVE OUTCOMES

Settlement Reached in Savannah River Site Qui Tam Investigation
The U.S. Department of Justice entered into a $4.6 million civil settlement agreement with a subcontractor on the Mixed Oxide Fuel Fabrication project at the Savannah River Site to resolve allegations made under the Civil False Claims Act. The qui tam investigation determined the subcontractor certified and billed the Government for reinforcing steel bars that met the Nuclear Quality Assurance-1 standard when the steel bars did not meet the standard. This investigation was coordinated with the U.S. Attorney's Office, Northern District of Georgia, and the U.S. Department of Justice's Civil Fraud Section, Washington, D.C.

Sentencing in Transportation of Child Pornography Investigation
A former technician at the Lawrence Livermore National Laboratory, was sentenced to 135 months incarceration in the U.S. District Court, Eastern District of California on Transportation of Child Pornography charges. The investigation was successful in removing a serious threat from the community. The filing of the Information and plea agreement were reported in the March 31, 2017, Semiannual Report to Congress. This was a joint investigation with the Federal Bureau of Investigation.

Sentencings in Bribery Investigation
A former senior Department employee pleaded guilty to Conspiracy and Bribery violations and was sentenced in the U.S. District Court, District of Maryland to 18 months incarceration, 3 years of probation and ordered to pay $469,287 in restitution, a $200 special assessment fee and a $75,000 fine. A prospective Department contractor employee was sentenced in U.S. District Court for the District of Maryland to 1 year and 1 day incarceration, 1 year of probation, ordered to pay $15,000 in fines with a $100 special assessment fee, and directed to forfeit $7,000 that was paid in bribe money. A former Department contractor employee was sentenced in U.S. District Court for the District of Maryland to 18 months incarceration to be followed by 1 year of supervised release and ordered to pay $70,000 in restitution with a $25,000 fine and a $200 special assessment fee. Additionally, a co-conspirator was sentenced in U.S. District Court for the District of Columbia to 2 years of probation. As reported in the March 31, 2017, Semiannual Report to Congress, a two-count Information was filed against the former senior Department employee, the prospective Department contractor employee pleaded guilty to one count of Bribery, and the co-conspirator pleaded guilty to one count of False Statements. The investigation determined the former senior Department employee solicited and was paid bribes to secure Department contracts for various companies and individuals, the prospective Department contractor employee paid bribes to secure a contract with the Department, the former Department contractor paid bribes to secure and maintain its contract with the Department, and the co-conspirator made false statements to federal agents related to bribery payments made to the senior Department employee. This is an ongoing, joint investigation with the Federal Bureau of Investigation.

Civil Settlement in Qui Tam Investigation
The U.S. Department of Justice entered into a $2.35 million settlement agreement with two Department subcontractors to resolve allegations of false claims made by relators in a qui tam lawsuit. The investigation determined the prime contractor knowingly misrepresented to the Department that the other subcontractor was a legitimate small disadvantaged business and used the other subcontractor as a pass-through front company to fraudulently obtain two multi-million dollar subcontracts that were reserved for legitimate small disadvantaged businesses. This is an on-going joint investigation with the Small Business Administration OIG and is being coordinated with the U.S. Attorney's Office for the Eastern District of Washington.

Sentencing in Conspiracy to Defraud the United States and Violation of Sex Offender Registration and Notification ACT (SORNA) Investigation
A former Department subcontractor employee was sentenced at the U.S. District Court, Eastern District of Tennessee to 41 months incarceration followed by three years' probation and $1,441,818 restitution to the Internal Revenue Service on Conspiracy violations. The former Department subcontractor employee was also sentenced to 15 months incarceration followed by three years' probation, to be served concurrently, for violating the SORNA. The investigation determined the former Department subcontractor employee, a registered sex offender, conspired with the subcontractor to file or cause others to file fraudulent tax returns. Additionally, the tax preparer attempted to evade prosecution by fleeing the state of his registered address without updating his registration as required by the SORNA. This is an on-going joint investigation with the Internal Revenue Service Criminal Investigation Division and the Federal Bureau of Investigations.

Sentencing in Grant Fraud Investigation
The former Chief Executive Officer (CEO) of a non-profit organization receiving Department funds was sentenced in the U.S. District Court, District of Minnesota to 48 months incarceration, 2 years supervised release and ordered to pay $387,063 in restitution with a special assessment fee of $1,600. As reported in the March 31, 2017, Semiannual Report to Congress, the CEO pleaded guilty to charges of Conspiracy to Commit Theft Concerning Programs Receiving Federal Funds, Mail Fraud, Wire Fraud, and Theft Concerning Programs Receiving Federal Funds. The investigation determined the former CEO diverted at least $250,000 in grant funds to pay personal expenses, including the purchase of automobiles, airline tickets, hotel expenses, rental cars, a Caribbean cruise, and paying his son $140,000 for work not performed. An Investigative Report to Management was issued recommending suspension and/or debarment of the former CEO and his son, who was employed by the same organization. This is a joint investigation with the Federal Bureau of Investigation, Internal Revenue Service Criminal Investigation Division, and Department of Health and Human Services OIG.

Guilty Plea by Former National Nuclear Security Administration Contractor
A former National Nuclear Security Administration (NNSA) contractor pleaded guilty in the U.S. District Court, District of South Carolina to Conspiracy. As previously reported in the March 31, 2016, Semiannual Report to Congress, two NNSA contractors were indicted on thirteen counts of Wire Fraud, one count of Conspiracy, and one count of Theft of Government Funds. As reported in the March 31, 2017, Semiannual Report to Congress,

the other contractor pleaded guilty to Conspiracy. The investigation determined that from 2009 to 2015 the indicted subjects stole over $6.5 million of Department funds by submitting fictitious invoices to NNSA's contractors for materials supposedly used to build the Mixed-Oxide (MOX) Fuel Fabrication Facility located at the Savannah River Site. A portion of the stolen Department funds were used to purchase gratuities for other contractors at the MOX Project. In addition to these defendants, four other former contractors were charged with violations of Gratuities and False Statements. This is an ongoing joint investigation with the Federal Bureau of Investigation.

Guilty Plea, Pretrial Diversion and Sentencing in Recovery Act Grant Fraud Investigation

The president and Chief Executive Officer (CEO) for a green technology startup company were each indicted on five counts of Wire Fraud in the U.S. District Court, Northern District of Illinois. The president of the green technology startup company pleaded guilty to one count of Wire Fraud and was sentenced to 24 months incarceration, 1 year supervised release, and 60 hours of community service. This sentencing was continued to assess an appropriate restitution amount. The CEO entered into a Pretrial Diversion Agreement and was ordered to pay a $10,000 fine, serve 200 hours of community service, and was further ordered to not apply for, or hold, any management, executive or leadership role in any entity which is the recipient or administrator of grant funding from any governmental entity. The investigation determined the president and CEO of the green technology startup company fraudulently obtained approximately $1.4 million in Recovery Act grant funds by falsifying vendor and subcontractor payment documents submitted to the City of Chicago, Pennsylvania Department of Environmental Protection, and Bay Area Air Quality Management for installing electric vehicle charging stations in Chicago, Pennsylvania and California. This is a joint investigation with the Federal Bureau of Investigation and the City of Chicago Office of Inspector General.

Settlement Reached with Department Subcontractor

The U.S. Department of Justice entered into a $100,000 settlement agreement with a Department subcontractor to resolve allegations made under the Civil False Claims Act. The investigation determined the subcontractor fraudulently received reimbursement of performance bond premium expenses that were not incurred in relation to a repaving contract at the Los Alamos National Laboratory. This investigation was coordinated with the U.S. Attorney's Office for the District of New Mexico, Civil Division.

Sentencing in Theft of Government Property Investigation – Kansas City National Security Campus

A former contractor employee of the Kansas City National Security Campus (KCNSC) was sentenced in the U.S. District Court, Western District of Missouri to 12 months and 1 day incarceration, 3 years of supervised release, and ordered to pay $50,480 in restitution and a $400 special assessment fee. As previously reported in the March 31, 2017, Semiannual Report to Congress, the former contractor employee pleaded guilty to four counts of Wire Fraud. The investigation determined that from June 2010 to August 2014 the former contractor employee purchased unauthorized and unnecessary items through KCNSC's procurement system which were subsequently sold for personal gain on eBay.

Sentencing in Theft of Government Property Investigation – Western Area Power Administration

A former Western Area Power Administration (WAPA) employee was sentenced in the U.S. District Court, District of Arizona to 5 years of probation and ordered to pay $168,418 in restitution with a $100 special assessment fee. As reported in the March 31, 2017, Semiannual Report to Congress, the former WAPA employee pleaded guilty to a one-count Information charging Theft of Government Property. The investigation determined the former WAPA employee knowingly used a Government purchase card to make multiple unauthorized purchases for his personal benefit. In response to an Investigative Report to Management, the WAPA employee was suspended from Government contracting and notified of proposed debarment. This was a joint investigation with the General Services Administration OIG.

Civil Settlement in False Claims Act and Anti-Kickback Act Investigation

A former Department subcontractor employee and spouse entered into a $9,000 civil settlement agreement with the U.S. Attorney's Office, Northern District of West Virginia to resolve allegations made under the False Claims Act. Two subcontractor companies and two corporate officers also entered into a $72,272 civil settlement agreement to resolve allegations under the False Claims and Anti-Kickback Acts. The investigation determined the former Department subcontractor employee, in their capacity as administrative assistant to the subcontractor's principal investigator, knew of misconduct by the spouse but failed to report it; assisted with efforts to secure employment for family members and associates; conspired to secure employment for the spouse; and submitted invoices to the Department for reimbursement of fraudulent labor and services. The investigation further determined the subcontractor companies and officers provided kickbacks to the principal investigator of two National Energy Technology Laboratory (NETL) cooperative agreements in the form of payments and employment for family members in exchange for subcontract awards and reimbursement for unsubstantiated project billings. As reported in the March 31, 2017, Semiannual Report to Congress, a civil complaint was filed in U.S. District Court, Northern District of West Virginia, charging 15 individuals and 12 companies with violations of the Anti-Kickback and False Claims Acts. The investigation determined that approximately $3 million of two National Energy Technology Laboratory prime contracts valued at $85 million were paid to contractors engaged in a kickback scheme and that the principal investigator assigned to the two contracts received at least $230,000 in kickbacks.

Sentencing in Theft of Government Property Investigation

A former Western Area Power Administration (WAPA) employee was sentenced in the U.S. District Court, District of Colorado to 3 years supervised release, 100 hours of community service and ordered to pay $27,237 in restitution with a $100 special assessment fee. As reported in the March 31, 2017, Semiannual Report to Congress, the former WAPA employee pleaded guilty to one count of Theft of Government Property. The investigation determined the former WAPA employee fraudulently used a Government purchase card to obtain over $27,000 worth of property for personal benefit. An Investigative Report to Management was issued recommending suspension and/or debarment of the former WAPA employee from Government contracting. This was a joint investigation with General Services Administration OIG.

Guilty Plea and Sentencing in Child Solicitation Investigation
A contractor employee pleaded guilty in the Benton County Superior Court to Gross Misdemeanor Communication with a Minor for Immoral Purposes and was sentenced to 364 days incarceration with 364 days suspended, 2 years of probation and was required to register as a sex offender. An Investigative Report to Management was issued recommending consideration for suspension and/or debarment actions. This is a joint investigation with Homeland Security Investigations Task Force and Kennewick Police Department.

Sentencing in Travel and Time and Attendance Fraud Investigation
A former Department employee was sentenced in the U.S. District Court, Eastern District of Tennessee to 7 months incarceration, 6 months home confinement, 3 years supervised release, ordered to pay $40,112 in restitution, and a special assessment of $2,300 on charges of Wire Fraud, False Claims, and False Statements. As reported in the March 31, 2016 Semiannual Report to Congress, the investigation determined that the former Department employee submitted numerous fraudulent travel vouchers totaling approximately $22,000 and fraudulent time and attendance documents totaling approximately $67,000, for work not performed. An Investigative Report to Management has been issued recommending debarment of the former employee from Government business.

Guilty Plea in Government Purchase Card Fraud Investigation
A former Western Area Power Administration (WAPA) employee pleaded guilty in the U.S. District Court, District of South Dakota to one count of Theft of Government Property. As reported in the March 31, 2017, Semiannual Report to Congress, the former WAPA employee was indicted in the U.S. District Court, District of South Dakota on one count of Theft of Government Property and one count of Bank Fraud. The former WAPA employee was subsequently arrested. The investigation determined the former WAPA employee fraudulently used a Government purchase card to obtain property worth over $20,450 which was subsequently sold for personal benefit. The former WAPA employee resigned in lieu of termination prior to the opening of this investigation. This is a joint investigation with General Services Administration OIG.

Guilty Pleas in Conspiracy to Defraud the Government Investigation
A subcontractor business co-owner and a subcontractor production manager pleaded guilty to one count of Knowingly Storing Hazardous Waste Without a Permit and one count of Accessory After the Fact, respectively, in the U.S. District Court, Eastern District of Tennessee. As reported in the March 31, 2017, Semiannual Report to Congress, both the production manager and the business co-owner were named in a Superseding Indictment charging the production manager with a single count of Conspiracy to Defraud the Government, in concert with the business co-owner, who was previously charged with the same violation plus three counts of Wire Fraud and two counts of Money Laundering. The production manager and the business co-owner were suspended from doing business with the Government. This investigation involves alleged criminal acts surrounding post-cleaning waste storage and disposal operations of a metal cleaning and plating business. This is an ongoing joint investigation with the U.S. Environmental Protection Agency

Criminal Investigation Division, Tennessee Valley Authority OIG, Defense Criminal Investigative Service, and Federal Bureau of Investigation

Guilty Plea and Sentencing in Theft Investigation
A former Department employee pleaded guilty in the Bonneville County District Court in Idaho to Felony Theft. The former Department employee was sentenced to 20 days incarceration, 4 years of probation, ordered to pay $1,600 in restitution and fined $1,200. The investigation determined the former Department employee stole numerous Government-purchased gift cards designated for employee recognition awards and used the gift cards to pay for personal expenses. The former employee also admitted to forging documents to fraudulently obtain additional Government-purchased gift cards.

No Contest Plea and Sentencing in Theft of Government Property Investigation - Third Degree Larceny
A former Los Alamos National Laboratory (LANL) contractor employee pleaded no contest in the Los Alamos Magistrate Court to Third Degree Larceny charges and was sentenced to 3 years of probation and ordered to pay $3,474 in restitution. The investigation determined the former contractor employee stole copper fittings and tubing from LANL and sold the items at a local metal recycling facility. This was a joint investigation with the Los Alamos Police Department.

No Contest Plea and Sentencing in Theft of Government Property Investigation – Larceny and Tampering with Evidence
A former Los Alamos National Laboratory (LANL) contractor employee pleaded no contest in the First Judicial District Court, County of Los Alamos to Larceny and Tampering with Evidence charges and was sentenced to 2 years of probation. The investigation determined the former subcontractor employee stole several tools from a LANL Technical Area used to process radiological waste. This was a joint investigation with the Los Alamos Police Department and Federal Bureau of Investigation.

Indictment and Arrest in Grant Fraud Investigation
A Department grantee was arrested and charged with Conspiracy to Defraud the Government. Simultaneous to the arrest, search warrants were served at the grantee's residence, as well as the grantee's offices and university laboratory. The investigation determined the grantee conspired with other employees of his company to submit false claims and false statements to the Government in relation to Small Business Innovation Research and Small Business Technology Transfer grants; as well as steal trade secrets from former company employees and transfer the technology overseas. This is a joint investigation with the National Science Foundation OIG and the Federal Bureau of Investigation.

Indictment Returned in Bid Rigging Investigation
A Federal Grand Jury in the U.S. District Court, Northern District of California returned an eight-count indictment against eight individuals for engaging in a contract bid-rigging scheme at the Lawrence Berkeley National Laboratory (LBNL). The indictment included charges of Receiving a Bribe, False Statements, Conspiracy to Receive a Bribe, and Conspiracy to Defraud the United States. The investigation determined the individuals

conspired to submit four multi-million dollar bids for a renovation contract at LBNL. An Investigative Report to Management was issued recommending consideration of suspension and/or debarment of the eight individuals and their respective companies from Government contracting. This is a joint investigation with the Federal Bureau of Investigation.

Indictment and Arrest in Theft Investigation
A former contractor employee was indicted for Theft in the 7th District for the State of Tennessee, Anderson County Criminal Court, and subsequently arrested. The investigation determined the contractor employee removed 298 sheets of tin metal and associated parts valued at approximately $18,380 from the Y-12 site without permission.

Information in Theft of Government Property Investigation
The U.S. Attorney's Office for the Northern District of California, filed an Information charging two former Lawrence Berkeley National Laboratory (LBNL) contractor employees with one count of Theft of Government Property. The investigation determined the two former LBNL contractor employees stole scrap copper wire from LBNL valued at approximately $39,000 and sold the copper wire for personal gain. The OIG took possession of $21,381 in cash after one of the two former LBNL employees admitted during an interview that the money was criminal proceeds derived from multiple thefts of copper wire from LBNL.

Response to Investigative Report to Management in False Claims Act Investigation
In response to an Investigative Report to Management, the Department conducted an evaluation of a Waste Treatment Plant (WTP) project to identify deficient materials and/or work products, and conducted a review of the WTP contract to determine if any remedial action or adjustment was warranted. The Department advised that many of the issues raised during the investigation had open corrective action plans. Additionally, the Department is monitoring resolution of the technical issues associated with the High-Level Waste and Pretreatment Facilities and coordinating with the Defense Nuclear Facilities Safety Board to ensure all identified concerns with nuclear safety and implementation of NQA-1 are addressed. Furthermore, ongoing oversight of programs and field implementation continues to identify and address issues associated with nuclear safety, welding, fire safety, and inadequate implementation of quality assurance requirements. As previously reported in the March 31, 2017, Semiannual Report to Congress, the U.S. Department of Justice entered into a $125 million civil settlement agreement with a Department contractor to resolve allegations made under the False Claims Act. The qui tam investigation determined that from approximately January 2001 to June 2013, the contractor made false statements and claims to the Department for deficient nuclear quality materials, services, and testing at the WTP at the Department's Hanford Site. In addition, the settlement also resolved allegations that the contractor improperly used Federal contract funds to pay for lobbying activities involving Congress and other Federal officials for continued funding at the plant. This investigation was coordinated with the U.S. Attorney's Office, Eastern District of Washington and the U.S. Department of Justice's Civil Fraud Section, Washington, D.C.

Debarment Action in Per Diem Fraud Investigation
In response to an Investigative Report to Management, a former Department contractor employee was debarred from Government contracting for a period of 5 years. As reported in the March 31, 2017, Semiannual Report to Congress, the former Department contractor employee was sentenced in the U.S. District Court, Eastern District of Tennessee to 3 years of probation, ordered to pay $116,493 in restitution, and perform 150 hours of community service. The former contractor employee pleaded guilty to one count of False Claims. The Department was designated to receive $7,383 of the restitution as reimbursement for fraudulently claimed relocation expenses. The former contractor employee was discharged and their security clearance determination discontinued. The investigation determined the former contractor employee provided false information to the Tennessee Valley Authority (TVA) and the Department in order to receive relocation pay to which the former contractor employee was not entitled. This was a joint investigation with TVA OIG.

Debarment Action in Theft of Government Property Investigation
In response to an Investigative Report to Management, a former Department contractor employee was debarred from Government contracting for a period of 3 years. As previously reported in the March 31, 2017, Semiannual Report to Congress, the investigation determined that from October 2010 until January 2015, the former contractor employee stole approximately $510,000 of machine components made of Tungsten steel and copper from Argonne National Laboratory. As a result of this theft, the former contractor employee caused damage to the machine components comprised of the Tungsten steel, rendering the machines inoperable. As reported in the September 30, 2016, Semiannual Report to Congress, the former contractor employee pleaded guilty to a single-count Information for embezzling $64,263 in union funds. As part of the guilty plea, the former contractor employee stipulated to having committed theft of Government property valued at approximately $510,973. The former contractor employee was sentenced to 30 months incarceration, 2 years supervised release and ordered to pay $510,974 in restitution to the Department.

Debarment Action in Property Theft Investigation
In response to an Investigative Report to Management, a former Department contractor employee was debarred from doing business with the Government for a period of 5 years. The investigation determined the former contractor employee stole at least 42,782 pounds of copper from the Lawrence Livermore National Laboratory and sold it for $117,379. This investigation is being coordinated with the U.S. Attorney's Office for the Northern District of California.

Debarment Action in Receiving Stolen Property Investigation
In response to an Investigative Report to Management, a former Sandia contractor employee and the contractor employee's company were debarred from doing business with the Government for a period of 5 years. The investigation determined the former contractor employee received stolen metal fabrication equipment from the Sandia Fabrication Plant prior to it ceasing operation. The former contractor employee used the stolen equipment, valued at $43,000, in the former contractor employee's business.

Debarment Action in Fraudulent Use of Government Purchase Card Investigation
In response to an Investigative Report to Management, a former Los Alamos National Laboratory contractor employee was debarred from doing business with the Government for a period of 3 years. The investigation determined the former contractor employee made multiple purchases of gasoline for personally owned vehicles using multiple Government Fleet Services cards. This was a joint investigation with the General Services Administration OIG.

Debarment Action in Timecard Fraud Investigation
In response to an Investigative Report to Management, a former National Renewable Energy Laboratory (NREL) contractor employee was debarred from Government contracting for a period of 3 years. As reported in the March 31, 2017, Semiannual Report to Congress, the former contractor employee pleaded guilty to a one-count Information charging Criminal Attempt of Theft in the First Judicial District of Colorado. The former contractor employee received a deferred sentence pending successful completion of two years supervision in an Adult Diversion Program and was ordered to pay $4,208 in restitution to the management and operating contractor of NREL. The investigation determined the former contractor employee submitted numerous falsified time and attendance documents to NREL claiming $50,570 for work not performed. NREL reimbursed the Department the amount paid for work not performed. This was a joint investigation with the First Judicial District of Colorado.

Debarment Action in Small Business Innovation Research Fraud Investigation
In response to an Investigative Report to Management, a former grantee and the grantee's company were debarred for a period of 5 years. The investigation determined the former grantee used false and fraudulent letters of support, along with false claims regarding corporate facilities, equipment, and materials to be used to conduct research in its applications for Small Business Innovation Research grant funds. This is a joint investigation with the NSF OIG and the National Aeronautics and Space Administration OIG.

Notice of Suspension and Proposed Debarment in False Claims Investigation for Former Grantee
In response to an Investigative Report to Management, a former Department grantee and five affiliate companies were suspended and notified of a proposed 3 year debarment from Government contracting. As reported in the March 31, 2017, Semiannual Report to Congress, the former grantee pleaded guilty in the U.S. District Court, Western District of Pennsylvania, to a one-count Information charging submission of False Claims to the Department. The investigation determined the former grantee submitted false claims for work not performed and converted over $5.7 million in grant funds to personal use.

Notice of Suspension and Proposed Debarment in False Claims Investigation for Former Contractor
In response to an Investigative Report to Management, a former National Renewable Energy Laboratory (NREL) contractor employee was suspended and notified of a proposed 3 year debarment from Government contracting. As reported in the March 31, 2017, Semiannual Report to Congress, the contractor employee entered into an $80,000 civil settlement agreement with the U.S. Department of Justice to resolve allegations of false

claims arising from the contractor employee's use of NREL-paid work time, NREL-owned equipment, and NREL-owned resources for personal financial gain while consulting for three private companies. The contractor employee resigned in lieu of termination.

Notices of Suspension in False Claims Investigation
A Small Business Innovation Research grantee company, two co-owners and an employee were suspended from doing business with the Government pending completion of legal proceedings. The investigation determined the company and its employees submitted false claims and certifications to the Department and numerous other Government agencies in its applications for awards. This is an ongoing, joint investigation with the National Science Foundation OIG, the National Aeronautics and Space Administration OIG, the Defense Criminal Investigative Service, the Air Force Office of Special Investigations and the Naval Criminal Investigative Service.

Response to Investigative Report to Management Issued in Waste Management Investigation
In response to an Investigative Report to Management, the Office of Environmental Management notified a Special Waste Disposal Facility that the facility had received radiologically contaminated material. The investigation determined radiologically contaminated material was improperly disposed of at the facility during a Department funded decontamination and decommission project.

Response to Investigative Report to Management Issued in Employee Misconduct Investigation
In response to an Investigative Report to Management, the Western Area Power Administration (WAPA) agreed to implement initial and recurring WAPA-wide procurement law and policy training for all employees acting on behalf of or advising on procurement actions for the Federal Government. Additionally, WAPA advised that the subject of the OIG investigation received a 7-day suspension without pay for violating WAPA's vehicle use policy. The investigation determined the WAPA employee, acting as a technical representative in a WAPA solicitation, violated the Procurement Integrity Act by releasing competitor bid information and market research prior to a contract being awarded. WAPA cancelled the solicitation, which resulted in no loss to the Department. Additionally, the investigation determined the WAPA employee was arrested for soliciting a prostitute while driving a Government owned vehicle.

Investigative Report to Management Issued to Bonneville Power Administration
An Investigative Report to Management was issued to the Bonneville Power Administration (BPA) recommending BPA determine whether administrative action is warranted for a BPA employee who stole Government property. The investigation determined that a BPA employee stole BPA-owned fuel, tires, and other miscellaneous property. A portion of the stolen Government property, valued at $3,711, has been recovered.

Employee Termination in Theft of Government Property Investigation
A Lawrence Livermore National Laboratory contractor employee was terminated for theft of Government property. The investigation determined the former contractor employee stole numerous Government-purchased, freon-cylinder containers, valued at

approximately $20,000, and used them for a personal business. The employee also admitted to selling some of the containers online.

Demand Letter Issued in Misrepresentation Investigation

The Savannah River Nuclear Solutions, LLC (SRNS) issued a demand letter to a Department subcontractor company requiring the subcontractor reimburse the SRNS $98,576. The investigation determined the subcontractor was awarded a $9.087 million subcontract based on false small business status representations. The subcontractor claimed to meet the North American Industry Classification System size standard required for the subcontract, when in fact the subcontractor's revenues exceeded the standard. As a result, the SRNS incurred costs associated with selecting the subcontractor company and later, for transitioning the subcontract to a qualified small business.

AUDIT REPORTS

Followup on the Small Business Innovation Research and Small Business Technology Transfer Programs

The Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs are congressionally-mandated programs that require Federal agencies with large research and development budgets to set aside a certain percentage of their funding for small businesses to develop innovative technologies. The Office of Science (Science) manages these programs for all Department offices except the Advanced Research Projects Agency-Energy (ARPA-E), which independently manages its own programs. While Science administers its awards through grants, ARPA-E uses cooperative agreements as its primary funding mechanism. With cooperative agreements, substantial Government involvement in the project is expected. In FY 2015, annual funding for the Department's SBIR and STTR programs was approximately $198 million for Science and $12.3 million for ARPA-E.

In our previous audit of these programs, The Department's Small Business Innovation Research and Small Business Technology Transfer Programs, DOE/IG-0876, we identified significant delays in the closeout of grants, substantiated allegations relating to conflicts of interest during the award selection process, and found erroneous and unsupported costs charged by a grant recipient. Due to the issues identified in our prior audit and ARPA-E's relatively limited experience with these programs, we initiated this audit to determine whether the Department is efficiently and effectively managing its SBIR and STTR programs.

Through our review of eight Science grants and one ARPA-E cooperative agreement (awards), we found:

- Three recipients had not properly accounted for, or maintained adequate supporting documentation for, a portion of their project expenses.
- The Department had not ensured that three recipients met all terms and conditions of their awards.
- Science had not always ensured recipients submitted all final expenditure reports within the required timeframe and had not always adequately documented its rationale for decisions to waive closeout requirements for recipients to submit final project deliverables.

The issues that we identified were primarily due to recipients having a lack of awareness of regulations and specific award terms and conditions and, at times, Department officials providing limited oversight.

To address the issues noted in this report related to Science's management of SBIR and STTR awards, we made recommendations to the Acting Director for the Office of Science and the Acting Director for the Advanced Research Project Agency- Energy. (OAI-M-17-06)

Followup on the K Basin Sludge Removal Project

The K West Reactor Fuel Storage Basin is one of the last facilities along the Columbia River at the Department's Hanford Site that contains nuclear material. The K Basin contains highly radioactive sludge resulting from long-term storage and degradation of spent nuclear fuel. CH2MHill Plateau Remediation Company, LLC (CHPRC), managed by the Department's Richland Operations Office, has a mission to begin removal of 27 cubic meters of radioactive sludge by September 30, 2018.

In February 2011, we reported that the project's previous contractor and one of its subcontractors failed to apply key project management principles and did not ensure that the contractor followed best business practices. Therefore, we initiated this followup audit to determine whether the Department was effectively managing the K Basin Sludge Removal Project at the Hanford Site.

Although the K Basin project has experienced cost and schedule performance issues throughout its history, according to CHPRC and the Department's records, as of October 20, 2016, the Sludge Removal Project appears to be on schedule to meet current milestones. However, we identified a concern where management reserve was used to reset the project's performance measurement baseline, which included completed workscope. This occurred because CHPRC did not follow specific guidance required by the contract on the accepted use of management reserve. We followed up on issues identified in a prior audit report and found that the Department made changes to the Sludge Treatment Project which addressed the project management concerns.

We are aware that the circumstances associated with this project were unique, and are not likely to recur. However, we are concerned that CHPRC's performance on this project will be overstated. Accordingly, to ensure the accuracy of the Sludge Removal Project's historical cost variances, we suggest the Acting Assistant Secretary, Office of Environmental Management and CHPRC coordinate with the Director, Office of Project Management Oversight and Assessments to take necessary steps to ensure the Sludge Removal Project's historical cost variances remain visible for project performance reporting purposes. (OAI-L-017-04)

The Department of Energy's Improper Payment Reporting in the Fiscal Year 2016 Agency Financial Report

This report presents the results of an audit of the Department's Improper Payment Reporting in the FY 2016 Agency Financial Report. To fulfill the our audit responsibilities, we contracted with the independent public accounting firm of KPMG LLP (KPMG) to express an opinion on whether the Department met the Office of Management and Budget's criteria for compliance with the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA). KPMG expressed the opinion that the Department complied with all requirements of IPERIA. (OAI-FS-17-09)

Department of Energy's West Valley Demonstration Project

From 1966 to 1972, Nuclear Fuel Services Inc. operated a commercial nuclear fuel reprocessing plant at the Western New York Nuclear Services Center near West Valley, New York. The plant was the first and only U.S. plant in history to commercially reprocess

uranium and plutonium from spent nuclear fuel. Operations at the plant generated more than 600,000 gallons of liquid high-level waste, which was stored on-site in underground tanks. In 1980, Congress passed the West Valley Demonstration Project Act, which required the Department, in cooperation with the State of New York, to solidify high-level waste, develop containers suitable for permanent disposal of the high-level waste, transport the waste to a permanent Federal repository, dispose of low-level and transuranic waste, and decontaminate and decommission the associated facilities and tanks.

The Department reported that it had developed suitable containers and solidified the high-level waste via vitrification by 2002, fulfilling its first two responsibilities under the West Valley Demonstration Project Act. The Department then commenced interim activities for decontaminating and decommissioning the facilities and managing wastes until it issued its Record of Decision in 2010. We initiated this audit to determine whether the Department was effectively managing the West Valley Demonstration Project (West Valley) cleanup efforts.

We identified several significant issues with the management of the West Valley cleanup effort. In particular, we found substantial weaknesses related to the Department's project and contract management that contributed to the inability to meet the major milestones established in the Phase I – Facility Disposition contract. Specifically, we found the following:

- Although the West Valley Phase I activities had been underway since 2011 and had incurred costs of $264 million by October 2015, the project was not administered using basic project management principles.

- The Department had omitted or had not explicitly described critical activities from the Phase I contract's original scope. As of November 2015, the contract value had increased by $196 million as a result of differing site conditions and inaccurate scope.

These conditions occurred, in part, because the Department had not ensured that project management policies and procedures were followed. Despite the requirements established in the Office of Management and Budget's Capital Programming Guide, Department Order 413.3B, Program and Project Management for the Acquisition of Capital Assets, and Environmental Management's Portfolio Management Framework, the site did not manage the West Valley decontamination and decommissioning work as a capital project.

To minimize future cost overruns and schedule delays, we made a series of recommendations designed to assist management and improve oversight of the West Valley project. Management concurred with our recommendations and identified a series of actions that were either underway or were planned to address our recommendations. Management's actions are responsive to our recommendations. (DOE-OIG-17-05)

Audit Coverage of Cost Allowability for Princeton University During Fiscal Years 2013 Through 2015 Under Department of Energy Contract No. DE-AC02-09CH11466
Since 1951, Princeton University has operated the Princeton Plasma Physics Laboratory (PPPL) under a contract with the Department. PPPL is part of the Department's Office of

Science dedicated to developing the scientific and technical knowledge base for fusion energy as a safe, economical, and environmentally attractive energy source for the world's long-term energy requirements. During FY 2013 through 2015, Princeton University incurred and claimed $253,847,637.75 for PPPL.

As an integrated management and operating contractor, Princeton University's financial accounts for PPPL are integrated with those of the Department, and the results of transactions are reported monthly according to a uniform set of accounts. Princeton University is required by its contract to account for all funds advanced by the Department annually on its Statement of Costs Incurred and Claimed, to safeguard assets in its care, and to claim only allowable costs. Allowable costs are incurred costs that are reasonable, allocable, and in accordance with the terms of the contract as well as applicable cost principles, laws, and regulations.

Our office along with the Department's Office of Acquisition Management, and the integrated management and operating contractors and other select contractors have implemented a Cooperative Audit Strategy to make efficient use of available audit resources while ensuring that the Department's contractors claim only allowable costs. This strategy places reliance on the contractors' internal audit function (Internal Audit) to provide audit coverage of the allowability of incurred costs that are claimed by the contractors. To help ensure that audit coverage of cost allowability was adequate for FYs 2013 through 2015, the objectives of our assessment were to determine whether:

- Internal Audit conducted cost allowability audits that complied with professional standards and could be relied upon;

- Princeton University conducted or arranged for audits of its subcontracts when costs incurred were a factor in determining the amount payable to the subcontractor; and

- Princeton University adequately resolved questioned costs and internal control weaknesses affecting allowable costs that were identified in audits and reviews.

Based on our assessment, nothing came to our attention to indicate that the allowable cost-related audit work performed by Internal Audit for FYs 2013 through 2015 could not be relied upon. We did not identify any material internal control weaknesses with the cost allowability audits, which generally met the Institute of Internal Auditors International Standards for the Professional Practice of Internal Auditing (IIA Standards). Further, Princeton University had conducted reviews and arranged for audits of subcontractors to PPPL when costs incurred were a factor in determining the amounts payable to the subcontractors. Internal Audit identified $1,173.53 in questioned costs during audits of cost allowability and PPPL subcontract reviews identified another $18,787.53 in questioned costs, all of which have been resolved. (OAI-V-17-03)

Audit Coverage of Cost Allowability for Battelle Memorial Institute Under its Contract to Manage the Pacific Northwest National Laboratory During Fiscal Years 2013 and 2014 Under Department of Energy Contract No. DE-AC05-76RL01830

Since 1965, Battelle Memorial Institute (Battelle) has operated the Pacific Northwest National Laboratory under contract with the Department. This Laboratory, in the Department's Office of Science, performs research and innovations in the areas of environmental protection and clean up, energy resources, and national security. The Laboratory is managed under a performance-based management contract, through September 30, 2022. During FYs 2013 through 2014, Battelle expended and claimed costs totaling approximately $1.8 billion.

Battelle is required by its contract to account for all funds advanced by the Department annually on its Statement of Costs Incurred and Claimed, to safeguard assets in its care, and to claim only allowable costs. Allowable costs are incurred costs that are reasonable, allocable, and allowable in accordance with the terms of the contract, applicable cost principles, laws, and regulations. To help ensure only allowable costs are claimed by the Department's integrated contractors and to make efficient use of available audit resources, our office, the Department's Office of Acquisition Management, and the integrated management and operating contractors and other select contractors have implemented a Cooperative Audit Strategy.

To help ensure that audit coverage of cost allowability was adequate during FYs 2013 through 2014, the objectives of our assessment were to determine whether:

- Internal Audit conducted cost allowability audits that complied with professional standards and could be relied upon;

- Battelle conducted or arranged for audits of its subcontractors when costs incurred were a factor in determining the amount payable to a subcontractor; and

- Questioned costs and internal control weaknesses identified in audits and reviews and affecting allowable costs have been adequately resolved.

Based on our assessment, nothing came to our attention to indicate that the allowable cost related audit work performed by Battelle's Internal Audit for FYs 2013 through 2014 could not be relied upon. We did not identify any material internal control weaknesses with cost allowability audits, which generally met the Institute of Internal Auditors International Standards for the Professional Practice of Internal Auditing (IIA Standards). During its FYs 2013 and 2014 audits of cost allowability, Internal Audit identified $375,983 in questioned costs, all of which had been resolved. However, we identified the following issues that need to be addressed to ensure that only allowable costs are claimed by and reimbursed to the contractor. Specifically:

- Although we ultimately determined that we could rely on Battelle's Internal Audit work, we noted that work papers did not always include sufficient documentation.

- Battelle did not always conduct periodic post-award or interim audits of subcontracts. We noted that Battelle did not have a documented risk-based approach for conducting periodic post-award or interim audits of cost reimbursement subcontractors in effect during FY 2013 and most of FY 2014.

We made recommendations to the Manager, Pacific Northwest Site Office, and Management agreed with the findings, concurred with the recommendations, and proposed planned corrective actions that were responsive to our recommendations. (OAI-V-17-04)

Maintenance and Testing of Intrusion Detection and Alarm Systems

The Department is responsible for some of the Nation's most complex and technologically advanced programs, including cutting edge work in basic and applied sciences, environmental cleanup, and nuclear weapons stewardship. Department Order 473.3A Protection Program Operations establishes requirements for the physical security of property and personnel at Department sites, including requirements for intrusion detection and alarm systems. These systems are intended to ensure breaches of security barriers or boundaries are detected and responded to appropriately. Maintenance and testing of these systems is vital to ensure continuous operation.

Given the critical importance of physical security at Department sites, we initiated this audit to determine whether the Department effectively and efficiently managed the maintenance and testing of intrusion detection and alarm systems at selected sites.

Nothing came to our attention to indicate that the Department had not managed the maintenance and testing of intrusion detection and alarm systems effectively and efficiently at the three sites reviewed. Generally, we found that the sites were in compliance with relevant regulations over maintenance and testing of their intrusion detection and alarm systems. However, during the course of our review, we identified several opportunities for improvement at two of the three sites we visited. Specifically, at the Hanford Site (Hanford) we found opportunities for improvement related to:

- The collection and analyses of false and nuisance alarm rates (FAR/NAR) data;

- Documentation related to corrective actions taken on failures identified during testing of system elements; and

- The certification process of security system testers.

Additionally, we found that the Pantex Plant (Pantex) could improve its maintenance close-out procedures related to security work orders. Our audit identified no reportable issues at the third site, the Pacific Northwest National Laboratory.

We made a suggestion that the Manager of the National Nuclear Security Administration Production Office direct Consolidated Nuclear Security LLC, the contractor responsible for managing Pantex, to develop a formal process to ensure that all Computerized Maintenance Management System security-related work orders are closed when work is completed.

Pantex officials agreed a formal process is necessary to ensure that work orders are closed out within the system when work is completed or no longer needed. (OAI-L-17-06)

The Office of Enterprise Assessments Testing Incident at the 2016 Department of Energy Cyber Conference

The Department's Office of Enterprise Assessments is responsible for conducting independent assessments on behalf of the Secretary and Deputy Secretary in the areas of nuclear and industrial safety and cyber and physical security. Within the Office of Enterprise Assessments, the Office of Cyber Assessments evaluates the effectiveness of cybersecurity policy throughout the Department, as well as program and site office performance as it relates to implementation of cybersecurity programs. Assessments can be announced or unannounced and typically include a programmatic cybersecurity policy review in conjunction with technical performance testing. Announced testing is coordinated with the organization being tested and conducted as part of a scheduled appraisal activity. Unannounced tests, also known as red team exercises, are conducted without informing the site but are required to include coordination with a trusted agent. Due to the potential operational impacts, assessments must be carefully and thoroughly conducted and coordinated.

The Office of the Chief Information Officer (OCIO) recently sponsored the Department's 2016 Cyber Conference, held at a non-Federal facility located in Atlanta, Georgia. During the conference, the Office of Cyber Assessments conducted an unannounced assessment related to the use of mobile device charging stations. Officials indicated that the purpose was to determine whether conference participants would connect government and/or personal devices to a charging station. Due to concerns raised by various Department officials related to the Office of Cyber Assessments' lack of coordination with the OCIO prior to the assessment, we initiated a special inquiry to determine the facts and circumstances surrounding the assessment.

Our review of the cyber conference testing incident substantiated concerns that the assessment had not been appropriately coordinated with the OCIO. We also identified issues related to the resulting response by OCIO officials. Although they participated in planning the conference, we found that the Office of Cyber Assessments had not taken appropriate planning and coordination steps when conducting its security assessment during the Department's 2016 Cyber Conference. Specifically, we found that Office of Cyber Assessments officials placed two data collection devices disguised as charging stations outside the conference exhibit hall just prior to commencement of the conference, without coordination with any individual responsible for planning or hosting the conference. In addition, once discovered, OCIO officials may not have taken the appropriate steps in responding to the identification of the uncoordinated devices. While it was ultimately determined that the devices were not malicious, did not pose a risk to the conference attendees, and no data was collected during the conference, we are concerned about the lack of coordination among Department elements and the related OCIO response to the potential threat that such devices could have posed. While not specifically addressing the operations related to the Department's 2016 Cyber Conference, a review conducted in November 2016 by the Associate Deputy Secretary found that the Office of Enterprise Assessments acted within its authorities.

We found that a number of factors contributed, at least in part, to the testing incident that occurred at the Department's Cyber Conference. In particular, we noted that the Office of Cyber Assessments procedures were not always followed by personnel during this unannounced assessment. Similarly, the response by the OCIO did not adhere to Department incident response guidance, leaving conference attendees and other facility patrons vulnerable to potential unmitigated threats. Furthermore, we determined that the Office of Enterprise Assessments should have been more diligent in monitoring the execution of the assessment.

This incident illustrates shortcomings in the planning and operations of the Office of Enterprise Assessments and operations of the OCIO. The lack of adequate management and oversight of the unannounced assessment illustrated weaknesses in the performance of assessment operations that, if left uncorrected, could have the potential for negative repercussions on future operations.

To help improve the Department's processes related to planning and executing cybersecurity assessments, we made recommendations to the Director, Office of Enterprise Assessments and the Acting Chief Information Officer. Management concurred with each of the report's recommendations and indicated that corrective actions had been taken, or were being planned, to address the identified issues. (OIG-SR-17-05)

Review of Training Expenses at the Department of Energy's Office of Fossil Energy

The Department's Office of Fossil Energy (Fossil Energy) is responsible for Federal research, development, and demonstration efforts on advanced fossil energy technologies, as well as management of the Nation's Strategic Petroleum Reserve. Fossil Energy is committed to providing its Federal workforce with learning opportunities required to ensure success within their current positions, while supporting their Program office's mission critical goals and objectives. As part of a well-rounded continuing education program, Fossil Energy has created numerous training assistance programs to provide its employees with opportunities to enhance their skills and competencies through advanced degrees and college-level courses.

In May 2016, we received a Hotline Complaint alleging that Fossil Energy had paid for an employee's college degree that was unrelated to his current position. We initiated this review to examine the facts surrounding the allegation.

We substantiated the allegation that Fossil Energy officials approved training for one employee that was not applicable to his official workplace responsibilities, as required by Departmental regulations. This employee left the Department for work in the private sector shortly after receiving his law degree in May 2013.

We found that from 2009 through 2013, Fossil Energy paid for 29 college courses, totaling approximately $138,000, for a general engineer to obtain a law degree. This employee enrolled in three to four law-related courses a semester at the American University in Washington, DC. Based on our review, we concluded that a majority of the courses taken by the employee were unrelated to his position at the Department.

We found that although Fossil Energy had sufficient review/approval policies and procedures in place, in this instance, these controls were overridden by senior management officials in the approval chain at the time, including the Chief Operating Officer and Principal Deputy Assistant Secretary. Specifically, training approval officials told us that when they questioned the applicability of the law-degree courses for a general engineer, senior management officials verbally directed them to approve the training requests. Although the applicability of training courses had been questioned on a number of occasions (and by a number of reviewers), no documentation existed to explain why senior management officials directed training officials to approve the courses. Further, we were unable to interview these management officials because they had left the agency. We found that Fossil Energy had not considered obtaining a continued service agreement for the employee, even though he had taken extensive training at considerable cost to the Department. While the Department regulation only requires continued service agreements for training activities that exceed 180-training hours, it allows Department elements, such as Fossil Energy, to establish a lesser hour threshold for continued service agreements, if applied equitably to all participants. Refining its training policies to allow for an expansion in the consideration of continued service agreement requirements would help to ensure that Department funds are expended efficiently and effectively.

Without ensuring that funds are spent on training related to job responsibilities, the Department may not receive the maximum benefit of training funds spent and enhance the capabilities of the Federal workforce at Fossil Energy. Further, taxpayer funds may not be put to the most beneficial use in support of the Program's mission. Finally, by not considering the use of continued service agreements, Fossil Energy may not fully benefit from enhancing its workforce's capabilities over time.

To ensure that Fossil Energy obtains the maximum benefit from training its employees with taxpayer dollars, we made recommendations to the Acting Assistant Secretary, Office of Fossil Energy. Management generally concurred with the report's recommendations and identified a number of actions that were either completed or planned to address our recommendations. (OAI-M-17-08)

Audit Coverage of Cost Allowability for Consolidated Nuclear Security LLC during July 1, 2014, through September 30, 2015, under Department of Energy Contract No. DE-NA-0001942

Since July 1, 2014, Consolidated Nuclear Security LLC (CNS) has managed and operated the Y-12 National Security Complex and Pantex Plant under contract with the Department. Both the Y-12 National Security Complex and the Pantex Plant are part of the Department's National Nuclear Security Administration, which has responsibilities that include ensuring the safety, security, and effectiveness of the nation's nuclear weapons stockpile. During the period of July 1, 2014, through September 30, 2014, and FY 2015, CNS incurred and claimed costs of $396,655,647 and $1,640,090,371, respectively on its FY 2014 and FY 2015 statements of costs incurred and claimed.

CNS is required by its contract to account for all funds advanced by the Department annually on its Statement of Costs Incurred and Claimed, to safeguard assets in its care, and

to claim only allowable costs. The Department's Cooperative Audit Strategy makes efficient use of available audit resources while ensuring that the Department's contractors claim only allowable costs. This strategy places reliance on the contractors' internal audit function (Internal Audit) to provide audit coverage of the allowability of incurred costs claimed by contractors.

Based on our assessment, nothing came to our attention to indicate that the allowable cost-related audit work performed by CNS' Internal Audit for the period of July 1, 2014, through September 30, 2015, could not be relied upon. We did not identify any material internal control weaknesses with the cost allowability audits, which generally met the Institute of Internal Auditors International Standards for the Professional Practice of Internal Auditing. During the period under review, Internal Audit identified questioned costs totaling $36,706 in its cost allowability audits, all of which had been resolved. Additionally, we found that CNS conducted or arranged for audits of subcontractors when costs incurred were a factor in determining the amount payable to a subcontractor. Internal Audit conducted 27 audits of subcontractors, identifying $13,993,275 in questioned costs and two control weaknesses, all of which had been resolved. We noted that costs totaling $1,482,161 for FY 2013 and $517,604 for FY 2014 questioned in our previous report, Assessment of Audit Coverage of Cost Allowability for Babcock and Wilcox Technical Services Y-12 LLC During FYs 2013 and 2014 Through June 30, 2014, Under Department of Energy Contract No. DE-AC05-00OR22800 (OAS-V-15-05), had been resolved. Finally, we determined that Internal Audit did not test executive compensation costs for allowability. As such, we consider $4,012,957, the total compensation of CNS executives charged to the contract for the period under review, unresolved pending audit. This did not adversely affect our ability to rely on Internal Audit's work. (OAI-V-17-05)

Followup on Bonneville Power Administration's Cybersecurity Program

The Bonneville Power Administration (Bonneville) was established in 1937 as a Federal nonprofit power marketing administration and provides approximately 28 percent of the electric power used across 300,000 square miles in the Pacific Northwest. Although Bonneville is part of the Department of Energy, it is self-funded and covers its costs by selling products and services such as wholesale electrical power from 31 Federal hydroelectric projects in the Northwest and operating and maintaining about three-fourths of the high-voltage transmission in its service territory. With an overall budget of $4.3 billion, Bonneville utilizes numerous information systems to conduct business and electricity-related operations, including financial and administrative systems. In FY 2017, Bonneville budgeted more than $7 million for its cybersecurity program to protect systems that, if compromised, could have a significant impact on Bonneville and its customers.

Prior reviews have identified weaknesses related to Bonneville's cybersecurity program. For example, our report on the Management of Bonneville Power Administration's Information Technology Program (DOE/IG-0861, March 2012) identified cybersecurity weaknesses in areas such as access control, vulnerability management, configuration management, least privilege, and contingency and security planning. More recently, we received two allegations – one that alleged Bonneville officials had required nearly all teams to stop patching its systems and another that officials did not ensure systems stayed up-to-date on security controls. We initiated this followup audit to determine whether

Bonneville effectively implemented its cybersecurity program over financial and administrative systems and to evaluate the circumstances surrounding the allegations. While we did not substantiate all information included in the allegations, we did identify various weaknesses related to vulnerability management similar to those included in the allegations. Specifically, we were unable to substantiate that Bonneville required officials to stop patching systems. However, we did note that officials had not ensured all systems contained up-to-date security controls. Notably, Bonneville made efforts to improve its cybersecurity program since our prior review such as elevating the Chief Information Officer position for greater visibility, accountability, and oversight. However, we found that Bonneville had not implemented a fully effective cybersecurity program and continued to identify weaknesses in the areas of access controls, vulnerability and configuration management, and contingency planning. We also noted weaknesses related to risk management. In particular, we identified the following:

- Bonneville had not fully implemented effective logical access controls;

- We also found that physical access to Bonneville's data centers was not properly monitored;

- Similar to the findings from our prior report on Management of Bonneville Power Administration's Information Technology Program, a number of configuration management vulnerabilities existed on systems reviewed that weakened Bonneville's security posture; and

- Contingency planning and testing issues continued to exist at Bonneville.

The issues identified occurred, at least in part, because officials had not ensured that Federal and Bonneville requirements were updated and/or fully implemented. In addition, even when policies existed related to access control, configuration management, and vulnerability management, Bonneville officials had not taken appropriate actions to ensure that the policies were fully implemented. We also determined that, contrary to Federal requirements, Bonneville had not implemented an effective continuous monitoring program. For instance, Bonneville lacked separation of duties related to the individuals that designed security controls and tested those controls. Moreover, Bonneville did not effectively utilize plans of action and milestones, a critical component of an effective continuous monitoring program. In many instances, Bonneville did not track weaknesses through plans of action and milestones or did not correct weaknesses in a timely manner. Notably, Bonneville had created a distinct remediation team dedicated to monitoring identified weaknesses, focusing on those with the highest risk.

Notably, Bonneville had taken action to enhance access controls by significantly reducing the number of local system administrators with elevated privileges since our prior review. However, without improvements to its cybersecurity program, Bonneville may continue to operate systems at a higher than necessary risk of compromise, loss, modification, and non-availability. For instance, certain vulnerabilities identified could have permitted an attacker or malicious user to make unauthorized changes to data, disclose sensitive information, or deny legitimate users access to systems supporting business operations and other general

support systems. In addition, unaddressed weaknesses related to risk management and continuous monitoring will continue to contribute to vulnerable systems being approved to operate by the authorizing official. In light of the weaknesses identified, we made several recommendations that, if fully implemented, should aid officials in improving Bonneville's cybersecurity posture.

Management generally concurred with the report's recommendations and indicated that corrective actions had been initiated or were planned to address issues identified in the report.

Management did not concur with a portion of one recommendation concerning separation of duties, asserting that Bonneville's organizational structure sufficiently mitigated risk. (DOE-OIG-17-06)

Interim Storage of Transuranic Waste at the Department of Energy

The Department's National Transuranic (TRU) Program is an integral part of the mission to ensure the environmental cleanup of the nation's nuclear weapons complex. TRU waste includes radioactive waste resulting from national nuclear defense program activities. The National TRU Program integrates TRU waste cleanup goals and activities of independently managed Department sites across the complex. This includes TRU waste inventory characterization, certification, packaging, interim storage, transportation, and final disposal at the Department's Waste Isolation Pilot Plant (WIPP). In 2016, the Department estimated that about 97 percent of anticipated TRU waste was stored, or will be generated at large quantity sites. These sites consist of the Savannah River Site, Hanford Site (Hanford), Oak Ridge National Laboratory (ORNL), Idaho National Laboratory (Idaho), and Los Alamos National Laboratory (Los Alamos).

WIPP is the nation's only repository for the permanent disposal of defense-related TRU waste. In 2014, two unrelated incidents (a fire involving a salt haul truck on February 5th and a radiological release event on February 14th) led to the suspension of WIPP waste emplacement operations until January 4, 2017. As a result of the suspension, WIPP was unable to receive TRU waste shipments. Given the Department's regulatory commitments associated with TRU waste at multiple sites across the complex, we initiated this audit to evaluate the Department's strategy for interim storage of TRU waste until WIPP accepted TRU waste again. WIPP resumed waste emplacement operations on January 4, 2017.

Our evaluation of the Department's strategy for interim storage of TRU waste at large quantity sites found that the sites were able to meet their individual interim TRU waste storage needs until WIPP resumed operations. Also, although the Department did not satisfy all of its regulatory commitments related to TRU waste stored at large quantity sites, nothing came to our attention that would indicate that regulatory commitments impacted large quantity sites' plans to store TRU waste on-site until WIPP resumed operations.

The Department's guiding strategy for interim storage of TRU waste was to retain the waste at each individual site pending resumption of WIPP operations and, if possible, continue cleanup efforts. The Department's strategy also included evaluating the impact of interim on-site storage and commitments with state regulators at TRU waste sites. These

commitments affected the Department's decisions to either maintain TRU waste on-site or move TRU waste to an off-site interim storage location.

Because we found that large quantity sites were able to meet their individual interim TRU waste storage needs until WIPP resumed operations and there was no impact to the Department regarding regulatory commitments, we are not making any formal recommendations. (OAI-L-17-07)

Quality Assurance Management at the Waste Isolation Pilot Plant

The Department's Waste Isolation Pilot Plant (WIPP) in southeastern New Mexico is the nation's only geologic repository for the disposal of radioactive waste materials generated by atomic energy defense activities. WIPP is managed and operated by Nuclear Waste Partnership, LLC with oversight by the Department's Carlsbad Field Office. Its mission is to protect human health and the environment through safe management and disposal of certain transuranic wastes. WIPP is categorized as a Hazard Category 2 Nonreactor Nuclear Facility because it has the potential for significant radiological consequences. To provide protection against such consequences, WIPP utilizes Safety Class/Safety Significant systems and components in its infrastructure and equipment. These items are designed to provide protection against radioactive exposure to the public and safety to the worker.

WIPP's management and operating contract requires compliance with the Department Order 414.1D Quality Assurance, and that WIPP develop and conduct work in accordance with a Department approved quality assurance plan. In addition, WIPP's contract requires the implementation and maintenance of a quality assurance program in accordance with the provisions of 40 Code of Federal Regulations Part 194. The Carlsbad Field Office provides oversight to ensure proper implementation of quality assurance at WIPP. Due to the importance of protecting the public, workers, and environment, we initiated this audit to determine whether WIPP effectively managed quality assurance requirements.

Our review found that WIPP had not always effectively managed quality assurance requirements. Specifically, we found that WIPP did not always effectively:

- Perform commercial grade dedications of items relied on for safety. We found instances where WIPP did not effectively perform technical evaluations and/or the acceptance process, which are both key parts of an effective commercial grade dedication.

- Evaluate suppliers' abilities to meet quality assurance requirements prior to and after contract award. One of WIPP's methods for evaluating suppliers prior to contract award did not effectively evaluate a supplier's ability to meet quality assurance requirements.

- Identify the appropriate quality assurance requirements in contract documents. We found instances where WIPP did not specifically state in procurement documents the quality assurance program or standard that the supplier should adhere to.

- Maintain adequate document control of quality assurance documents. We found instances where WIPP did not include document revision numbers, dates, and titles in its procurement documents to ensure the appropriate documents were utilized.

We concluded that these weaknesses were attributable to limited oversight by the Carlsbad Field Office. In particular, although the Carlsbad Field Office provided oversight of quality assurance activities through audits and surveillances, we determined that, since May 2013, its oversight was limited and did not identify these weaknesses until after we brought the issues to the attention of the Carlsbad Field Office.

Ineffective implementation of quality assurance requirements limits WIPP's ability to provide reasonable assurance of safe future operations. Furthermore, problems associated with poor quality assurance can result in increased costs and future operational delays. Given WIPP's integral role in the Department's cleanup mission, it is imperative that quality assurance requirements are met in order to help eliminate future delays and additional costs to taxpayers.

Although the Department and WIPP have taken positive steps to address some of the weaknesses identified, we believe that additional steps are needed to ensure that quality assurance requirements are met for all future operations at WIPP. Accordingly, we made recommendations to ensure effective quality assurance performance at WIPP. Management concurred with our recommendations and has initiated corrective actions. (DOE-OIG-17-07)

The Department of Energy's Implementation of Multifactor Authentication Capabilities

The Department operates many types of information systems supporting mission related activities such as nuclear security, scientific research and development, and environmental management. Strengthening cybersecurity over its information technology environment is a significant challenge facing the Department. Federal requirements and industry best practices indicate that multifactor authentication is one of the most effective methods of safeguarding information systems. In its most basic form, authentication is the process of verifying the identity of a user prior to allowing access to an information system. While the most common method of authentication is username and password, multifactor authentication adds rigor to the authentication process using two or more different authenticators such as hardware security tokens and personal identity verification (PIV) cards.

Federal requirements concerning multifactor authentication on Federal information systems, including those operated by contractors, have existed for many years. For instance, the Office of Management and Budget (OMB) issued M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, in August 2005 which required Federal agencies to implement multifactor authentication, in the form of PIV cards, for logical and physical access to Federal facilities and information systems. More recently, in June 2015, OMB initiated a 30-day Cybersecurity Sprint initiative to further emphasize access controls over Federal information systems by directing that all privileged users and most standard

users utilize PIV card credentials to access information systems by September 30, 2016. We initiated this audit to determine whether the Department effectively implemented multifactor authentication when securing its information systems.

The Department made progress towards fully implementing multifactor authentication in accordance with Federal requirements. Specifically, the Department recently invigorated its efforts to meet the demands of the OMB Cybersecurity Sprint; however, we found that additional effort was needed for access to technology resources to ensure that multifactor authentication, including the use of PIV cards, was fully implemented across the Department. In particular, our review of 18 Federal information systems, including those systems operated by contractors, identified weaknesses related to ensuring adequate protections over access to network and application resources, and noted that information reported to OMB related to the Cybersecurity Sprint was not always consistent. Specifically, we found:

- Although requirements existed for more than 10 years, none of the locations reviewed had fully implemented multifactor authentication for secure access to information systems and resources.

- Federal and contractor locations tested had not always considered the applicability of multifactor authentication for software applications, including those that contained sensitive information such as personally identifiable information and personal health information.

- Information reported to OMB by the Department related to progress implementing the Cybersecurity Sprint was not consistent and did not portray an accurate accounting of its use of multifactor authentication.

The weaknesses identified occurred, in part, because officials had not fully planned for implementation of multifactor authentication on information systems. Department guidance and requirements related to multifactor authentication technologies also were not always communicated effectively. Without development and implementation of a Department-wide multifactor authentication process, the Department's information, including sensitive data, will continue to be at a higher-than-necessary risk of compromise. We have made recommendations that, if fully implemented, should help the Department enhance its cybersecurity posture through effective implementation of multifactor authentication. Management concurred with the report's recommendations and indicated that corrective actions had been initiated or were planned to address the issues identified in the report. (DOE-OIG-17-08)

Allegation of Nepotism and Misuse of Position Within the Office of Management

The Office of Management provides the Department with direction and oversight for management, procurement, and administrative services. The Office of the Chief Human Capital Officer (Human Capital) leads the Department on the impact and use of policies and programs related to human capital management. However, while Human Capital provides various hiring related services to program offices, selection authority is vested in individual offices such as the Office of Management.

In the past, the Department has experienced violations of laws and regulations regarding nepotism, misuse of position, and prohibited personnel practices by employees in various program offices seeking employment for their relatives. In June 2016, we were informed by senior Office of Management officials that one if its employees (herein identified as "Employee") within the Office of Policy potentially violated the statute on nepotism and regulations regarding misuse of position when he provided his daughter's resume to a Headquarters Procurement Services' (Procurement Services) hiring official within the Office of Management. We initiated this audit to ascertain the facts and circumstances surrounding the attempted hiring action, and to determine whether it was conducted in compliance with Federal laws, regulations, and Departmental policies.

We determined, based on coordination and confirmation from the Department's Office of the General Counsel, actions taken by the Employee and Procurement Services' hiring officials resulted in violations of laws and regulations pertaining to prohibited personnel practices and misuse of position. We found that the Employee advocated for employment for his daughter. Specifically, the Employee provided his daughter's resume to a Procurement Services' hiring official and communicated with the hiring official regarding potential Federal employment on at least two occasions. Additionally, we determined that three Procurement Services' hiring officials demonstrated a loss of impartiality and granted an unauthorized preference to the Employee's daughter when hiring actions were taken while being aware of the family relationship. Hiring actions included interviewing and recommending employment for the Employee's daughter.

Based on work performed, we concluded that the Employee violated the regulation governing misuse of position, but the Employee had not violated the statute related to nepotism as alleged in the complaint. Confirmation received from the Department's Office of the General Counsel stated that the Employee was not a public official, as defined in Title 5 U.S. Code, Section 3110 (a), and was not subject to the laws pertaining to nepotism. As such, we determined that the Employee could not have violated the statute related to nepotism.

Senior officials within the Office of Management took prompt action to stop the hiring action when notified of the employment selection. The hiring request was also separately flagged by Human Capital's Human Resources Service Center because the resume was not submitted under, nor did it meet the experience requirements of, the vacancy announcement. Although the hiring issue was identified and dealt with in a timely and proper manner, it raises concerns regarding the hiring practices within the Office of Management, and more specifically Procurement Services, that require immediate attention.

Prohibited personnel practices and misuse of position circumvent the integrity of the competitive hiring process, can damage the effectiveness and morale of an organization, and can erode the public's trust in the Federal hiring system. Even though the Office of Management took prompt action to identify and address the matter, and the Employee's daughter was not hired, we identified some issues we believe need to be addressed by the Office of Management and the Acting Chief Human Capital Officer.

To address the specific instance of misuse of position and violations of the prohibited personnel practices described in this report, we made recommendations to the Director of the Office of Management and the Acting Chief Human Capital Officer. Management concurred with the report's recommendations and identified a number of actions that were either completed or planned to address our recommendations. (DOE-OIG-17-09)

INSPECTION REPORTS

Alleged Security and Safety Concerns at the Oak Ridge National Laboratory

The Oak Ridge National Laboratory (ORNL) is the Department's largest science and energy laboratory. ORNL operates in an open campus environment to encourage collaboration and the sharing of knowledge, and is co-located with a Federal site office managed by the Office of Science, which oversees its operations. Federal managers are responsible for ensuring that ORNL is adequately defended against actions that could result in destruction of Government property or endanger the health and safety of employees or the public. ORNL is also subject to additional security requirements because it is home to Building 3019, a facility that stores Special Nuclear Materials (SNM).

We received a complaint involving perceived security concerns at Building 3019 and safety and security concerns at a vehicle entry portal on the ORNL site. We initiated a review to determine the severity of these issues and whether Department management had taken or planned any necessary corrective actions.

We substantiated that some of the situations described by the complainant did exist, as alleged. We noted however, that these situations were aligned with procedures and strategies approved by cognizant managers, and Federal officials were aware of the practices employed at the site. After reviewing the results of our observations and testing, we concluded that the allegations were likely based on the complainant's interpretations of activities at Building 3019, which did not always benefit from a full understanding of the observed operations. During our review, we also identified other concerns related to vehicle searches at the site's entry portals and the secondary response force.

During our review, we identified other concerns related to vehicle searches at the entry portals and the secondary response force. While observing search procedures at ORNL's entry portal, we identified two instances where the search was not conducted in accordance with established requirements. A senior protective force official concurred with our conclusions and promptly issued clarification of procedures to be followed in such cases. Further, site officials developed official policy on this matter and agreed to coordinate with protective force management to prevent future occurrences.

The false and nuisance alarms at Building 3019 were due, in part, to the selection and configuration of alarm system components, but upgrades to the system were underway prior to our review and are expected to be completed by June 2017. Therefore, we are not making any recommendations, but we suggest that the ORNL Site Office Manager ensure these upgrades are completed to mitigate the possibility of alarms causing complacency among protective force personnel in the future. (OAI-L-17-05)

Construction Rework at the Mixed Oxide Fuel Fabrication Facility

In 1999, the National Nuclear Security Administration (NNSA) contracted with a consortium, now named CB&I AREVA MOX Services LLC (MOX Services), to design, build, and operate a Mixed Oxide Fuel Fabrication Facility (MOX Facility). This facility is intended to be a major component in the United States' program to dispose of surplus weapons-grade plutonium. At that time, the MOX Facility had an estimated total project cost of

almost $5 billion with a projected completion date of September 2016. According to the 2016 Updated Performance Baseline for the Mixed Oxide Fuel Fabrication Facility at the Savannah River Site, issued in September 2016, the MOX Facility is expected to cost $17 billion with a completion date as late as 2048.

Over the last several years, the MOX Facility has been the focus of several audits and reviews to evaluate project cost increases and schedule delays. Additionally, our Hotline received and referred to NNSA an allegation that construction rework contributed to the cost issues at the MOX Facility and resulted in a waste of Department's funds. In response to the OIG Hotline referral, NNSA performed an assessment that substantiated the allegation. We initiated this inspection to determine whether NNSA had responded to concerns regarding construction rework at the MOX Facility.

We found that NNSA had directed MOX Services to establish an effective management system to address construction rework at the MOX Facility. As a result, MOX Services developed and implemented a comprehensive new desktop procedure. NNSA also increased its oversight of rework. Because the construction rework procedure and oversight processes were recently implemented, we determined that it was too early to fully assess their effectiveness. However, we noted that NNSA was still in the process of resolving the alleged waste of Department funds related to construction rework substantiated in its assessment.

We suggest NNSA continue to monitor construction rework and implement additional process improvements deemed necessary to mitigate future occurrences. However, to improve MOX Facility construction rework management, we made recommendations to the Contracting Officer for the MOX Project Management Office. Management concurred with the report's recommendations and provided a path forward to address the issues identified in the report. (OAI-M-17-07)

Alleged Tesa Access Issues At Lawrence Livermore National Laboratory

The National Nuclear Security Administration's Lawrence Livermore National Laboratory (Livermore) is managed and operated by Lawrence Livermore National Security, LLC (LLNS). The Livermore Field Office administers the National Nuclear Security Administration's management and operating contract with LLNS. As a national security laboratory, Livermore has an extensive security infrastructure in place. Livermore's Locks, Keys, and Tesa Group (LKTG) manages the Tesa locks at the site. Tesa locks are electro-mechanical locks that are accessed by inserting a Tesa-encoded card into the lock. Tesa locks can be attached to internal and external doors, or lockboxes to a classified network. A personalized pin may also be required to access certain Tesa locks. LKTG also maintains a Tesa database that is required to contain information on all Tesa locks to which individuals have access at Livermore.

We received an allegation that Livermore's Tesa database contained outdated and incorrect data and that this constituted a serious security issue. This incorrect data surfaced after an employee lost his/her Tesa-encoded Livermore Site identification (ID) card in 2014. Specifically, it was alleged that the employee's Tesa locking plan included numerous Tesa locks for which the employee did not have a current need, could not access, or could not

locate. We initiated this inspection to examine the facts and circumstances surrounding the allegation.

We substantiated the allegation that Livermore's Tesa database contained incorrect data. Of the 63 locks on the employee's locking plan we found:

- 44 Tesa locks for which the employee had no current mission-related need, 5 Tesa locks that the employee was erroneously given access to, and 1 Tesa lock that had been removed from service; and

- 13 locks on the employee's locking plan for Tesa lockbox's related to a classified network account.

A Livermore official told us that any individual that has access to a Tesa lockbox must have an established account to access Livermore's classified network. The employee had an established account to access Livermore's classified network, so he/she had a need for the 13 Tesa lockboxes on his/her locking plan. However, since the employee did not fully complete the lost badge recovery process, LKTG took action to remove the employee's access to 6 of the 13 Tesa lockboxes related to a classified network account. When we discussed this issue with Livermore management, a senior official indicated that this individual's circumstances posed no risk to Livermore's classified network.

Additionally, we found that for 23 of the 85 Livermore employees included in a judgmental sample, information stored in the Tesa database had not been updated in a timely manner or in accordance with Livermore's Locks, Keys, and Tesa Policy and Procedures.

The Tesa database contained outdated and incorrect data because Livermore did not always accurately maintain its employee's Tesa locking plans within its areas of responsibility. The non-mission-related Tesa locks on the employee's locking plan, and the additional Tesa database issues from our sample existed because Livermore did not always have adequate controls in place to ensure that Tesa locks were removed from the employee's locking plans when the mission-related need ceased.

We made recommendations to the Manager of the Livermore Field Office. Management concurred with the report's recommendations and indicated that Livermore has already made process and internal control improvements and has additional actions planned to address the report's recommendations. (OAI-M-17-09)

Allegations of Mismanagement of the Human Reliability Program at the Oak Ridge National Laboratory

The Department's Human Reliability Program (HRP) was established to address the need for individuals involved in the nuclear weapons program to meet the highest standards of reliability including physical and mental suitability. Employees entering the program must possess a Q (which affords access up to the Top Secret level) clearance and submit to a multi-phase certification process that is designed to identify and evaluate behaviors and conditions that may disqualify employees from holding HRP positions. National Strategic Protective Services, LLC (NSPS) provides protective force services at the Department's

facilities in Oak Ridge, Tennessee, including the Oak Ridge National Laboratory. Security Police Officers guarding special nuclear material at the Oak Ridge National Laboratory are required to maintain HRP certification.

We received a complaint alleging NSPS management: (1) failed to provide employees timely written notifications when an employee's HRP certification was removed; (2) used disparate application of discipline; and (3) did not follow proper HRP drug testing procedures by ordering drug tests without cause.

Although we substantiated the allegation that NSPS management did not provide employees timely written notifications when an employee's HRP certification was removed, this occurred because there was no requirement for NSPS to do so in all instances. In addition, we were unable to substantiate the allegation regarding disparate discipline, nor did we substantiate the allegation that NSPS management did not follow proper HRP drug testing procedures.

We identified opportunities for improvement in HRP internal controls related to recordkeeping and access control procedures. Specifically, none of the parties involved in the NSPS HRP process maintained a complete list of all employees whose certifications had been temporarily or immediately removed, including such information as the dates of removal and any subsequent reinstatements. Without comprehensive recordkeeping, certification reviewers and management could be lacking vital information to easily trend an employee's personnel actions when making future certification and employment decisions.

We made a recommendation and suggestions designed to mitigate the risks associated with concerns noted in our inspection. Management concurred with the report's recommendation and provided a path forward to address the issues identified in the report. Management's planned actions are responsive to our recommendation. (OAI-M-17-10)

The following identifies the sections of this report that address each of the reporting requirements prescribed by the Inspector General Act of 1978, as amended.

SECTION	REPORTING REQUIREMENT	PAGE
4(a)(2)	Review of Legislation and Regulations	14
4(A)(17)(A)	Total number of issued investigative reports	3
4(D)(17)(B)	Referrals to prosecuting authorities for criminal prosecution	3
4(D)(17)(C)	Total number of persons referred to the State local prosecuting authorities for criminal prosecution	3
4(D)(17)(D)	Total number of indictments and criminal informations during the reporting period that resulted from any prior referral to prosecuting authorities	3
4(D)(18)	Description of the metrics used for developing the data for the statistical tables	3
4(D)(19)	Investigation Involving Senior Government Employees	14
4(D)(20)	Instances of Whistleblower Retaliation	15
4(D)(21)	Information Assistance Refused or Not Provided	14
4(D)(22)	Reviews Closed and Not Disclosed to the Public	22
5(a)(2)	Recommendations for Corrective Action to Significant Problems	34-54
5(a)(3)	Previous Reports' Recommendations for Which Corrective Action Has Not Been Implemented	16-20
5(a)(4)	Matters Referred to Prosecutive Authorities	23-33
5(a)(6)	Audit Reports Issued in This Reporting Period	11-12
5(a)(7)	Summary of Significant Reports	34-54
5(a)(8)	Reports with Questioned Costs	4
5(a)(9)	Reports with Recommendations That Funds Be Put to Better Use	4
5(a)(10)	Previous Audit Reports Issued with No Management Decision Made by End of This Reporting Period	15
5(a)(11)	Significant Revised Management Decisions	N/A
5(a)(12)	Significant Management Decisions with which the OIG is in Disagreement	N/A
5(a)(13)	Federal Financial Management Improvement Act-related Reporting	N/A
5(a)(14–16)	Peer Review Results	22

The U.S. Department of Energy is headquartered in Washington, DC and currently operates the Energy Information Administration, the National Nuclear Security Administration, 21 preeminent research laboratories and facilities, four power marketing administrations, nine field offices, and 10 Program Offices which help manage the Department's mission with more than 15,000 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 260 employees, the organization strives to be a highly effective organization that promotes positive change.

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

Contact Information:

- Complaint Form: http://energy.gov/ig/office-inspector-general
- Toll Free Telephone Number: 1-800-541-1625
- Washington DC Metro Telephone Number: 202-586-4073
- Email Address: ighotline@hq.doe.gov
- Physical Address: U.S. Department of Energy
  1000 Independence Ave, SW
  Washington, DC 20585

FEEDBACK

The contents of this Semiannual Report to Congress comply with the requirements of the Inspector General Act of 1978, as amended. If you have any suggestions for making the report more responsive, please provide the following information by clicking the "submit email" button below:

- Name
- Telephone Number
- Comments/Suggestions/Feedback