

# Semiannual Report to Congress

April 1, 2017 – September 30, 2017

OIG-CA-18-004

Office of Inspector General  
Department of the Treasury



## Highlights

During this semiannual reporting period, the Office of Audit issued 30 products. The office also identified more than \$1 million in questioned costs. Work by the Office of Investigations resulted in 74 arrests, 35 indictments, and 32 convictions. Some of our more significant results for the period are described below:

- Office of Audit issued six reports to the Department of the Treasury (Treasury) on States' compliance with State Small Business Credit Initiative (SSBCI) program requirements and prohibitions. Reports issued for Rhode Island, Wisconsin, and Oregon identified questioned costs of \$803,644, \$261,000, and \$6,750, respectively.
- In our 2017 report on Treasury's compliance with the Federal Information Security Modernization Act of 2014 (FISMA), we recounted unresolved issues from the prior year and identified new matters that need improvement related to Treasury's information security program and practices for its intelligence systems.
- For the sixth consecutive year, we concluded that Treasury was not in compliance with the Improper Payments Elimination and Recovery Act of 2010 (IPERA) due to the Internal Revenue Service's Earned Income Tax Credit program deficiency reported by the Treasury Inspector General for Tax Administration.
- Our investigation, involving allegations that a solar energy company violated the False Claims Act by submitting thousands of inflated applications to Treasury under Section 1603—Payments for Specified Energy Property in Lieu of Tax Credits of the American Recovery and Reinvestment Act of 2009 (1603 Program) resulted in a multi-level agreement wherein the company agreed to a settlement of \$29.5 million.
- Our investigation of a check cashing business in Dallas, Texas, determined that the owner of the money services business facilitated in the negotiation of nearly 3,500 fraudulently obtained Treasury checks totaling \$16.6 million. The subject pled guilty to Failure to Develop, Implement, and Maintain an Anti-Money Laundering Program in the Northern District of Texas, Dallas Division.
- Our investigation of a stolen Treasury check for \$28,000 revealed a criminal scam orchestrated by a subject that involved a business and personal email compromise scheme prompting wire transfers amounting to over \$227,000 from victims. Additionally, the subject fraudulently obtained and negotiated business checks totaling over \$52,000, and falsely filed Federal income tax returns. The subject was charged with Mail Fraud, Bank Fraud, and Aggravated Identification Theft and sentenced to 168 months in prison, 60 months of probation, and ordered to pay \$722,000 in restitution for fraud attempts exceeding \$32 million that affected 3,000 victims. Upon the subject's release from prison, an immigration deportation review will determine continued residency in the United States.



## Message from the Inspector General

I am pleased to present the Department of the Treasury (Treasury) Office of Inspector General (OIG) Semiannual Report to Congress for the 6 month period ended September 30, 2017.

I would like to acknowledge the work of our Office of Audit and Office of Counsel on Treasury's State Small Business Credit Initiative (SSBCI) Program that ended on September 27, 2017. This program disbursed \$1.4 billion to various State programs to encourage lending to and investment in small businesses. Given the program's sunset date, we considered these audits high priority as we continued to find misuse of funds. In this semiannual period alone, we issued reports that identified more than \$1 million in questioned costs.

Our Office also continued to focus its resources on meeting its statutory obligations. This included completing our annual evaluation of Treasury's information security program and practices required by the Federal Information Security and Modernization Act of 2014 (FISMA), and reporting on Treasury's compliance with the Improper Payments Elimination and Recovery Act of 2010 (IPERA). We assigned our remaining resources to Congressional requests and discretionary work that results from emerging risks with potential impact to programs and operations under our oversight.

Our Office of Investigations teamed up with the Internal Revenue Service Criminal Investigations and the U.S. Postal Inspection Service to identify multiple fraud schemes that have resulted in a loss of over \$20 million to Treasury. The team's efforts have been instrumental in preventing the loss of an additional \$25 million and helping to build filters to reduce the success rate of fraud schemes confronting Treasury programs and operations.

In closing, I would like to express my appreciation to all Treasury OIG staff for making possible the significant audit and investigative results that are summarized in this Semiannual Report, and to Congress and Treasury for their sustained commitment to the important work of our office.

/s/

Eric M. Thorson  
Inspector General

This page intentionally left blank.

# Contents

<b>Highlights</b> .....	<b>i</b>
<b>Message from the Inspector General</b> .....	<b>ii</b>
<b>Office of Inspector General Overview</b> .....	<b>1</b>
<b>Management and Performance Challenges</b> .....	<b>5</b>
<b>Office of Audit – Significant Audits and Other Products</b> .....	<b>11</b>
State Small Business Credit Initiative .....	11
Cyber/Information Technology .....	15
DATA Act.....	16
RESTORE Act.....	18
American Recovery and Reinvestment Act.....	19
Financial Management .....	20
Other Audits of Treasury Programs and Operations .....	24
<b>Office of Investigations – Significant Investigations</b> .....	<b>29</b>
<b>Other OIG Accomplishments and Activities</b> .....	<b>47</b>
<b>Statistical Summary</b> .....	<b>55</b>
Summary of OIG Activity .....	55
Metrics Used for Office of Investigations Activities .....	55
Reports With Unimplemented Recommendations.....	56
Closed Investigations of Senior Government Employees Not Publicly Disclosed.....	63
Summary of Instances of Whistleblower Retaliation.....	63
Summary of Attempts to Interfere With OIG Independence, Including Instances Where Information or Assistance Request was Refused .....	63
Listing of Audit Products Issued .....	64
Audit Reports Issued With Questioned Costs.....	68
Audit Reports Issued With Recommendations that Funds Be Put to Better Use .....	69
Reports for Which No Management Comment was Returned Within 60 Days .....	70
Reports Issued Over 6 Months for Which No Management Decision Has Been Made .....	70
Significant Revised Management Decisions .....	70
Significant Disagreed Management Decisions .....	70
Peer Reviews .....	71

**Other Reporting Requirements and Requests..... 73**  
**References to the Inspector General Act ..... 77**  
**Abbreviations ..... 79**

## Office of Inspector General Overview

The Department of the Treasury's (Treasury) Office of Inspector General (OIG) was established pursuant to the 1988 amendments to the Inspector General Act of 1978. OIG is headed by an Inspector General appointed by the President with the advice and consent of the Senate.

OIG performs independent, objective reviews of Treasury programs and operations, except for those of the Internal Revenue Service (IRS) and the Troubled Asset Relief Program (TARP), and keeps the Secretary of the Treasury and Congress fully informed of problems, deficiencies, and the need for corrective action. The Treasury Inspector General for Tax Administration (TIGTA) performs oversight related to IRS. A Special Inspector General and the Government Accountability Office (GAO) perform oversight related to TARP.

OIG also performs independent oversight of programs and operations funded by the Gulf Coast Restoration Trust Fund (Trust Fund) established within Treasury by the Resources and Ecosystems Sustainability, Tourist Opportunities, and Revived Economies of the Gulf Coast States Act of 2012 (RESTORE Act). In addition to performing oversight of Treasury-related activities, OIG performs oversight of programs and operations administered by the Gulf Coast Ecosystem Restoration Council (Council), established as an independent Federal entity, and the Gulf Coast Ecosystem Restoration Science, Observation, Monitoring, and Technology Program (Science Program) administered by the National Oceanic and Atmospheric Administration (NOAA). With regard to the Council and the Science Program, OIG keeps the appointed Chairperson of the Council, the NOAA Science Program Administrator, and Congress fully informed of problems, deficiencies, and the need for corrective actions.

OIG has four components: (1) Office of Audit; (2) Office of Investigations; (3) Office of Counsel; and (4) Office of Management. OIG is headquartered in Washington, DC. OIG also has an audit office in Boston, Massachusetts, and investigative offices in Greensboro, North Carolina; Houston, Texas; and Jacksonville, Florida.

The Office of Audit, under the leadership of the Assistant Inspector General for Audit, performs and supervises financial and performance audits, attestation engagements, and evaluations. The Assistant Inspector General for Audit also serves as the Special Deputy Inspector General for Small Business Lending Fund (SBLF) Program Oversight. Under the Assistant Inspector General for Audit, there are three deputies. The first

deputy is primarily responsible for financial sector audits to include audits of banking supervision, manufacturing of currency and coins, and alcohol and tobacco excise tax revenue collection activities; the second deputy is primarily responsible for financial management and transparency audits to include financial audits of Treasury and the Council performed by OIG staff and contractors, audits of Government-wide collection, payment, and debt programs and operations, and audits of anti-money laundering/terrorist financing, foreign sanction, and intelligence programs and operations; and the third deputy is primarily responsible for cybersecurity and financial assistance audits to include audits of Treasury and the Council information systems performed by OIG staff and contractors, and audits of the SBLF, State Small Business Credit Initiative (SSBCI), and RESTORE Act programs and operations.

The Office of Investigations, under the leadership of the Assistant Inspector General for Investigations, performs investigations and conducts initiatives to detect and prevent fraud, waste, and abuse in programs and operations under our jurisdiction. The Office of Investigations also manages the Treasury OIG Hotline to facilitate reporting of allegations involving these programs and operations. The Assistant Inspector General for Investigations is supported by a deputy in leading both the day-to-day operations and task force initiatives in Washington, DC; Greensboro, North Carolina; Houston, Texas; and Jacksonville, Florida.

The Office of Counsel, under the leadership of the Counsel to the Inspector General, provides legal advice to the Inspector General and all OIG components. The office represents the OIG in administrative legal proceedings and provides a variety of legal services, including (1) processing Freedom of Information Act and *Giglio*<sup>1</sup> requests; (2) conducting ethics training; (3) ensuring compliance with financial disclosure requirements; (4) reviewing proposed legislation and regulations; (5) reviewing administrative subpoena requests; and (6) preparing for the Inspector General's signature, cease and desist letters to be sent to persons and entities misusing the Treasury seal and name. Counsel also responds to media and Congressional inquiries and serves as the Whistleblower Ombudsman for Treasury, pursuant to the Whistleblower Protection Enhancement Act of 2012.

The Office of Management, under the leadership of the Assistant Inspector General for Management, provides services to maintain the OIG administrative infrastructure.

---

<sup>1</sup> *Giglio* information refers to material that may call into question the character or testimony of a prosecution witness in a criminal trial.

OIG's fiscal year 2017 appropriation is \$37 million; the OIG's oversight of SBLF and SSBCI programs and operations is funded on a reimbursable basis. As of September 30, 2017, OIG had 169 full-time staff.

This page intentionally left blank.

## Management and Performance Challenges

The Reports Consolidation Act of 2000 requires that the Department of the Treasury (Treasury) Inspector General annually provide his perspective on the most serious management and performance challenges facing Treasury and the Gulf Coast Ecosystem Restoration Council (Council). The following is a synopsis of Inspector General Thorson's annual assessments which are available, in their entirety, on the Treasury Office of Inspector General (OIG) [website](#).

### Treasury's Management and Performance Challenges

In a memorandum to Secretary Steven Mnuchin dated October 16, 2017, Inspector General Eric Thorson reported four challenges facing Treasury. Three are repeat challenges previously reported and one is new. One previously reported challenge and one other matter of concern were removed.

The four challenges that were reported follow.

#### Operating in an Uncertain Environment (New Challenge)

In assessing Treasury's most serious challenges, we remain mindful of external factors and future uncertainties that affect its operations. Most notable are the proposed budget cuts and new requirements imposed by Executive Order (EO) 13781, "Comprehensive Plan for Reorganizing the Executive Branch" (March 13, 2017). In its implementation of EO 13781, Office of Management and Budget (OMB) required agencies to submit Agency Reform Plans, which include long-term workforce plans in alignment with their strategic plans, to OMB concurrently with their fiscal year 2019 budget requests. After consideration of all Agency Reform Plans, OMB intends to work with agencies in developing crosscutting reform proposals that involve multiple agencies, which could include merging agencies, components, programs, or activities that have similar missions. These proposals, along with the agency plans and public input, will be used by OMB in developing its comprehensive Government-wide Reform Plan to reorganize the Executive Branch. With looming uncertainties as to the impact of the Government-wide Reform Plan, Treasury must plan for the potential long-term restructuring of certain functions or offices/bureaus and/or budget cuts. In addition, Congress has yet to resolve unfinished business when it comes to the Nation's debt, and the long-term sustainability of large programs. Tackling these more critical matters at hand could be more

challenging as several Presidentially-appointed, Senate-confirmed leadership positions within Treasury remain vacant since January 2017.

### **Cyber Threats (Repeat Challenge)**

Cybersecurity is a long-standing and serious challenge facing the Nation today. A reliable critical infrastructure, including information systems and networks, is vital to our national security and economic stability. Cyber threats are a persistent concern as Treasury's information systems are critical to the core functions of Government and the Nation's financial infrastructure. As cyber threats continue to evolve and become more sophisticated and subtle, they pose an ongoing challenge for Treasury to fortify and safeguard its internal systems and operations and the financial sector it oversees. This challenge acknowledges that it is a Government-wide challenge to ensure there are sufficient numbers of cybersecurity professionals.

### **Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement (Repeat Challenge)**

This challenge focuses on the difficulties Treasury faces in identifying, disrupting, and dismantling the financial networks that support terrorists, organized transnational crime, weapons of mass destruction proliferators, and other threats to international security that continue to be challenging. Concerns over Office of Terrorism and Financial Intelligence's ability to meet mission critical objectives are heightened by multiple vacant key positions and the strained relationship among several of its offices. Some key leadership positions have been vacant for a number of years. Major challenges for the United States and Treasury involve stopping the Islamic State of Iraq and Syria (ISIS), rogue regimes and countries, and other bad actors who want to harm people and properties and disrupt the global financial system. Enhancing the transparency of the financial system is one of the cornerstones of the effort to disrupt the ability of terrorist organizations. Other concerns include the increasing use of mobile banking, internet banking, internet gaming, and peer-to-peer transactions; and money service businesses, including virtual currency administrators and exchanges. Given the criticality of Treasury's mission to combat terrorist financing and money laundering, we consider anti-money laundering and combating terrorist financing to be inherently high-risk areas.

### **Efforts to Promote Spending Transparency and to Prevent and Detect Improper Payments (Repeat Challenge)**

Treasury continues to make progress in its Government-wide and Department-wide implementation of the Digital Accountability and Transparency Act of 2014 (DATA Act). The DATA Act requires the Federal Government to provide consistent, reliable, and useful online data about how it spends taxpayer dollars. Given the broad Government-wide implications and critical roles assigned to Treasury by the DATA Act, we consider this an ongoing high-risk implementation project and management challenge.

In light of the continuing problem with improper payments (estimated at \$144 billion, or 4.67 percent of all program outlays, for fiscal year 2016), the Federal Government has intensified efforts to reduce improper payments in major Federal programs. The Do Not Pay Initiative and the Bureau of the Fiscal Service's (Fiscal Service) Do Not Pay Business Center are chief components of efforts designed to prevent and detect improper payments to individuals and entities. As previously reported, the effectiveness of the Do Not Pay Business Center as a tool to prevent and detect improper payments is hindered because the center does not have access to, among other things, Social Security Administration's full death data. With its potential to reduce improper payments, the Do Not Pay Business Center is a major and important undertaking by Fiscal Service and Treasury.

### **Other Matters of Concern**

In addition to the above challenges, Inspector General Thorson reported elevated concerns about two matters that were repeated from last year's memorandum, (1) challenges with currency and coin production and (2) lapses by Treasury in maintaining a complete and concurrent record of key activities and decisions.

## **Gulf Coast Ecosystem Restoration Council Management and Performance Challenges**

In an October 16, 2017, letter to the Acting Executive Director for the Chairperson of the Gulf Coast Ecosystem Restoration Council, Inspector General Thorson acknowledged the continuing challenges of establishing a relatively new Federal entity emphasizing the following management and performance challenges, two of which

were repeated from last year and one is a new challenge. One previously reported challenge was removed.

### **Implementing an Infrastructure to Administer Gulf Coast Restoration Activities (Repeat Challenge)**

While Council made progress in filling critical administrative and programmatic positions and solidified many policies and procedures supporting internal control, problems still exist in filling key positions necessary to complete an organizational infrastructure. Most notable, the Executive Director departed on January 26, 2017, leaving this position vacant over the past 8 months. Furthermore, the Acting Executive Director dedicates about 50 percent of his time to the Council and must rely heavily on the senior executive staff. Key positions remain vacant in other operational areas, and only until quite recently has a person been identified and selected for the position of Chief Information Officer. Inconsistent staffing impedes the Council's ability to address information technology related challenges and risks. Infrastructure challenges should also be considered in context with OMB's update to Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control." The Council completed its initial risk management profile in May 2016. One of the key recommendations was to create an Enterprise Risk Management (ERM) staff function. Accordingly, the Council determined that a dedicated ERM Specialist position will be created to manage and implement ERM. To date, the Council has not filled this critical position.

### **Federal Statutory and Regulatory Compliance (Repeat Challenge)**

The Council must ensure that activities and projects funded by the RESTORE Act meet all environmental laws and regulations at the Federal and State level. The Council must also ensure its own compliance with applicable laws and regulations as a Federal entity. This challenge focuses on the Council's ability to meet requirements of the DATA Act and the Improper Payments Elimination and Recovery Act of 2010 (IPERA). The Council relies on a manual review and reconciliation process with limited staff to comply with all DATA Act requirements. Complicating this situation is the recent decision of the Council's contractor to no longer support the Restoration Assistance and Award Management System application. As such, the Council will need to acquire and migrate its financial assistance award and interagency agreement data to a new system and ensure all Federal information system and security requirements are met. As the Council continues to grow and anticipates the volume of reportable

data to significantly increase, a more automated process will be necessary to ensure complete and accurate data is reported on USAspending.gov. In addition, we expect that in the upcoming years as grant activity increases, the Council will be above the threshold of reporting requirements of IPERA.

### **Grant and Interagency Agreement Compliance Monitoring (New Challenge)**

The Council established the Initial Comprehensive Plan in 2013 and the Initial Funded Priorities List in 2015, and now staff are transitioning into the tasks of awarding funds. As such, the Council must now begin to conduct the necessary monitoring of projects and award recipients' progress, reporting, and compliance with their award agreements. The Council awarded over 20 grants and interagency agreements valued at approximately \$70 million under the Council Selected Restoration Component (\$64 million) and the Spill Impact Component (\$6 million). Current staffing levels may be sufficient to ensure the proper oversight of grants for this volume of awards. However, a significant increase in grant activity could potentially overwhelm a new and developing grants management staff. Additionally, compliance monitoring of grants, contracts, and interagency agreements should be considered in the context of the ERM requirements and the related staffing challenges. Specifically, of the seven top risks identified resulting from the Council's initial ERM risk management profile, five of them relate to the oversight and monitoring of grants.

This page intentionally left blank.

# Office of Audit – Significant Audits and Other Products

## State Small Business Credit Initiative

As part of our oversight of the Department of the Treasury’s (Treasury) State Small Business Credit Initiative (SSBCI), authorized by the Small Business Jobs Act of 2010 (the Act), we conducted audits of awards made to select States, Territories, and eligible Municipalities (hereinafter referred to as States) to support their capital access and small business credit programs. The purpose of these audits was to assess States’ compliance with SSBCI program requirements and prohibitions to identify any reckless or intentional misuse of funds. In this semiannual reporting period, we assessed State’s compliance at Rhode Island, Wisconsin, Oregon, New Hampshire, New York, and Oklahoma. It should be noted that the SSBCI program ended September 27, 2017, and with that, our audit oversight has ceased. While we have completed audits of select States and have included audit reports that have been issued this semiannual reporting period, we will include the remaining audit report(s) issued subsequent to this semiannual period in the semiannual report covering October 1, 2017 through March 31, 2018.

### **Rhode Island’s Use of Federal Funds for Its Betaspring Fund 100, LLC Venture Capital Program**

Our audit of SSBCI funds awarded to Rhode Island focused on the State’s compliance with respect to its \$2 million investment in its venture capital program, Betaspring Fund 100, LLC (Fund). The Fund was one of two Rhode Island venture capital programs approved to participate in SSBCI. We issued a separate report on Rhode Island’s other venture capital program, Slater Technology Fund, in October 2014.<sup>2</sup> We determined that the Fund’s investments in seventeen beneficiary companies constituted a misuse of \$803,644 in SSBCI funds because at the time the investments were made, there was no private capital at risk. The misuse was intentional because Betaspring Managers 100, LLC (Betaspring Managers) knew that 20 percent private capital for each investment was required, but made the seventeen investments anyway. We also found that Rhode Island did not seek and receive Treasury’s approval to invest all \$2 million of SSBCI funds in Startup Investments, LLC (Startup) instead of directly investing into the Fund as

---

<sup>2</sup> *State Small Business Credit Initiative: Rhode Island’s Use of Federal Funds for the Slater Technology Fund*, (OIG-SBLF-15-001; (October 31, 2014).

required by its *Allocation Agreement*. In addition, the Fund used some SSBCI Funds to pay Betaspring, LLC (Betaspring) for accelerator program services<sup>3</sup> rather than making direct cash investments in beneficiary companies, which was inconsistent with Rhode Island’s stated use of SSBCI Funds in its application, as referenced in the *Allocation Agreement*.

We recommended that the Deputy Assistant Secretary for Small Business, Community Development, and Housing (1) declare a specific event of default of its *Allocation Agreement* with Rhode Island and recoup the \$803,644 of SSBCI funds found to be intentionally misused; (2) determine whether Rhode Island is in default of its *Allocation Agreement* due to the unapproved investment in Startup; and (3) determine whether Rhode Island is in default of the its *Allocation Agreement* due to the Fund’s use of SSBCI funds to pay Betaspring for accelerator program services rather than making direct cash investments in beneficiary companies. In response to all three recommendations above, Treasury decided that it would not disburse the \$2 million that had been withheld from Rhode Island’s third disbursement (an amount which covered the funds invested in Betaspring) pending the results of our audit. We consider Treasury’s response to meet the intent of our recommendations. **(OIG-17-057, Questioned Costs \$803,644)**

### Wisconsin’s Use of Federal Funds for the Kegonsa Growth Fund, LP

Our audit focused on Wisconsin’s compliance with respect to the funds invested in its venture capital program, Kegonsa Growth Fund, LP (Kegonsa). We found that Kegonsa investments did not fully comply with all SSBCI venture capital program requirements and prohibitions. Specifically, Kegonsa’s investments in two beneficiary companies constituted a reckless misuse of \$261,000 of SSBCI funds because Kegonsa Capital Partners, LLC (KCP), the general partner of Kegonsa, had a financial interest in the beneficiary companies through prior investments using non-SSBCI funds, which violated Treasury’s SSBCI National Standards for Compliance and Oversight regarding conflicts of interest.

We recommended that the Deputy Assistant Secretary for Small Business, Community Development, and Housing declare a specific event of default of its *Allocation Agreement* with Wisconsin and recoup the \$261,000 of SSBCI funds found to be recklessly misused by Kegonsa. Treasury agreed to declare a

---

<sup>3</sup> The Fund’s accelerator program provided support in the form of space, intensive mentorship, coaching, networking support, and seed investment in participating companies.

specific event of default under Section 6.3 of Wisconsin’s *Allocation Agreement* and recoup \$261,000. We consider Treasury’s response to meet the intent of our recommendation. **(OIG-17-059, Questioned Costs \$261,000)**

### **Oregon’s Use of Federal Funds for Capital Access and Other Credit Support Programs**

Our audit focused on Oregon’s compliance with the SSBCI program requirements and prohibitions with respect to its approximately \$16.5 million SSBCI funds awarded. We found that Oregon generally complied with the SSBCI program requirements and prohibitions with respect to the State’s three small business development programs and administrative expenses. However, Oregon contributed \$6,750 in SSBCI funds to a reserve fund for a \$225,000 capital access program (CAP) loan that refinanced a line of credit made to the borrower by the same lender. This was a misuse of funds because the refinancing of existing debt is prohibited by the Act and *SSBCI Policy Guidelines*. Although the use of SSBCI funds for the loan in question was prohibited, we did not find that the misuse was “intentional” or “reckless,” because Oregon obtained a lender assurance affirming the loan was not a refinancing of a loan previously made to that borrower by the financial institution lender, which is required by *SSBCI Policy Guidelines*. Additionally, upon learning of the use of loan proceeds to refinance an existing debt, the State agreed that it was prohibited and told us they would request approval from Treasury to un-enroll the loan from the CAP portfolio and replenish its SSBCI account in the amount of \$6,750.

We recommended that the Deputy Assistant Secretary of Small Business, Community Development, and Housing verify that \$6,750 in SSBCI funds has been withdrawn from the prohibited loan and that the SSBCI account is reimbursed for the same amount. Additionally, we requested that the State amend its 2013 Annual Report and the appropriate Quarterly Report to reflect the un-enrolled loan. Treasury agreed to work with Oregon to address our recommendations, which meets our intent. **(OIG-17-049, Questioned Costs \$6,750)**

### **New Hampshire’s Use of Federal Funds for the Borealis Granite Fund, LP**

Our audit focused on New Hampshire’s compliance with respect to funds invested in its venture capital program, Venture Capital Fund (Fund). We found

that the Fund’s venture capital fund, Borealis Granite Fund (Borealis), which invested \$1.3 million of SSBCI funds between January 2013 and June 2014, generally complied with the SSBCI program requirements and prohibitions governing SSBCI venture capital programs. As such, we made no recommendations. **(OIG-17-058)**

### **New York’s Use of Federal Funds for Six of Innovate Fund’s Venture Capital Funds**

Our audit focused on the New York’s compliance with respect to funds invested in its venture capital program, Innovate NY Fund, LP (Innovate Fund). We found that 6 of Innovate Fund’s venture capital funds, which invested approximately \$18.1 million of SSBCI funds between December 2012 and December 2014, generally complied with SSBCI program requirements and prohibitions. As such, we made no recommendations. We reported on Innovate Fund’s venture capital fund, Canrock Innovate NY Fund LLP separately.<sup>4</sup> **(OIG-17-056)**

### **Oklahoma’s Use of Federal Funds for Its Venture Capital Programs**

Our audit focused on Oklahoma’s compliance with SSBCI requirements and prohibitions with respect to approximately \$10.8 million used for its venture capital programs as of December 2015. We found that Oklahoma generally complied with SSBCI program requirements and prohibitions governing its four venture capital programs. As such, we made no recommendations. **(OIG-17-048)**

---

<sup>4</sup> *State Small Business Credit Initiative: New York’s Use of Federal Funds for Other Credit Support Programs* (OIG-17-035; issued January 24, 2017).

## Cyber/Information Technology

During this semiannual period, we performed a cyber/information technology audit of Treasury’s information security program and practices and a survey of Treasury’s information sharing policies and procedures.

### 2017 Audit of Treasury’s Compliance With the Federal Information Security Modernization Act for Its Intelligence Systems

As part of our ongoing oversight of Treasury’s compliance with the Federal Information Security Modernization Act of 2014 (FISMA), we are required to annually evaluate Treasury’s information security program and practices. In our 2017 report, we recounted unresolved issues from the prior year and identified new matters that need improvement. Due to the sensitive nature of Treasury’s intelligence systems, this report is classified. **(OIG-17-052, Classified)**

### Cybersecurity Survey

We conducted a survey of Treasury’s activities to implement the information sharing provisions under Title I, the Cyber Information Sharing Act (CISA) of the Cybersecurity Act of 2015. We conducted this survey in support of the first joint biennial report required by Section 107 of CISA, which requires the Inspectors General of the “appropriate Federal entities,”<sup>5</sup> in consultation with the Intelligence Community Inspector General (IC IG) and the Council of Inspectors General on Financial Oversight (CIGFO), to jointly report to Congress on the actions taken by the respective agencies over the recent 2-year period to carry out the requirements of CISA. The first report is due in December 2017 and biennially thereafter.

The objective of our survey was to answer the common question set developed by the IC IG for the first joint report. The scope of our work included all Treasury information sharing policies and procedures as well as activities covering the most recent 2-year period (calendar years 2015 and 2016). We did not find any issues or matters of concern in Treasury’s responses to the survey that are in need of immediate attention and would require our office to initiate a more in-depth audit or evaluation. **(OIG-CA-17-020)**

---

<sup>5</sup> The Office of the Director of National Intelligence and the departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury.

## DATA Act

Treasury and Office of Management and Budget (OMB) are leading the Government-wide implementation of the Digital Accountability and Transparency Act of 2014 (DATA Act). As part of our ongoing oversight of the DATA Act implementation, we are conducting a series of audits reviewing Treasury's efforts to meet its responsibilities under the Act.

### **ARC Is Making Progress in Meeting DATA Act Reporting Requirements Despite Challenges**

We performed an audit to gain an understanding of the processes, systems, and controls that the Bureau of the Fiscal Service's (Fiscal Service) Administrative Resource Center (ARC), a Federal shared service provider, implemented or planned to implement as of September 30, 2016, to report financial and payment information in accordance with the requirements of the DATA Act.

We found that as of September 30, 2016, ARC had made progress toward compliance with the DATA Act. It had designed a comprehensive implementation plan that conforms to the Government-wide technical and informational guidance issued by Treasury's Program Management Office (PMO) and OMB. If fully executed, we anticipated that ARC would meet the DATA Act reporting requirements by the established May 2017 deadline. Specifically, ARC's DATA Act implementation plan and project management documents (1) identified its senior accountable officials; (2) estimated resource requirements; (3) proposed an implementation timeline; and (4) identified foreseeable challenges that it may encounter while implementing the DATA Act on behalf of its financial management customer agencies, as well as potential resolutions.

Fiscal Service management acknowledged the value and unique opportunity this audit provided in assessing their efforts to comply with the DATA Act and identifying further areas of improvement. Fiscal Service also expressed confidence that it expected to meet the DATA Act reporting requirements by the May 2017 deadline and provided an update on how some of the challenges we identified had been addressed since the end of our fieldwork.

**Update:** ARC, through Treasury, made its first required DATA Act submission in May 2017. As of the end of this reporting period, we were conducting the first

in a series of required reviews of Treasury’s data submissions and of its use of data standards. We will issue our report in November 2017. **(OIG-17-039)**

### **Council Is Making Progress in Meeting DATA Act Reporting Requirements Despite Challenges**

We also performed an audit of the Gulf Coast Ecosystem Restoration Council’s (Council) readiness to implement the requirements of the DATA Act. As of April 6, 2017, the Council had made progress toward compliance with the DATA Act by establishing a comprehensive implementation plan and project planning documentation that conform to the technical and informational guidance issued by Treasury’s PMO and OMB. Specifically, the Council’s DATA Act implementation plan and project planning documentation (1) identified its Senior Accountable Official; (2) estimated resource requirements; (3) proposed an implementation timeline; and (4) identified foreseeable challenges that it may encounter while implementing the DATA Act, as well as potential resolutions.

The Council also identified risks and challenges associated with its reliance on manual processes and limited staff, and delays in additional guidance from Treasury’s PMO and OMB. The Council recognized that these risks and challenges will need to be addressed as it continues to refine its DATA Act implementation. However, the Council did not believe that these risks and challenges would affect its ability to meet the established May 2017 deadline for submitting data. As such, the Council had plans to automate more data transfer and reconciliation processes, and continue to assess its staff requirements relative to the growth of its operations.

**Update:** The Council made its first required DATA Act submission in May 2017. As of the end of this reporting period, we were conducting the first in a series of required reviews of the Council’s data submissions and of its use of data standards. We will issue our report in November 2017. **(OIG-17-045)**

### **FAEC DATA Act Working Group Frequently Asked Questions**

Our office developed a Frequently Asked Questions (FAQ) document on behalf of the Federal Audit Executive Council (FAEC) DATA Act Working Group. The FAQ document includes responses to questions we received regarding the Inspectors General DATA Act required reviews. This document will be updated with additional FAQs as needed. **(OIG-CA-17-019)**

## RESTORE Act

As part of our ongoing oversight of Resources and Ecosystems Sustainability, Tourist Opportunities, and Revived Economies of the Gulf Coast States Act of 2012 (RESTORE Act) programs, we are assessing the Gulf Coast Ecosystem Restoration Council's (Council) and Treasury's activities funded by the act.

### Gulf County's Policies and Procedures Did Not Reflect All Uniform Guidance Requirements

An independent certified public accounting firm, McConnell & Jones LLP (McConnell & Jones), under a contract monitored by our office, assessed whether Gulf County, Florida (the County), used awarded funds in compliance with applicable Federal statutes, regulations, and its award agreement with Treasury.

McConnell & Jones reported that it did not identify any areas of noncompliance in the use of the County's Multiyear Implementation Plan (MYIP) Planning Assistance award. However, the County's policies and procedures did not reflect all "Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards," 2 CFR Part 200 (Uniform Guidance) requirements. Accordingly, McConnell & Jones recommended that Treasury considers the County's need to further develop and strengthen its policies and procedures to fully document the Uniform Guidance as part of Treasury's oversight and administration of the County's MYIP Planning Assistance award, as well as risk assessments required by the Uniform Guidance for future awards.

Treasury management concurred with McConnell & Jones' findings and noted that they will consider the County's need to further develop and strengthen its policies and procedures to document the Uniform Guidance, as applicable, as part of Treasury's oversight and administration of all future County awards. McConnell & Jones determined that Treasury's response met the intention of its recommendation. **(OIG-17-046)**

## American Recovery and Reinvestment Act

The American Recovery and Reinvestment Act of 2009 (Recovery Act) authorized Treasury's Payments to States for Low-Income Housing Projects in lieu of Low-Income Housing Tax Credits (1602 Program). As part of our ongoing oversight of the 1602 Program, we conducted audits of awards made to selected State housing credit agencies. The objective of these audits was to assess whether the agencies awarded funds under Treasury's 1602 Program complied with the program's overall requirements and the "Grantee Terms and Conditions" (together referred to as 1602 Program requirements). In this semiannual reporting period, we provided our assessment of 1602 Program awards made to Arkansas and Rhode Island.

### Arkansas Development Finance Authority's Payment Under the 1602 Program

We found that the Arkansas Development Finance Authority (ADFA) did not fully comply with Treasury's 1602 Program requirements. Although ADFA substantially met the eligibility and compliance requirements set forth in both Section 42 of the Internal Revenue Code (IRC) and Section 1602 of the Recovery Act for receiving its approximately \$92.9 million 1602 Program award, it did not meet all subaward requirements related to one low-income housing project. Specifically, ADFA did not complete the final financial feasibility underwriting for one project, Rock Creek of Conway (Rock Creek), at the time it was placed in service. Furthermore, although ADFA established compliance monitoring oversight, it did not perform a timely on-site inspection for Rock Creek within the second full calendar year after being placed in service. Accordingly, we recommended that Treasury ensure ADFA completes the final financial feasibility underwriting for Rock Creek, and that going forward, ADFA performs timely future on-site inspections of all 1602 Program funded projects.

ADFA performed asset management for monitoring the long-term viability of 1602 Program funded projects. At the time of our review, there were no matters impacting the long-term viability of projects. ADFA also complied with 1602 Program reporting requirements. That said, we emphasized the need for continued diligence on the part of ADFA to ensure compliance with the terms and conditions over the remaining 15-year compliance period.

In response to our recommendations above, Treasury stated it will monitor ADFA's efforts to complete the financial feasibility underwriting. Treasury also

stated that it will continue to require ADFA to submit annual compliance reports for all funded projects and will monitor ADFA's compliance with program requirements to include on-site inspections. Treasury's response meets the intent of our recommendations. **(OIG-17-041)**

### Rhode Island Housing's Payment Under the 1602 Program

We found that Rhode Island Housing (RIH) generally complied with Treasury's 1602 Program requirements which capture the eligibility and compliance requirements set forth in Section 42 of the IRC and Section 1602 of the Recovery Act. Specifically, RIH met all applicable requirements for receiving its approximately \$36.9 million 1602 Program award, as well as requirements for subawarding funds to 6 eligible low-income housing projects.

RIH also established a process for monitoring the long-term viability of projects. At the time of our review, there were no matters impacting the long-term viability of 1602 Program funded projects and their compliance with Section 42 of the IRC. Furthermore, RIH complied with 1602 Program reporting requirements in submitting quarterly project performance reports and annual certification reports to Treasury. Nonetheless, we do want to emphasize the need for continued diligence on the part of Treasury and RIH to ensure compliance with the 1602 Program requirements over the remaining 15-year compliance period.

We made no recommendations in this report. **(OIG-17-042)**

### Financial Management

As required by the Improper Payments Elimination and Recovery Act of 2010 (IPERA), we reported on Treasury's and the Gulf Coast Ecosystem Restoration Council's (Council) overall compliance with IPERA for fiscal year 2016. We also assessed compliance with additional improper payment reporting requirements set forth in Executive Order (EO) 13520, "Reducing Improper Payments and Eliminating Waste in Federal Programs," and the Improper Payment Elimination and Recovery Improvement Act of 2012 (IPERIA).

## Treasury Was Not in Compliance With IPERA for Fiscal Year 2016

For the sixth consecutive year, we concluded that Treasury was not in compliance with IPERA due to the Internal Revenue Service's (IRS) Earned Income Tax Credit (EITC) program deficiency reported by the Treasury Inspector General for Tax Administration (TIGTA). Specifically, IRS has not reported an overall improper payment rate of less than 10 percent for EITC as required by IPERA. We also determined that Treasury did not fully comply with OMB's reporting requirements for payment recapture audits. In addition, our report included TIGTA's determination that Treasury's revised annual risk assessment process still does not provide a valid assessment of risks of refundable tax credit improper payments related to the Additional Child Tax Credit and American Opportunity Tax Credit. In addition, TIGTA determined that the assessment of risk of the Premium Tax Credit (PTC) may not be reliable. We determined that Treasury was in compliance with all other IPERA, EO 13520, and IPERIA improper payment reporting requirements.

We recommended that Treasury ensure (1) its components submit accurate and complete payment recapture audit information for inclusion in the Annual Financial Report; and (2) it strengthens its review and oversight of the data reported by components on payment recapture audits to accurately reflect the results of recapture audits. Treasury management's agreement and actions, both taken and planned, to address the improper payments reporting deficiencies identified in our report meet the intent of our recommendations.

TIGTA recommended that the IRS ensure that the methodology used to conduct the Annual Improper Payment Risk Assessment for refundable tax credits, including the PTC, include a quantitative assessment of IRS compliance data. TIGTA also recommended that the IRS work with the Department of Health and Human Services Centers for Medicare and Medicaid Services to develop a collaborative strategy to assess the comprehensive risk of improper PTC payments. IRS management did not agree with TIGTA's recommendations. However, in response to the summarized report, Treasury officials noted that they will work in conjunction with IRS management to re-evaluate and continue refining, as necessary, the IRS's methodology for properly conducting and assessing improper payment risks associated with refundable tax credits. **(OIG-17-043)**

## **Gulf Coast Ecosystem Restoration Council Did Not Administer Programs and Activities Susceptible to Significant Improper Payments**

Based on the results of the Council’s fiscal year 2016 financial statement audit, we determined that the Council did not have programs and activities susceptible to significant improper payments in fiscal year 2016. That is, total program and activity expenditures were less than the threshold of reporting requirements for “significant improper payments” specified in Appendix C to OMB Circular No. A-123, “Requirements for Effective Estimation and Remediation of Improper Payments” (OMB M-15-02).<sup>6</sup> Additionally, the Council did not have any OMB designated high priority programs or other risk susceptible programs. Furthermore, although expenditures were greater than \$1 million, the Council justified that conducting a payment recapture audit program for its programs and activities was not cost effective. Accordingly, the Council was not required to perform, and did not perform, payment recapture audits during fiscal year 2016. We did, however, determine that the Council was compliant with all of the applicable requirements set forth in PART II A. 3) of OMB M-15-02. **(OIG-CA-17-018)**

## **Attestation Engagements**

We completed three reports described below in support of the audit of Treasury’s fiscal year 2017 consolidated financial statements and the financial statement audits of certain other Federal agencies.

### **Reports on the Processing of Transactions by Fiscal Service**

KPMG LLP (KPMG), under a contract monitored by our office, examined the accounting and procurement processing and general computer controls related to financial management services provided to various Federal agencies by Fiscal Service’s ARC for the period beginning July 1, 2016, and ending June 30, 2017. KPMG found, in all material respects, that the controls were fairly presented in the description of controls for these activities and suitably

---

<sup>6</sup> "Significant improper payments" are defined as gross annual improper payments (i.e., the total amount of overpayments and underpayments) in the program exceeding (1) both 1.5 percent of program outlays and \$10 million of all program or activity payments made during the fiscal year reported or (2) \$100 million (regardless of the improper payment percentage of total program outlays).

designed. The service auditor also found that controls tested operated effectively throughout the period. **(OIG-17-050)**

KPMG, under a contract with our office, examined general computer and investment/redemption processing controls used for various Federal agencies’ transactions by Fiscal Service’s Federal Investments and Borrowings Branch, and general computer and trust funds management processing controls used for various Federal and State agencies’ transactions by the Fiscal Service’s Funds Management Branch for the period beginning August 1, 2016, and ending July 31, 2017. KPMG found, in all material respects, that the controls were fairly presented in the description of controls for these activities and suitably designed. The service auditor also found that controls tested operated effectively throughout the period. **(OIG-17-053, OIG-17-054)**

**Treasury Financial Audits**

The following instances of noncompliance with the Federal Financial Management Improvement Act of 1996 were reported in connection with the audit of Treasury’s fiscal year 2016 consolidated financial statements.

Condition	Type of noncompliance
IRS continues to have deficiencies in its financial management systems. Specifically, IRS did not consistently design, implement, and operate information system controls and security programs over its financial systems in accordance with the Federal financial management system requirements. (first reported in fiscal year 1997)	Federal financial management systems requirements
IRS has a material weakness that affected Treasury’s ability to prepare its financial statements in accordance with the Federal accounting standards. Specifically, IRS subsidiary records and supporting financial systems were unable to support the Federal taxes receivable amount on the consolidated balance sheet, and the compliance assessments and write-offs in the required supplementary information disclosures, in accordance with the Federal accounting standards. (first reported in fiscal year 1997)	Federal accounting standards

The status of these instances of noncompliance, including progress in implementing remediation plans, will be evaluated as part of the audit of Treasury’s fiscal year 2017 consolidated financial statements.

## Other Audits of Treasury Programs and Operations

### TTB Appropriately Designates American Viticultural Areas, But Improvements Would Strengthen the Program

We audited the Alcohol and Tobacco Tax and Trade Bureau's (TTB) existing controls over its program to designate American Viticultural Areas (AVA) and to determine whether decisions to designate AVAs were made consistently and in accordance with established laws, Federal regulations, and guidance.

We concluded that TTB consistently designated AVAs in accordance with law, Federal regulations, and TTB guidance. However, we found that TTB had not established formal written standard operating procedures documenting how the functions necessary for processing AVA petitions were performed; and could improve the review and transparency of the AVA designation process and program by providing the public a U.S. Geological Survey (USGS) map of the proposed, as well as the approved boundary of an AVA as a digital document.

We recommended that TTB (1) develop written standard operating procedures for the AVA program that properly document the fundamental steps taken during the AVA designation process and (2) examine the capability to provide USGS maps as digital documents to enhance and improve transparency of the AVA program both during and after the rulemaking process, including consideration of the cost and benefits for doing this. TTB concurred with our recommendations and its actions, both taken and planned, meet the intent of our recommendations. **(OIG-17-038)**

### TTB Has Strengthened Controls Over Conference, Travel, and Employee Award Administration

In recent years, spending on Federal agency conferences, travel, and employee awards has received increased scrutiny from Inspectors General, OMB, and Congress. We performed an audit of TTB's administration of those three areas and found that TTB planned and executed conferences, conducted travel, and distributed employee awards in compliance with applicable Federal laws, regulations, executive orders, and Treasury policies. However, we identified three activities that management needed to strengthen internal controls over: (1) TTB incurred \$14,000 in extra costs for a conference because it did not pay for lodging using a centrally billed account (CBA); (2) TTB's supervisors approved their own travel authorizations; and (3) TTB's employee award policy was not updated to reflect the Treasury Directive requiring

Departmental Oversight for executive misconduct when awarding monetary recognition.

Subsequent to the completion of our fieldwork, TTB management strengthened internal controls related to those activities. TTB management provided us with evidence of using a CBA for two conferences held in fiscal years 2013 and 2014, respectively, to confirm their new practice of using a CBA to pay for conferences that cost more than \$40,000, and updated its travel policy to require the use of a CBA for conferences exceeding \$40,000. TTB management also updated its travel policy to prohibit self-travel authorizations. In addition, TTB management updated its employee award policy to address consideration of non-executive misconduct and monetary recognition in February 2017. But because consideration of executive misconduct for monetary recognition for executives was not addressed in the policy, we recommended that the TTB Administrator revise TTB's award policy to incorporate the Treasury Directive regarding executive misconduct when awarding monetary recognition.

TTB management stated that a separate TTB-specific policy to address the issue would increase administrative costs without offsetting benefits because the bureau currently adheres to and meets the intent of this directive, as it follows all relevant Treasury directives and guidance throughout this award process to support the Department's administration of executive awards. We accepted TTB's commitment to adhere to relevant Treasury directives and guidance as meeting the intent of our recommendation. **(OIG-17-040)**

### **Federal Agencies Are Generally Satisfied With TFFC's Collaboration Efforts, but Enhancements Can Be Made**

We reviewed the Office of Terrorist Financing and Financial Crimes' (TFFC) interagency collaboration efforts with Federal agencies to identify and address threats to the international financial system from money laundering and other forms of illicit finance. TFFC serves as the policy development and outreach office for Treasury's Office of Terrorism and Financial Intelligence (TFI). As part of this responsibility, TFFC leads or assists in leading several task forces or working groups. In 2009, the Government Accountability Office (GAO) reported that collaborating with interagency partners is important to TFI's ability to perform effectively and made two recommendations for TFI in its oversight of TFFC which were to (1) establish compatible policies, procedures, and other means to operate across agency

boundaries; and (2) develop a mechanism for monitoring, evaluating, and reporting on the results of collaborative efforts.<sup>7</sup>

We found that TFFC had not addressed GAO's recommendations and did not have policies and procedures for its daily operations. We also found that most Federal agency officials we interviewed voiced satisfaction with TFFC's collaboration efforts overall and expressed a belief that TFFC took their concerns and comments into consideration when developing positions. However, some Federal agency officials believed there were opportunities for enhancing collaboration by improving communication through feedback, holding intersessional meetings, and widening inclusion in bilateral meetings with TFFC and foreign countries during the Financial Action Task Force (FATF) Plenary.<sup>8</sup>

We recommended that TFFC (1) develop policies and procedures to ensure continuity and consistency in collaboration efforts with interagency task forces and workgroups; (2) develop and implement a mechanism to monitor, evaluate, and report on the effectiveness of TFFC's interagency collaboration; (3) develop meaningful performance measures specific to TFFC collaboration; and (4) address areas of concern expressed by Federal agencies regarding TFFC's collaboration that includes feedback, intersessional meetings, and invitations to participate in bilateral meetings with foreign countries during the FATF Plenary. TFFC concurred with our recommendations and its actions, both taken and planned, meet the intent of our recommendations.

**(OIG-17-044)**

### **FinCEN's 314 Information Sharing Programs Are Useful but Need FinCEN's Attention**

Section 314 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) created two programs to facilitate the sharing of information about financial crimes between Government agencies and financial institutions. We performed an audit of the programs to determine the extent to which information sharing is occurring among the Government and financial institutions.

---

<sup>7</sup> GAO, *Combating Illicit Financing: Treasury's Office of Terrorism and Financial Intelligence Could Manage More Effectively to Achieve Its Mission*, GAO-09-794 (September 24, 2009)

<sup>8</sup> FATF is the international body that develops and implements multilateral standards relating to anti-money laundering and counterterrorist financing. FATF Plenaries occur three times a year during the months of February, June, and October. FATF Plenary meetings are open to delegations from FATF members, observer jurisdictions, and observer organizations and are not open to the public.

We found that a majority of law enforcement agency (LEA) users we interviewed believed the Financial Crimes Enforcement Network's (FinCEN) Section 314(a) program was very helpful during investigations and they were satisfied with the way FinCEN operated the program. However, some users suggested that FinCEN could make enhancements to the program that would provide more information to assist in investigations, with subpoena preparation, or with both of these activities. FinCEN exempted financial institutions from providing all information set forth by its regulations. As a result, the information provided by these financial institutions did not always provide consistent information for LEAs. We also found that feedback requested by FinCEN from LEA representatives regarding the Section 314(a) program was limited, in part because some investigations take years to complete. FinCEN's user survey needed improvement as responses may be difficult for LEAs to quantify since multiple sources of information can aid in their investigations. As another matter, we noted that financial institutions submitted duplicate responses to Section 314(a) inquiries despite FinCEN's instructions prohibiting them. FinCEN revised the Section 314(a) module in a subsequent systems project, which officials stated would prevent duplicate entries. In February 2016, FinCEN issued a notice in the Federal Register for comment to renew the Section 314(a) program without change.

Regarding FinCEN's voluntary Section 314(b) program, Federal bank regulatory agency officials we interviewed stated that financial institutions were concerned about participating in the program even after FinCEN issued guidance (including an explanation of safe harbor provisions) for the program in June 2009.

We recommended that FinCEN (1) incorporate the user recommendations for enhancements in addition to the public comments received when evaluating its proposed renewal of the Section 314(a) program; (2) identify the impact on LEAs of exempting information from the responses to their 314(a) requests and determine if FinCEN should continue to exempt information set forth in its regulations; (3) ensure the Section 314(a) survey questions are clarified to provide for consistent interpretation and responses about the program, and allow sufficient time for feedback in order to gain a more complete understanding of how Section 314(a) information benefits law enforcement cases; and (4) identify and address areas of concern regarding the Section 314(b) program and include these in guidance and outreach to encourage greater participation in the program. FinCEN management agreed with our recommendations and its actions, both taken and planned, meet the intent of our recommendations. **(OIG-17-055)**

## Independent Examination Report of WaveFront Technology Inc.'s Accounting System

We performed an examination of WaveFront Technology, Inc.'s accounting system in response to an April 27, 2017, request from Bureau of Engraving and Printing (BEP) to conduct a pre-award accounting system review. Our examination results, which were reported to BEP, will be used when BEP reviews WaveFront Technology, Inc.'s proposal(s) in response to BEP's Solicitation Number BEP-RFP-17-0488 and anticipated resultant contract task orders. Due to the proprietary nature of contractor accounting systems, this report was designated Sensitive But Unclassified. **(OIG-17-051, Sensitive But Unclassified)**

## **Office of Investigations – Significant Investigations**

### **False Claims Act Violation Results in a \$29.5 Million Settlement**

Our investigation, initiated based on a referral from the Department of the Treasury (Treasury) Departmental Offices, involved allegations that a solar energy company violated the False Claims Act by submitting thousands of inflated applications on behalf of itself and affiliated investment funds to the Treasury’s American Recovery and Reinvestment Act (Recovery Act) 1603 program—Payments for Specified Energy Property in Lieu of Tax Credits (1603 Program). The applications falsely overstated the cost bases of solar energy properties and resulted in Treasury issuing inflated 1603 payments to the solar energy company. A multi-level agreement was reached between the Department of Justice, Treasury, and the solar energy company, wherein the company, agreed to a settlement of \$29.5 million. As part of the settlement, the company agreed to dismiss a lawsuit that it had filed against Treasury in the Court of Federal Claims. The company and its affiliates also agreed to release all pending and future claims for additional payments under the 1603 Program.

### **Money Services Business Owner Pleads Guilty to Failing to Develop, Implement, and Maintain an Anti-Money Laundering Program**

Our investigation of a check cashing business in Dallas, Texas, determined that the owner of the money services business (MSB) facilitated in the negotiation of nearly 3,500 fraudulently obtained Treasury checks totaling \$16.6 million. The subject failed to establish an anti-money laundering program required by a business working as a money transmitter. The subject pled guilty to Failure to Develop, Implement, and Maintain an Anti-Money Laundering Program in the Northern District of Texas, Dallas Division. Sentencing is pending.

### **Subjects Arrested for Submitting Fraudulent Recovery Act Applications**

Our joint investigation with the Internal Revenue Service Criminal Investigations (IRS-CI) determined that two subjects conspired to submit fraudulent applications to Treasury on behalf of four Massachusetts companies for energy grants under the 1603 Program. The subjects, who claimed that the four companies had acquired, placed into service, or started construction on three biofuel gasification systems and one wind farm project sought to be reimbursed for more than \$50 million based on the costs of the systems, and received payments totaling more than \$8 million. The subjects submitted fraudulent documentation to a Massachusetts-based attorney who submitted the applications to Treasury on their behalf. The subjects were indicted in

the U.S. District Court, District of Massachusetts, and subsequently arrested for Wire Fraud and Conspiracy to Defraud the Government with Respect to Claims. Judicial action is pending.

### **Subject Sentenced for Stolen Treasury Checks and Email Compromise**

Our investigation of a stolen Treasury check for \$28,000 revealed a criminal scam orchestrated by a subject that involved a business and personal email compromise scheme prompting wire transfers amounting to over \$227,000 from victims. Additionally, the subject fraudulently obtained and negotiated business checks totaling over \$52,000, and falsely filed Federal income tax returns. The subject was charged with Mail Fraud, Bank Fraud, and Aggravated Identification Theft and sentenced to 168 months in prison, 60 months of probation, and ordered to pay \$722,000 in restitution for fraud attempts exceeding \$32 million that affected 3,000 victims. Upon the subject's release from prison, an immigration deportation review will determine the subject's continued residency in the United States.

### **Subjects Arrested for Structuring Over \$4.6 Million through Financial Institutions**

Our joint investigation with IRS-CI, the Social Security Administration (SSA) Office of Inspector General (OIG), the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG), the U.S. Secret Service (USSS), and State and local police determined that two subjects, who have no legitimate source of income, structured over \$4.6 million through financial institutions within one year. Additionally, both subjects fraudulently obtained Social Security child auxiliary benefits and made false statements. The subjects were indicted and subsequently arrested in the Middle District of Florida for Structuring, False Statements, and Theft of Public Money. Trial is pending.

### **Hospital Employee Arrested for Embezzlement**

Our joint investigation with USSS involved allegations of bank fraud by an employee of a hospital in High Point, North Carolina. The subject oversaw the hospital's financial programs, including accounts payable and payroll. The subject embezzled over \$3.5 million of hospital funds. The funds were directly traced to the subject's personal use and the purchase of at least 15 motor vehicles. Federal search and seizure warrants were obtained for the subject's residence and the 15 vehicles were seized to recover assets. Two vehicles were located in Germany and Romania, where foreign law enforcement officials are assisting in the recovery. To date, this investigation has

recovered \$1.5 million in assets. The subject was arrested on State Embezzlement charges pending Federal indictment in North Carolina. Judicial action is pending.

### **Subjects Arrested for Stealing and Negotiating Altered Treasury Checks**

Our joint investigation with the U.S. Postal Inspection Service (USPIS), SSA OIG, and the U.S. Postal Service (USPS) OIG determined that over 580 Treasury checks were stolen, altered, and negotiated around the Chicago, Illinois area by an organized criminal group. The value of the stolen Treasury checks was over \$605,000, but the altered value totaled over \$2.6 million. A USPS mail carrier was identified and admitted to stealing the checks. The mail carrier identified a second subject. Both subjects were arrested and charged in U.S. District Court, Northern Illinois with Dealing in Counterfeit Obligations. A third subject was arrested in the same venue and charged with Bank Fraud. Judicial action is pending for these subjects and additional arrests are anticipated.

### **Subjects Sentenced in Stolen Identity Refund Fraud**

Our joint investigation with IRS-CI determined that a subject obtained stolen personal identifying information and used it to file fraudulent Federal income tax returns. Upon receipt of the refunds, the subject recruited a second subject who deposited the refunds into several bank accounts. Proceeds were shared between both subjects. The first subject pled guilty to Conspiracy to Defraud the Government and was sentenced in the U.S. District Court, District of Columbia. The subject was sentenced to 6 months in prison, 6 months home detention, 36 months of probation, and ordered to pay \$613,000 in restitution. The second subject pled guilty to Conspiracy to Defraud the Government and was sentenced to 60 months of probation, and ordered to pay \$351,000 in restitution to Treasury.

### **Subject Sentenced After Guilty Plea to Bank Fraud, Aggravated Identity Theft, and Money Laundering**

Our joint investigation with IRS-CI, USPIS, and the U.S. Attorney's Office, Western District of Missouri, determined that a subject stole Treasury and other checks from U.S. Postal mail. The subject used counterfeit identification to negotiate the checks at financial institutions, and laundered the illegal proceeds, \$460,000, through a gold coin dealer in California. The subject was indicted in U.S. District Court, Western District of Missouri for Bank Fraud, Aggravated Identity Theft, and Money Laundering, pled guilty, and was sentenced to 111 months in prison and ordered to pay \$248,000 in restitution.

### **Subject Sentenced for Wire Fraud and Money Laundering**

Our joint investigation with the Durham County, North Carolina's Sheriff's Office identified a subject who laundered over \$358,000 from his employer, impacting Office of the Comptroller of the Currency (OCC)-regulated financial institutions. Over 2 years, the subject approved numerous payments for service to a company in which the subject held a personal interest. The subject never reported this personal interest to the employer and no services were rendered. The subject was indicted and pled guilty in U.S. District Court, Middle District of North Carolina to Wire Fraud and Money Laundering. The subject was sentenced to 24 months in prison, 36 months of probation, and ordered to pay \$358,000 in restitution.

### **Civilian Contractor Pleads Guilty to Stealing Government Employee Payroll Deposits and Thrift Savings Plan Retirement Deposits**

Our joint investigation with the Department of Veterans Affairs OIG discovered a civilian contractor re-directed Government employee payroll deposits to multiple bank accounts controlled by the subject with a loss to the Government of \$270,000. The subject also transferred Thrift Savings Plan payroll deposits into personally owned bank accounts. The subject pled guilty to Theft of Public Money in the District of Maryland, Baltimore. Sentencing is pending.

### **Subject Indicted for Theft Scheme**

Our joint investigation with the New York Attorney General's Office revealed a subject who solicited unwitting victims into believing his company could arrange for tens of millions of dollars in loans provided the victims pay "fees" upfront to collateralize the loans. Instead of using the deposits to secure the promised loans, the subject diverted the money for his own personal use, including \$71,000 in cash withdrawals and transfers to his personal bank account, \$47,000 to pay for his Wall Street apartment, and an additional \$26,000 for assorted personal items. The subject stole a total of \$800,000 and was indicted by the State of New York for theft. The subject pled guilty and was sentenced to 12 months in prison and ordered to pay restitution of \$800,000. If restitution is not paid, the subject will serve from 36 to 108 months in prison.

### **Subjects Arrested for Money Laundering in Illegal Gambling Operation**

Our joint investigation with the Dallas, Texas, Police Department determined four subjects were involved in an illegal gambling operation and laundered \$898,000 over a period of 6 months through financial institutions regulated by Treasury. Arrest warrants were issued by the State of Texas and the subjects were arrested for Organized Criminal Activity and Laundering the Proceeds of Illegal Gambling. Judicial action is pending.

### **Subject Pleads Guilty to Theft of Government Property**

Our joint investigation with the Department of Veterans Affairs OIG determined a private citizen residing in Lexa, Arkansas, improperly received \$118,000 in veteran's benefits paid by Treasury. The subject maintained a joint bank account with the benefit recipient, where benefit payments were deposited, and continued to receive payments after the death of the recipient. In the U.S. District Court Eastern District of Arkansas, the subject pled guilty to Theft of Government Property. Sentencing is pending.

### **Former Mint Employee and Union Secretary-Treasurer Sentenced After Embezzling Union Funds**

Our investigation determined that a former United States Mint (Mint) employee, who served as a union secretary-treasurer and had both check writing authority and bookkeeping responsibility, wrote numerous checks to herself using union funds. The subject embezzled the funds by creating false journal entries in a ledger and forging signatures on checks. The subject was charged in U.S. District Court, District of Colorado and subsequently pled guilty to Wire Fraud. The subject was sentenced to 10 months home detention, 60 months of probation, 200 hours of community service, and ordered to pay \$71,000 in restitution.

### **Subject Indicted for Aggravated Identity Theft and Bank Fraud**

Our investigation determined a subject stole identities of multiple citizens within North Carolina. The stolen identities were used to cash over \$19,000 worth of stolen and forged checks from multiple OCC-regulated financial institutions. The subject was indicted and arrested within the Middle District of North Carolina for Federal Bank Fraud and Aggravated Identity Theft. Sentencing is pending.

### **Subjects Arrested for Engaging in Organized Criminal Activity by Laundering Money, Stealing Personally Identifiable Information, and Theft**

Our joint investigation with the Texas Department of Public Safety identified an organized criminal ring conducting identity theft, money laundering, theft of funds, fraudulent credit card usage, and theft of fuel in the Houston, Texas area impacting financial institutions and MSBs regulated by Treasury. The investigation resulted in State warrants issued to 12 subjects in connection with charges of Engaging in Organized Criminal Activity. Seven (7) of the 12 subjects were located and arrested by the Smith County Sheriff's Department, near Tyler, Texas. Judicial action is pending for the seven subjects. Investigative efforts continue to locate and arrest the remaining fugitives, and identify additional co-conspirators.

### **Subject Uses Stolen Identities to Cash Stolen Treasury Checks**

Our joint investigation with the Jacksonville, Florida, Sheriff's Office determined that the subject, a member of an organized criminal enterprise, used stolen identities to open accounts at OCC-regulated banks to cash fraudulently obtained Treasury checks. The subject was arrested in Jacksonville, Florida, and charged with Uttering and Possession of multiple stolen or fraudulently obtained Treasury checks in the Fourth Judicial Circuit of Florida. Additional judicial action is pending.

### **Subject Indicted for Preparing and Filing False Tax Returns**

Our joint investigation with IRS-CI and USPIIS determined that subjects prepared and submitted over 1,300 fraudulent Federal income tax returns for undocumented workers and resident foreign nationals. Subjects used other individual's wages and falsely reported a high number of dependents to produce an excessive tax refund. One subject was indicted in the District of Minnesota for Fictitious and Fraudulent Claims and Theft of Public Money. Additional judicial action is pending.

### **Sovereign Citizen Pleads Guilty in Forging Former Secretary Lew's Signature**

Our joint investigation with the Broward County, Florida, Sheriff's Office (BSO) identified a group of Sovereign Citizens who filed documents in the Broward County Clerk of Court's Office. The documents were filed in a foreclosure case against Bank of America and contained former Treasury Secretary Jacob J. Lew's forged signature on an Internal Revenue Service (IRS) Form 56, "Notice Concerning Fiduciary

Relationship.” The filings also contained IRS Form 56 documents with forged signatures from the Broward County Clerk of Court, Chief Executive Officer, Bank of America, and the law firm representing Bank of America. The documents were filed in support of a bankruptcy scheme to allow the subjects to “squat” in a residence they rented in 2008, for which they had made few payments. BSO felony State warrants were issued and the subject was arrested for Criminal Use of Personal Identity, Grand Theft, and Unlawful Filing of False Documents or Records against Property. The subject pled guilty in the Florida 17th Judicial District, Broward County, and was sentenced to 8 months in prison with credit for time served, along with 60 months of probation.

### **Subjects Arrested for Uttering Counterfeit Checks**

Our joint investigation with the Jacksonville, Florida, Sheriff's Office determined that 17 subjects conspired to cash counterfeit checks, drawn on OCC-regulated financial institutions in Jacksonville, Florida. Arrest warrants were issued for the 17 subjects in the Fourth Judicial Circuit of Florida. Five (5) of the 17 subjects have been arrested for Uttering Counterfeit Checks. Arrests are pending for 12 subjects and additional judicial action is pending.

### **Subject Pleads Guilty to Stolen Treasury Checks and Counterfeit Driver's License Scheme**

Our joint investigation with Fairfax City, Virginia, Police Department and USPIS uncovered a criminal fraud conspiracy involving subjects using counterfeit Washington, DC, drivers' licenses to negotiate stolen Treasury checks and Washington, DC, payroll checks. Three subjects have been identified. One subject pled guilty to charges of Bank Fraud. Investigative efforts continue to bring charges against the remaining subjects and identify additional subjects.

### **Alcohol and Tobacco Tax and Trade Bureau Auditor Charged With Gambling While Teleworking**

Our joint investigation with IRS-CI, revealed an Alcohol and Tobacco Tax and Trade Bureau auditor conducted personal business while teleworking to engage in gambling at legal establishments and not report the proceeds of winnings. The subject was charged with a Federal Criminal Information related to charges of Theft of Public Money in the U. S. District Court, Southern District of Ohio. The subject pled guilty and sentencing is pending.

### **Subject Stole Social Security Administration Disability Benefits**

Our joint investigation with SSA OIG determined that a subject stole Social Security disability benefits, paid by Treasury, intended for a minor child not in their custody. The subject was indicted and subsequently arrested in the Middle District of Florida for Theft of Public Money and False Statements. The subject entered a plea agreement in U.S. District Court, Middle District of Florida, and began an 18 month diversion program.

### **Sovereign Citizen Arrested for Creating and Uttering Fictitious Treasury Obligations**

Our joint investigation with the Federal Bureau of Investigation (FBI) determined that a subject, a Sovereign Citizen adherent, residing in Jacksonville, Florida, was creating and uttering fictitious Treasury obligations. The subject was indicted and subsequently arrested in the Middle District of Florida for 10 counts of Fictitious Obligations intended to Defraud. Trial has been postponed.

### **Sex Trafficker Steals Social Security Benefits of Victims and Commits Bank Fraud**

Our joint investigation with SSA OIG, the FBI, the U.S. Department of Health and Human Services OIG, Florida Department of Law Enforcement, and Columbia County Sheriff's Office determined that a subject living in Fort White, Florida, was a serial bigamist, who engaged in sex trafficking and involuntary servitude, concerning vulnerable victims. Additionally, the subject stole the victims' Social Security benefits paid by Treasury and committed bank fraud. The subject was indicted in the Middle District of Florida and was detained pending trial. The subject was found deceased in his jail cell, his death was ruled due to natural causes. The case was dismissed, without prejudice.

### **Subject Sentenced for Terroristic Threats to Bureau of the Fiscal Service Employee**

Our investigation concluded with a subject's arrest for making threats against a Bureau of the Fiscal Service (Fiscal Service) employee over the phone. The subject threatened violence against the employee, the employee's family, and a Fiscal Service facility. The subject was found guilty in Nacogdoches, Texas, for Terroristic Threats and sentenced

to 12 months of probation, 80 hours of community service, \$60 monthly fine for 12 months, required to attend anger management classes, and write a letter of apology to Fiscal Service.

---

**Following is information related to significant investigative activities from prior semiannual periods.**

### **Subjects Plead Guilty to Identity Theft and Tax Fraud**

As reported in previous semiannual periods, our joint investigation with the IRS-CI and USPIS revealed that multiple subjects conspired to defraud the Federal Government by producing at least 12,000 fraudulent Federal income tax returns using stolen identities, and negotiating the resulting tax refund payments, totaling \$40 million for personal gain.

**Update:** One subject pled guilty to Fraud and two subjects were indicted on charges of Conspiracy to Commit Theft of Public Funds. Five subjects were arrested for Conspiracy to Commit Theft of Public Funds, Theft, and Aggravated Identity Theft. The five subjects were sentenced to a total of 93 months in prison, 168 months of probation, and \$2.5 million in restitution. Sentencing is pending for the remaining subjects.

To date, the joint investigation has resulted in 49 arrests, including the arrest of employees of MSBs, financial institutions, and the USPS. Of the 49 arrests, 40 subjects pled guilty and 3 subjects were found guilty by jury trial. Twenty-one (21) subjects have been sentenced to 654 months in prison, 984 months of probation, and ordered to pay \$15.2 million in restitution to Treasury. Additional judicial action is pending in the case. The case is being prosecuted by the U.S. Attorney's Offices in the District of Columbia; District of Maryland, Greenbelt Office; and by the Department of Justice, Tax Division.

### **19 Subjects Indicted for International Fraud and Money Laundering**

As previously reported, our joint investigation with the FBI determined a transnational organized crime network conducted a multi-million dollar fraud and money laundering operation that resulted in the theft of over \$13 million from more than 170 victims. As a result of fraudulent transactions identified by this investigation, additional thefts of over \$56 million in victim funds were prevented, disrupted, or returned. The operation

involved online vehicle sales fraud, business email compromise schemes, and an unlicensed money transmitting and international money laundering network, “hawala.” These fraud schemes tricked both individuals and corporations into wiring millions of dollars to bank accounts under the control of the crime network. This network operated in the United States, Europe, and Israel. Nineteen (19) subjects were indicted by a Federal grand jury in U.S. District Court, District of Columbia, and subsequently arrested in New York, New York; Los Angeles, California; and Israel, Hungary, Bulgaria, and Germany. Those arrested were charged with various violations that include: Bank Fraud, Conspiracy to Commit Bank and Mail Fraud, Conspiracy to Commit Money Laundering, Conspiracy to Commit Wire Fraud, and Conspiracy to Operate an Unlicensed Money Transmitting Business. Trial dates are pending.

**Update:** An additional subject, previously indicted for Conspiracy within the District of Columbia, was arrested in Romania. Judicial action continues.

### **Subjects Arrested for Redirecting Treasury Funds from Supplemental Nutrition Assistance Program Benefits**

As reported in previous semiannual periods, our joint investigation with the Department of Agriculture and SSA OIGs, the Department of Homeland Security Investigations (HSI), USSS, the Drug Enforcement Administration, IRS-CI, and with State and local law enforcement agencies determined that complicit store owners and scheme organizers orchestrated the fraudulent exchange and redirection of over \$6.3 million in Treasury funded, State-managed welfare and benefit cards. Nine subjects were initially indicted and arrested for Conspiracy and Wire Fraud, with an additional charge of Drug Trafficking for two of the nine subjects. Two additional subjects were indicted for Wire Fraud, and another subject was charged with Theft of Public Funds. Eleven of the subjects pled guilty to Wire Fraud related charges, including the two subjects who also pled guilty to Drug Trafficking.

**Update:** One subject was found guilty of Conspiracy and Wire Fraud. Seven subjects were sentenced to prison terms, supervised release, and restitution up to \$1.3 million each. To date, total restitution for the subjects amounts to \$6.1 million. The subjects’ prison terms varied between 11 and 78 months, for a total of 343 months. The subjects’ probation terms varied from 24 to 36 months, for a total of 384 months. Sentencings are pending for the remaining subjects.

### Subjects Arrested for Bank Fraud

As reported in previous semiannual periods, our joint investigation with the Fayetteville, North Carolina, Police Department determined that multiple subjects in the Fayetteville area were involved in an organized scheme to defraud several local OCC-regulated banks and credit unions. The scheme involved opening accounts with stolen identities, depositing counterfeit business checks into those accounts, and removing the funds before the checks were identified as counterfeit. The estimated loss is \$3.7 million. Three subjects were indicted and subsequently arrested for Bank Fraud. One of the three subjects pled guilty to Bank Fraud in U.S. District Court, Eastern District of North Carolina and was sentenced to 1 month of home confinement, 60 months of probation, and ordered to pay \$2,100 in restitution. The other two subjects were in plea negotiations.

**Update:** Two subjects pled guilty to Bank Fraud and were sentenced. One subject was sentenced to 144 months in prison, 60 months of probation, and ordered to pay \$12,200 in restitution. The second subject was sentenced to 14 months in prison, 60 months of probation, and \$22,600 in restitution. This investigation is ongoing with preparations to indict additional subjects.

### Subject Found Guilty of Theft of Government Funds and Theft or Receipt of Stolen Mail

As reported in previous semiannual periods, our joint investigation with SSA OIG, USPIS, and USPS OIG determined that several Social Security recipients in the Pinellas County, Florida area did not receive their benefit checks. The stolen checks, totaling \$2.3 million, were subsequently cashed in North Florida and South Georgia. Five subjects, including a USPS employee, were arrested. Three of the five subjects pled guilty and were sentenced for Theft of Government Funds and Theft or Receipt of Stolen Mail. The fourth subject was found guilty of Theft of Government Funds in the U.S. District Court, Middle District of Florida, and was sentenced to 87 months in prison and was ordered to pay \$721,000 in restitution. The fifth subject, a former Postal employee, was found guilty of Theft of Government Funds and Theft or Receipt of Stolen Mail. Sentencing was pending for the former Postal employee.

**Update:** The fifth and final subject was sentenced in the U.S. District Court, Middle District of Florida to 52 months in prison, a seizure judgement of \$570,000, and restitution of \$152,000.

### Former Medical Center Employee Sentenced for Identity Theft

As reported in previous semiannual periods, our joint investigation with the USSS and IRS-CI determined that a former medical center employee abused her access to patient records to commit identity fraud. Specifically, the former medical center employee conspired with multiple subjects to defraud the Government and taxpayers by stealing personally identifiable information and using the stolen identify information to fraudulently obtain Federal income tax refund payments totaling over \$2 million. The former medical center employee pled guilty to 1 charge of Conspiracy, and was sentenced to 60 months of probation and \$6,500 in restitution.

**Update:** One subject was indicted and pled guilty to Theft of Public Money. To date the investigation has resulted in 11 arrests, 10 guilty pleas and 1 trial conviction. Eleven (11) subjects have been sentenced to 511 months in prison, 396 months of probation, and ordered to pay \$1.8 million in restitution. The case is being prosecuted by the U.S. Attorney’s Office, Middle District of Georgia.

### Subject Pleads Guilty to Wire Fraud and Aggravated Identity Theft

As reported in previous semiannual periods, our joint investigation with HSI, IRS-CI, SSA OIG, and USPIS determined that a citizen of the Ivory Coast, living in Ashburn, Virginia, used assumed identities to commit financial crimes. The subject claimed to be a tax preparer, filed false Federal income tax returns, and diverted tax refunds to bank accounts that the subject controlled. The subject pled guilty to Wire Fraud and Aggravated Identity Theft in the Eastern District of Virginia, and was sentenced to 54 months in prison and ordered to pay \$672,000 in restitution and \$652,000 in forfeiture. A second subject, who provided information to be used in the scheme to the first subject, was indicted for Wire Fraud, False Claims, and Conspiracy to Defraud the Government. The second subject pled guilty to Conspiracy to Commit Wire Fraud and False Claims, and was sentenced to 15 months in prison, 36 months of probation, and ordered to pay \$106,000 in restitution and \$38,000 in forfeiture. A third subject was arrested after being indicted in the U.S. District Court, Eastern District of Virginia for violations of Conspiracy, Aiding and Assisting in the Preparation of a False Tax Return, and Fraud and Misuse of Visa, Permit and Other Documents. The third subject opened several bank accounts where fraudulent Federal income tax return payments were deposited and was authorized to stay lawfully within the United States after making a false statement on his application for a Legal Permanent Resident card.

**Update:** The third subject pled guilty to Conspiracy to Commit Wire Fraud and Fraud and Misuse of Visa, Permit and Other Documents. Sentencing is pending for the third subject.

### Arrest Warrants Issued for Subjects Cashing Counterfeit Business Checks

As reported in previous semiannual periods, our joint investigation with the Jacksonville, Florida, Sheriff's Office determined that a subject was generating counterfeit identification documents to open accounts at OCC-regulated financial institutions to cash counterfeit business checks. There was \$1 million in fraudulent withdrawals and wire transfers. An arrest warrant was executed on the subject and a 2016 Ford Mustang was seized. An additional arrest warrant was obtained for a co-conspirator. The key subject pled guilty to Criminal Use of Personal Information and Dealing in Stolen Property. The case is being prosecuted by the Florida State Attorney's Office.

**Update:** The key subject was sentenced to 72 months in prison and 48 months of probation. The co-conspirator pled guilty to 2 counts of Criminal Use of Personal Information and was sentenced to time served and an additional 18 months of probation.

### Subject Pleads Guilty to False Claims and Conspiracy

As reported in previous semiannual periods, our joint investigation with IRS-CI and the OIG's of SSA and the U.S. Department of Health and Human Services determined that a subject filed false Federal income tax returns and received over \$800,000 in tax refunds that were directed to a business account under the control of the subject. The subject also received improper Social Security and Medicare benefits. The subject pled guilty to Theft of Public Money and Tax Fraud and was sentenced in the U.S. District Court of Eastern Virginia to 24 months in prison, 36 months of probation, and ordered to pay \$836,000 in restitution. Additionally, the subject had \$768,000 seized representing the proceeds of the charged offenses. A second subject, who assisted in submitting the false tax returns to the IRS, was indicted for Conspiracy to Defraud the Government with Respect to Claims, False Claims, Theft of Public Money, and Aggravated Identity Theft.

**Update:** The second subject pled guilty to Conspiracy to Defraud the Government with Respect to Claims and False Claims. Sentencing is pending.

### **Subject Arrested for Bank Fraud**

As reported in the previous semiannual period, our joint Investigation with the Randolph County, North Carolina, Sheriff's Office identified a subject who fraudulently used a corporate tax identification number to open numerous checking accounts at several OCC-regulated banks. The subject used checks from these accounts to kite<sup>9</sup> money to inflate the balances on his accounts and make large dollar purchases of vehicles, tractors, Rolex watches, and jewelry. Subsequently, the subject sold the items through online auction sites such as Craigslist and E-bay. The estimated loss in this case exceeded \$250,000. The subject was indicted by a Federal grand jury in the Middle District of North Carolina for Bank Fraud, Possession of a Counterfeit Security, and Aggravated Identity Theft. The subject pled guilty to Bank Fraud pursuant to a plea agreement. Sentencing was pending.

**Update:** A mental health evaluation of the subject was ordered by the court. Sentencing has been rescheduled.

### **Subject Arrested for Mail Fraud, Wire Fraud, and Aggravated Identity Theft**

As reported in the previous semiannual period, our joint investigation with the Durham, North Carolina, Police Department determined that a paralegal embezzled over \$180,000 from OCC-regulated bank accounts managed by two different law firms. The subject was indicted by a Federal grand jury in the Middle District of North Carolina for Mail Fraud, Wire Fraud, and Aggravated Identity Theft. Plea negotiations were ongoing.

**Update:** The subject pled guilty to Mail Fraud and Aggravated Identity Theft. Sentencing is pending.

### **Subject Arrested for Access Device Fraud and Aggravated Identity Theft**

As reported in the previous semiannual period, our investigation determined that a Durham, North Carolina, subject fraudulently used credit cards issued to a religious ministry organization. The subject obtained the credit cards and socially engineered retail merchants to “force” over 200 transactions, totaling over \$113,000 in attempted credit card purchases. The subject was indicted by a Federal grand jury in

---

<sup>9</sup> Kiting is a form of check fraud, involving taking advantage of the float to make use of nonexistent funds in a checking or other bank account.

the Middle District of North Carolina for Access Device Fraud, Use of an Unauthorized Access Device, and Aggravated Identity Theft. Plea negotiations were ongoing.

**Update:** An additional 200 transactions were identified, revising the total upwards to over 400 transactions and over \$170,000 in attempted credit card purchases. The subject pled guilty to Wire Fraud, Aggravated Identity Theft, and Access Device Fraud. Sentencing is pending.

### Two Sovereign Citizen Subjects Charged for Using Fictitious Obligations

As reported in previous semiannual periods, our investigation determined that two subjects, aligning themselves with the Sovereign Citizen ideology, presented a fictitious document titled "International Bill of Exchange" as payment to obtain seven new automobiles worth over \$160,000. Other attempts were made by the subjects, using the same method, to purchase additional new vehicles. Both subjects were arrested and criminally charged within the U.S. District Court, District of Maryland for using Fictitious Obligations. One subject pled guilty to Manufacturing/Uttering Fraudulent Financial Instruments, pursuant to a plea agreement. Additional judicial action was pending.

**Update:** The second subject pled guilty to Conspiracy to Defraud the Government with Respect to Claims and False Claims. Additional judicial action is pending.

### Individuals Indicted on Criminal Violations Under the Racketeer Influenced and Corrupt Organization and Street Gang and Terrorism Prevention Acts

As reported in previous semiannual periods, our joint investigation with USSS, IRS-CI, and Bibb County, Georgia, Sheriff's Office determined that between April and June 2014, several individuals were involved in a large-scale identity-theft operation/criminal organization. The group was filing false Federal income tax returns, as well as using stolen identities and fraudulently-obtained credit cards, to send money to local jail inmates who were attempting to make bond. In Bibb County, Georgia, 18 subjects were indicted for violations of Georgia's Racketeer Influenced and Corrupt Organization Act (RICO) and of its Gang and Terrorism Prevention Act. The investigation focused on three main subjects. One of these subjects pled guilty and was sentenced to 180 months in prison. The second subject pled guilty to violating Georgia's RICO and Gang and Terrorism Prevention Acts, and was sentenced to 240 months in prison and 96 months of probation.

**Update:** The third subject pled guilty to Possession of a Firearm by a Convicted Felon and was sentenced to 24 months in prison and 36 months of probation.

### Subject Pleads Guilty to Theft of Public Money

As reported in the previous semiannual period, our investigation determined that a subject converted funds from the District of Columbia Retirement Board (Board) intended for his grandmother, a retired annuitant, for his own personal use. When the subject's grandmother died in June 2012, the Board was not notified and payments continued into the grandmother's bank account, to which the subject had access. Approximately \$81,000 was deposited into the grandmother's bank account before the Board discovered the annuitant's death. The subject confessed that he withdrew all the money and knowingly converted the funds for his own personal use. The subject was prosecuted by the U.S. Attorney's Office, District of Columbia, and pled guilty to Theft of Public Money. Sentencing was pending.

**Update:** The subject was sentenced to 36 months of probation and ordered to pay \$81,000 in restitution.

### Two Subjects Indicted and Arrested for Negotiating Altered Treasury Checks

As reported in a previous semiannual period, our joint investigation with the USSS, USPIA, and SSA OIG determined that two California subjects negotiated stolen and altered Treasury checks totaling \$24,000. The subjects used stolen identities to create fictitious documents to facilitate this scheme. The subjects were indicted in U.S. District Court, Northern District of California and subsequently arrested for Bank Fraud, Aggravated Identity Theft, Theft of Government Money, and Possession with Intent to Distribute Methamphetamines. Both subjects were being held in Federal custody pending trial.

**Update:** One subject pled guilty in U.S. District Court, Northern District of California to Theft of Government Property, Possession with Intent to Distribute Methamphetamines, and Criminal Forfeiture. The second subject pled guilty and was sentenced to 25 months in prison, 60 months of probation, and ordered to pay \$23,000 in restitution. A third subject was arrested for Theft of Government Money and pled guilty to Theft of Government Property. Sentencing is pending for two of the subjects.

### **Subject Arrested for Cashing Altered Treasury Bonds**

As reported in a previous semiannual period, our joint investigation with the Michigan State Attorney General’s Office determined that a subject in the Detroit, Michigan area fraudulently obtained 143 Treasury bonds and cashed them at a bank. The subject’s illicit actions resulted in a \$19,000 loss to Treasury. A local arrest warrant was served on the subject. The subject was awaiting trial.

**Update:** The subject pled guilty to charges of Criminal Enterprise-Conducting and 10 counts of Uttering and Publishing. The subject was sentenced to 60 months of probation and ordered to pay \$19,000 in restitution.

### **Subject Arrested for Negotiating Multiple Replacement Treasury Checks**

As reported in the previous semiannual period, our investigation determined that a Richmond, Virginia, subject negotiated two Treasury checks totaling \$4,000. The subject negotiated the original Federal income tax refund check, received a replacement check, and attempted to cash the replacement check. After the subject admitted to not being entitled to the second check, the subject received a third check and successfully negotiated it. The subject was arrested for Obtaining Money under False Pretense. Judicial action was pending with the Commonwealth of Virginia.

**Update:** The Commonwealth of Virginia agreed that upon the subject paying \$1,900 in restitution to the victim, charges were reduced to misdemeanor Petit Larceny with 12 months in prison and 12 months suspended for a period of 36 months.

### **BEP Police Officer Arrested for Threats Against Another BEP Police Officer**

As reported in previous semiannual periods, our investigation determined that while off-duty, a Bureau of Engraving and Printing (BEP) police officer threatened violence against another BEP police officer. The subject made the threat over the telephone to a third-party, who was also a BEP police officer. The subject threatened to carry out the violent act at the BEP facility in Fort Worth, Texas. The subject was arrested for making terroristic threats and the subject’s employment was terminated by BEP security management. In response to the termination, the subject filed a complaint with the Merit Systems Protection Board and was later reinstated into a non-law enforcement position at BEP. The Tarrant County District Attorney’s Office was reviewing the case.

**Update:** The subject decided not to negotiate a plea and to go to trial if necessary. After reviewing the case, the Tarrant County Attorney’s Office interviewed the complainant and advised that the complainant may have to go to trial and testify. The complainant then requested all charges against the subject be dropped. The case was dismissed by the Court.

## Other OIG Accomplishments and Activities

### The Seventh Annual Treasury OIG Awards

On May 18, 2017, the Department of the Treasury (Treasury) Office of Inspector General (OIG) held its seventh annual awards program in the Cash Room of the Treasury Building. The program recognized the achievements and outstanding performance of OIG staff and its agency partners during calendar year 2016. Presented were 9 Individual Achievement Awards, 8 Teamwork Awards, 3 Customer Service Awards, 1 Rookie of the Year Award, 2 Special Inter-Agency Teamwork Awards, and 1 Special Inter-Agency Customer Service Award. Also awarded was the Inspector General Leadership Award, the highest honor bestowed on an OIG employee.

Inspector General Thorson presented awards to the following recipients:

#### Individual Achievement Award

Amy Altemus, Jeffrey Dye, Shaneasha Edwards, Bobbie Gambrell, Jacob Heminger, Peter LoJacono, Sergiu Prisacari, Anita Smith, and Dionne Smith

#### Intra-Component Teamwork Award

##### **Bureau of Engraving and Printing Authentix Team**

Timothy Cargill, Maryann Costello, Jenny Hu, Erin Mangino, and Sharon Torosian

##### **Digital Accountability and Transparency Act Audit Team 2016**

Herb Addy, Horace Bryan, Maria McLean, Jeneba Moiwo, Andrea Smith, Ashley Smith, Gregory Sullivan, John Tomasetti, and Avery Williams

##### **Fiscal Year 2016 Financial Statement Audits Team**

Nikki Akinyeye, Ade Bankole, Rafael Cumba, Rufus Etienne, James Hodge, Mark Levitt, Sergiu Prisacari, and Catherine Yi

##### **Federal Information Security Management Act Audit Team 2016**

Don'te Kelly, Larissa Klimpel, Robert Kohn, and Mike Patel

##### **Treatment of Legacy Financial Management Service Employees Audit Team**

Joshua Dreis, Shaneasha Edwards, and Myung Han

**Fraudulent American Recovery and Reinvestment Act Funds Team**

Brittany Bosak, Christopher LeFever, and Elliott Potts

**Inter-Component Teamwork Award**

**Customs Revenue Engagement Team**

Patrick Arnold, Richard Delmar, Erin Mangino, Mark Ossinger, Anne Ryer, and Sharon Torosian

**Iran Payment Inquiry Team**

Richard Delmar, Jeanne DiFruscia, Kenneth Dion, Jeffrey Dye, Shaneasha Edwards, Deborah Harker, Andrea Smith, and Gregory Sullivan

**Customer Service Award**

Kenneth Dion, Tracy George, and Valerie Toyé

**Rookie of the Year Award**

Nikki Akinyeye

**Special Inter-Agency Teamwork Award**

**Barber Shop Case**

Ivan Casilli, John Han, Joshua Henderson, and Jerry Marshall, Treasury OIG  
Maria Cuvillon and Christopher Saunders, U.S. Postal Inspection Service Inspectors  
Michael Helgesen, Joseph Larose and Gregory Milne, Internal Revenue Service  
Criminal Investigators  
Victoria Digiampaolo, Wayne Everett and Amy Frame, Bureau of the Fiscal Service  
Forensic Document Analysts  
Drew Mueller, Bureau of the Fiscal Service Data Analyst

**Operation Top Gear**

Jonathan Fraller and Daniel Harding, Treasury OIG  
Roland Chataway, Bridgit Depietto, Marc Hess, Joe Lewis, Tom Krall and John Wong,  
Federal Bureau of Investigation Special Agents  
Jennifer Bondgren and Jeremy Murphy, Federal Bureau of Investigation Analysts

### Special Inter-Agency Customer Service Award

David Ambrose, Bureau of the Fiscal Service



*Jeff Lawrence Receiving the  
Inspector General Leadership Award from  
Inspector General Thorson*

### **Continuing Professional Education Symposium**

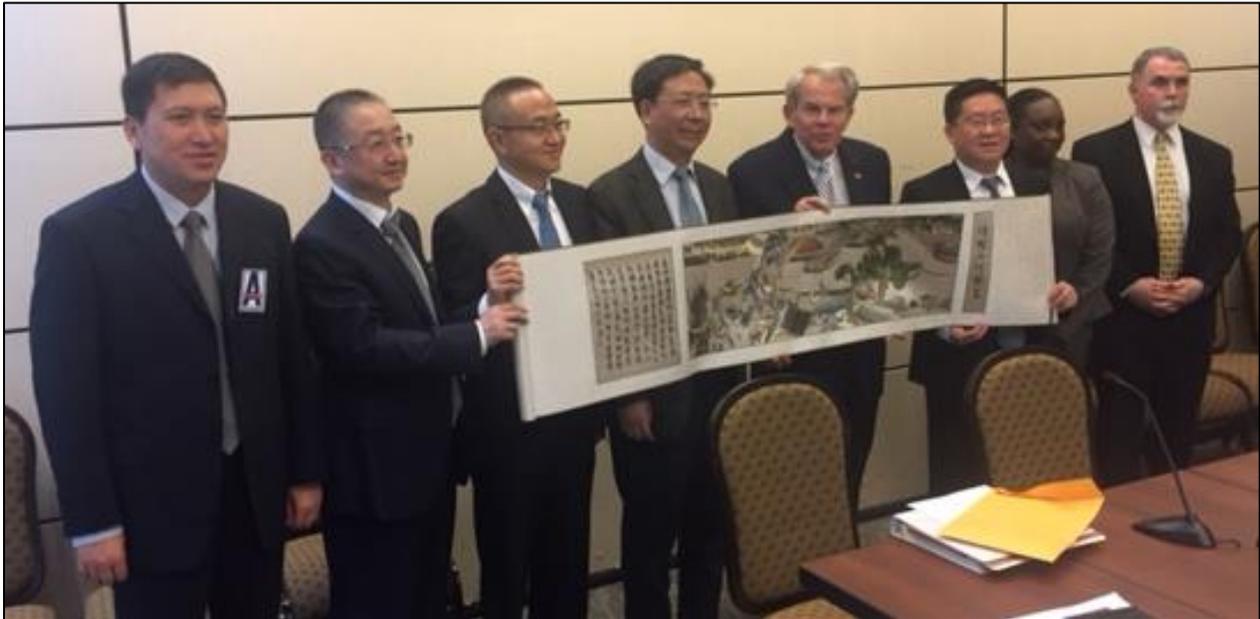
The Office of Audit held its biennial continuing professional education symposium July 31-August 4, 2017, at the Warwick Hotel Rittenhouse Square in Philadelphia, Pennsylvania. In attendance were 104 OIG staff members. The symposium provided 35.5 hours of quality training in the areas of (1) interviewing; (2) communication; (3) statistical sampling; (4) computer-processed data reliability; (5) report writing; and (6) leadership. At plenary sessions, the attendees heard from subject matter experts on topics such as creating a culture of excellence, change management, records

## Other OIG Accomplishments and Activities

management, cyber threats, and whistleblower protection. The office also conducted its second Audit IQ competition testing staff's knowledge of auditing and Treasury history. This year's Audit IQ champions were **Rebecca Berry**, Auditor; **David Hash**, Auditor; **Eleanor Kang**, Audit Manager; **Robert Kohn**, Information Technology Specialist; **Kar Lee**, Auditor; **Maria McLean**, Auditor; **Kieu Rubb**, Audit Director; **Olivia Scott**, Audit Manager; **John Snyder**, Auditor and **Greg Sullivan**, Audit Manager.

### OIG Hosts Chinese Delegation

On September 15, 2017, Inspector General Thorson and other OIG executives met with a 20-member delegation from the Ministry of the Treasury of P.R. China to discuss the mission of the U.S. Treasury, and its organizational structure; the internal control environment; and how OIG conducts independent audits of the Treasury.



**Pictured above are OIG executives with members of the Chinese Delegation**

### OIG Audit Leadership Roles

OIG's professionals serve on various important public and private professional organizations supporting the Federal audit community. Examples of participation in these organizations follow:

**Andrea Smith**, Audit Director, chairs the Federal Audit Executive Council's (FAEC) Digital Accountability and Transparency Act (DATA Act) Working Group which

educates the Inspectors General and Government financial communities on the DATA Act oversight process. As of the date of this report, the working group consists of approximately 200 members representing 38 OIGs. During the reporting period, Ms. Smith participated in a number of stakeholder outreach events to various Government-wide communities describing the Inspector General community's approach to its oversight requirements under the DATA Act as documented in the FAEC DATA Act Working Group's *Inspectors General Guide to Compliance Under the DATA Act*, including the: (1) Counsel of the Inspectors General on Integrity and Efficiency (CIGIE)/Government Accountability Office Financial Statement Conference at the U.S. Department of Agriculture Auditorium in Washington, DC, on April 27, 2017; (2) Joint Financial Management Improvement Conference at the Ronald Reagan Building and International Trade Center in Washington, DC, on May 8, 2017; (3) National Academy of Public Administration at its headquarters in Washington, DC, on May 19, 2017; (4) Data Coalition's DATA Act Summit at the Mayflower Hotel in Washington, DC, on June 29, 2017; and (5) American Institute of Certified Public Accountants (AICPA) Governmental Accounting and Auditing Update Conference at the Capital Hilton in Washington, DC, on August 7, 2017. Other OIG representatives that contributed to these efforts were **Debbie Harker**, Assistant Inspector General for Audit; **Pauletta Battle**, Deputy Assistant Inspector General for Audit; **John Tomasetti**, Audit Manager; and **Ashley Smith**, Audit Manager.

Also during this reporting period, Ms. Smith participated in a Career Day at the City Center Public Charter School in Washington, DC, on April 5, 2017. Ms. Smith provided an overview of the work Treasury performs and answered questions related to accounting and business-related career paths in the Federal sector.

In addition, Ms. Smith, led a half-day workshop OIG hosted for the National Association of Black Accountants, Inc. Accounting Career Awareness Program (ACAP) in OIG's Washington, DC office on July 19, 2017. ACAP's primary objective is to increase the understanding of accounting and business career opportunities among high school students from underrepresented ethnic groups. ACAP, a one-week residency program at Howard University, introduced students to accounting, finance, economics, and management through a focused, undergraduate-level program taught by college faculty and guest lecturers from business and Government. During the week, students had the opportunity to attend classes on careers in accounting and business, personal development, college preparation, and tour college campuses, local companies, and Certified Public Accounting firms. OIG invited the students to learn about auditing in the Federal sector. Other OIG representatives that contributed to these efforts were **Eric Thorson**, Inspector General; **Debbie Harker**, Assistant Inspector

## Other OIG Accomplishments and Activities

---

General for Audit; **Rich Delmar**, Counsel to the Inspector General; **James Hodge**, Audit Director; **Sonya Scott**, Special Agent-in-Charge; **Kim Mingo**, Human Resources Manager; **Myung Han**, Audit Manager; **Shiela Michel**, Audit Manager; **Nadine Forgenie**, Audit Manager; **Dionne Smith**, Auditor-In-Charge; **Lawrence Gonzalez**, Auditor; and **Nikki Akinyeye**, Auditor.

**Pauletta Battle**, Deputy Assistant Inspector General for Financial Management and Transparency Audits, presented on the Federal OIGs' approach to auditing the DATA Act at a training event sponsored by the Data Foundation in Washington, DC, on June 8, 2017. The event, titled "DATA Act Training," was geared toward Federal financial management, program management, procurement, and assistance professionals.

**Lisa Carter**, Deputy Assistant Inspector General for Financial Sector Audits, serves as the Treasurer for the Association of Inspectors General DC Chapter, an organization of Federal, State, and local Inspectors General. Ms. Carter is also a member of its Training committee. Treasury OIG hosted a DC Chapter meeting and training event on May 23, 2017. **Inspector General Thorson** opened the event, which featured speakers **Mr. James F. Trost**, a Program Analyst with the Department of Defense Inspector General Defense Criminal Investigative Services, who presented on developing cases and trend analyses within the IG community, **Mr. Robert Wuhrman**, Enterprise Architect at the General Services Administration Office of Government-wide Policy, Unified Shared Services Management, who spoke about shared services between the OIG and the agency, and **Mr. James Rohls**, Special Agent for the Federal Bureau of Investigation. Mr. Rohls spoke about the role of social media in conducting investigations.

**Jeff Dye**, Audit Director, regularly teaches a module of the Introductory Auditor course sponsored by the CIGIE Training Institute.

**Debbie Harker**, Assistant Inspector General for Audit, served as a panel member for a presentation at the Data Coalition's DATA Act Summit at the Mayflower Hotel in Washington, DC, on June 29, 2017.

**Donna Joseph**, Deputy Assistant Inspector General for Cyber and Financial Assistance Audits, serves as the National Single Audit Coordinator for Treasury, and is a member of the AICPAs' National Governmental Accounting and Auditing Update planning committee.

## Other OIG Accomplishments and Activities

---

**Kieu Rubb**, Audit Director, serves on the AICPA's Government Performance and Accountability Committee. The committee is comprised of 13 members representing Federal, State, and Local Government, and education. Ms. Rubb also teaches Peer Review and Introductory Auditor training sessions sponsored by the CIGIE Training Institute.

This page intentionally left blank.

# Statistical Summary

## Summary of OIG Activity

April 1, 2017 through September 30, 2017

OIG Activity	Number or Dollar Value
<b>Office of Counsel Activities</b>	
Regulation and legislation reviews	0
Instances where information was refused	0
<b>Office of Audit Activities</b>	
Reports issued and other products	30
Disputed audit recommendations	0
Significant revised management decisions	0
Management decision in which the Inspector General disagrees	0
<b>Monetary benefits (audit)</b>	
Questioned costs	\$1,071,394
Funds put to better use	\$0
Total monetary benefits	\$1,071,394
<b>Office of Investigations Activities</b>	
<b>Criminal and judicial actions (including joint investigations)*</b>	
Investigative reports issued	92
Cases referred for prosecution and/or litigation	31
Individuals referred for criminal prosecution to the Department of Justice	51
Individuals referred for criminal prosecution to state and local authorities	28
Cases accepted for prosecution and/or litigation	49
Arrests	74
Indictments/informations	35
Convictions (by trial and plea)	32

*\*During the reporting period, subjects were sentenced to 678 months of prison time, 792 months of probation, 13 hours of community service, and ordered to pay fines, restitution, and court fees in the amount of \$12.9 million. In addition, OIG seized \$2.2 million as the result of a criminal prosecution and participated in an investigation where a judgement of \$29.5 million was ordered and paid to Treasury.*

## Metrics Used for Office of Investigations Activities

Department of the Treasury (Treasury) Office of Inspector General (OIG) investigative statistics listed above were obtained through reports drawn from OIG's Office of Investigations case management system.

## Reports With Unimplemented Recommendations

Issued prior to April 1, 2017

The following list of Treasury OIG reports with unimplemented recommendations is based on information in the Treasury’s automated audit recommendation tracking system, which is maintained by Treasury management officials, and recommendations tracked by other Federal organizations related to OIG’s oversight of the Resources and Ecosystems Sustainability, Tourist Operations, and Revived Economies of the Gulf Coast States Act of 2012 (RESTORE Act) programs and activities of the Gulf Coast Ecosystem Restoration Council (Council) and the National Oceanic and Atmospheric Administration’s Gulf Coast Ecosystem Restoration Science, Observation, Monitoring, and Technology Program.

OIG is reporting 40 open and unimplemented recommendations for 14 reports issued prior to April 1, 2017. OIG does not have any potential cost savings to report for unimplemented recommendations on reports issued before the commencement of this reporting period.

OIG considers all unimplemented recommendations for reports issued over 6 months to be significant.

### Treasury Programs and Operations

Number	Date	Report Title and Recommendation Summary
OIG-15-036	06/15	<p><i>RESTORE Act: Alabama’s Center of Excellence Was Not Selected through Competitive Award</i></p> <p>The Fiscal Assistant Secretary should ensure that the Alabama Council selects its Centers of Excellence through a competitive process in accordance with the RESTORE Act and Treasury regulations prior to disbursing grant funds to the Alabama Council for funding Centers of Excellence. Management agreed with the recommendation. (1 recommendation)</p>

OIG-15-040 07/15 *OSP Needs to Promptly Inform OIG of Potential Illegal Activity and Improve Other Processes*

The Assistant Secretary for Intelligence and Analysis should (1) conduct, in conjunction with the Office of the Chief Information Officer, a resource analysis of the Office of Security Programs (OSP) to determine the proper information technology software, equipment, and support needed to comply with Central Verification System requirements; (2) ensure that OSP works with the Office of the Chief Information Officer and Office of Personnel Management, as appropriate, to resolve OSP system and data issues with the Central Verification System so that Treasury employee security clearance data is provided to and maintained in the Central Verification System on a complete, current, and accurate basis going forward; (3) improve the security clearance process guidance by streamlining the Treasury Security Manual and other related sources by, for example, including a roles and responsibilities matrix/cross-index of all the parties involved in the security clearance process; and (4) ensure that OSP develops and implements comprehensive standard operating procedures for the security clearance process. Management agreed with the recommendations. (4 recommendations)

---

OIG-CA-15-004 11/15 *Information Technology: Department of the Treasury Federal Information Security Management Act Fiscal Year 2014 Evaluation*

United States Mint (Mint) management, for the selected systems, should ensure National Institute of Standards and Technology Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations" (NIST P 800-53 Rev. 4) controls and enhancements are implemented on the systems and tested promptly. Management agreed with the recommendation. (1 recommendation)

---

OIG-16-001    10/15    *Libyan Sanctions Case Study*

The Director of the Office of Foreign Assets Control should (1) identify the actions required to implement and administer its sanctions programs and document these in written standard operating procedures. The standard operating procedures should provide sufficient information to key staff members to enable them to complete the fundamental steps necessary in implementing and administering sanctions programs; (2) implement a methodology to identify blocked assets that have been released by license type (general or directive); (3) continue to pursue development and implementation of electronic filing for high-volume filers; and (4) develop a lessons-learned process to capture and communicate acquired knowledge from past sanctions programs at a time appropriate for each sanctions program. Management agreed with the recommendations. (4 recommendations)

---

OIG-16-010    11/15    *Information Technology: Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2015 Performance Audit*

Mint management, for the selected system, should (1) ensure access forms are completed, properly reviewed by the help desk prior to granting access, and centrally retained by the help desk; (2) ensure that control implementation statements and statuses for all NIST P 800-53 Rev. 4 controls and control enhancements are fully addressed in the system security plan; (3) revisit the existing third-party cloud service provider's contract and ensure the appropriate Federal Risk and Authorization Management Program security clauses and requirements related to the Federal Information Security Modernization Act of 2014 (FISMA) and NIST guidance is incorporated; and (4) ensure that its third-party cloud service provider provides FISMA-related artifacts to demonstrate FISMA compliance to the Mint security compliance team. Management agreed with the recommendations. (4 recommendations)

---

OIG-16-047 06/16 *Treasury’s Government-wide DATA Act Implementation Continues, But Project Management Concerns Remain*  
 The Fiscal Assistant Secretary, working with the Office of Management and Budget where applicable, should continue efforts to strengthen project management over the Digital Accountability and Transparency Act of 2014 (DATA Act) implementation, ensuring that (a) progress metrics provide a consistent, accurate measure of task status and (b) key management decisions are documented. Management agreed with the recommendation. (1 recommendation)

OIG-16-050 07/16 *Information Technology: Vulnerabilities in Security Controls Over Mint’s Systems Need to Be Addressed*  
 The Principal Deputy Director of the Mint should ensure (1) all scanning capabilities look for all connected systems and scan results are reconciled against the Mint’s inventory; (2) obsolete software is either removed or upgraded; (3) software patches and updates are timely applied; (4) systems and software are securely configured; and (5) scanning capabilities detect published vulnerabilities. Management agreed with the recommendations. (5 recommendations)

OIG-16-059 09/16 *General Management: Treasury Has Policies and Procedures to Safeguard Classified Information but They Are Not Effectively Implemented*  
 The Assistant Secretary for Intelligence and Analysis should direct the Deputy Assistant Secretary for Security to (1) emphasize to derivative classifiers the importance of properly marking classification decisions, including adding a note in classified emails to remind employees to properly portion mark emails before sending; (2) update the Treasury Security Manual to include OSP responsibilities to (i) follow-up timely with Departmental Offices and bureaus on their Standard Form (SF) 311 submissions; (ii) review the SF 311s for completeness and accuracy; (iii) implement a mechanism such as a checklist or reconciliation to ensure complete and accurate

reporting of SF 311 information; and (iv) document explanations for corrections made to the Department Offices' and bureaus' SF 311 reporting if OSP makes any changes; (3) provide additional guidance and training to SF 311 preparers focusing on areas of repeated weaknesses such as difficulties identifying the difference between original and derivative classification decisions; and remind the Departmental Offices and bureaus of their responsibilities to ensure that the SF 311 is complete and accurate; (4) emphasize to bureaus with employees who handle and generate classified information the importance of conducting annual self-inspections, documenting the results, and submitting the reports to OSP; (5) update the Treasury Security Manual to include procedures requiring OSP to follow up and obtain all bureau self-inspection reports; (6) ensure that training materials are periodically reviewed and updated to include current Federal and Treasury requirements; and (7) use the Treasury Learning Management System (TLMS) or a similar system to retain records of training and monitor completion of required derivative classifier and original classifier training. Management agreed with the recommendations.  
(7 recommendations)

---

OIG-17-003    11/16 *Information Technology: Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2016 Performance Audit*

Bureau of the Fiscal Service (Fiscal Service) management, for the second system, should configure or acquire additional system capability to automatically disable user accounts in accordance with system and Fiscal Service defined frequency. Management agreed with the recommendation.  
(1 recommendation)

Mint management, for the selected system, should require that senior level officials document their approvals of the Contingency Plan by adding their signature to the Contingency Plan signature page following each annual plan audit.

Management agreed with the recommendation.  
(1 recommendation)

Departmental Offices, for the selected system, should configure the system to disable user accounts automatically after 120 days of inactivity. Management agreed with the recommendation and also agreed to document legitimate exceptions of accounts excluded from the scripts.  
(1 recommendation)

---

OIG-17-004    11/16 *Information Technology: Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2016 Performance Audit for Collateral National Security Systems (Sensitive But Unclassified)*  
Due to the sensitive nature of the findings and recommendations, we designated the report sensitive but unclassified. (2 recommendations)

---

OIG-17-012    11/16 *Audit of the Department of the Treasury's Consolidated Financial Statements for Fiscal Years 2016 and 2015*  
The Assistant Secretary for Management and the Deputy Chief Financial Officer should ensure that the (1) Internal Revenue Service (IRS) takes corrective action to improve controls over financial reporting; (2) Fiscal Service takes corrective action to resolve control deficiencies over its information systems; and (3) IRS implements its remediation plan outlining actions to be taken to resolve noncompliance with the Federal Financial Management Improvement Act of 1996 requirements and the resources and responsible organizational units for such planned actions. Management agreed with the recommendations.  
(3 recommendations)

---

OIG-17-030    12/16 *Management Letter for the Audit of the United States Mint's Fiscal Years 2016 and 2015 Financial Statements*  
Mint's management should (1) develop and implement policy and procedures to review the access of privileged Mint HR Connect users on a defined frequency and (2) review the

access of privileged HR Connect users based on the frequency defined in procedures mentioned in Recommendation No. 1. Management agreed with the recommendations. (2 recommendations)

---

## Other Federal Agency Programs and Operations

OIG-16-051    07/16    *RESTORE Act: Gulf Coast Ecosystem Restoration Council's Records Management System Needs Improvement*  
The Executive Director of the Council should establish and implement appropriate records management policies and procedures to document the decision making process and ensure transparency of the Council's operations. The records management policies and procedures should address the handling and public disclosure of comments related to proposed rulemaking. Management agreed with the recommendation. (1 recommendation)

---

OIG-17-011    11/16    *RESTORE Act: Council Faces Challenges in Establishing its Organizational Infrastructure*  
The Executive Director of the Council should (1) establish and document its information technology system strategic planning process including assigned accountability and responsibility for processes and (2) establish an oversight plan for ensuring information technology contract and interagency service agreements are properly monitored and that services are received and quality is acceptable. Management agreed with the recommendations. (2 recommendations)

---

---

## **Closed Investigations of Senior Government Employees Not Publicly Disclosed**

April 1, 2017 through September 30, 2017

There were no investigations involving senior Government employees that were closed during the period.

---

## **Summary of Instances of Whistleblower Retaliation**

April 1, 2017 through September 30, 2017

There were no established cases of whistleblower retaliation to report for this reporting period.

---

## **Summary of Attempts to Interfere With OIG Independence, Including Instances Where Information or Assistance Request was Refused**

April 1, 2017 through September 30, 2017

There were no attempts made to resist, delay, or restrict OIG access to records or other information and no instances where an information or assistance request was refused during this reporting period.

## Listing of Audit Products Issued

April 1, 2017 through September 30, 2017

In the list of 30 audit products below we identified 4 products that were issued during the reporting period that were not publicly disclosed.

### Office of Audit

*Revenue Collection and Industry Regulation: TTB Appropriately Designates American Viticultural Areas, But Improvements Would Strengthen the Program* (OIG-17-038, 04/3/2017)

*Quarterly Summary Memorandum for the Lead Inspector General, Department of Defense: Operation: Inherent Resolve - Summary of Work Performed by the Department of the Treasury and Office of Inspector General Related to Terrorist Financing, ISIL, and Anti-Money Laundering* (OIG-CA-17-016, 4/4/2017)

*DATA Act Readiness: ARC Is Making Progress in Meeting DATA Act Reporting Requirements Despite Challenges* (OIG-17-039, 4/13/2017)

*TTB Has Strengthened Controls Over Conference, Travel, and Employee Award Administration* (OIG-17-040, 5/1/2017)

*Review of the Gulf Coast Ecosystem Restoration Council's Compliance with the Improper Payments Elimination and Recovery Act of 2010 for FY 2016* (OIG-CA-17-018, 5/2/2017)

*Domestic Assistance-Recovery Act: Audit of Arkansas Development Finance Authority's Payment Under 1602 Program* (OIG-17-041, 5/11/2017)

*Domestic Assistance-Recovery Act: Audit of Rhode Island Housing's Payment Under 1602 Program* (OIG-17-042, 5/11/2017)

*Financial Management: Treasury Did Not Comply with the IPERA Requirements for Fiscal year 2016 Due to the Earned Income Tax Credit Program* (OIG-17-043, 5/12/2017)

*FAEC DATA Act Working Group Frequently Asked Questions* (OIG-CA-17-019, 5/15/2017)

*Terrorist Financing/Money Laundering: Federal Agencies Are Generally Satisfied with TFFC's Collaboration Efforts, but Enhancements Can Be Made* (OIG-17-044, 5/23/2017)

*DATA Act Readiness: Council is Making Progress in Meeting DATA Act Reporting Requirements Despite Challenges* (OIG-17-045, 6/2/2017)

*RESTORE ACT: Gulf County's Policies and Procedures Did Not Reflect All Uniform Guidance Requirements* (OIG-17-046, 6/5/2017)

*Classified Audit Report* (OIG-17-047, 6/5/2017) **Classified, Not Publicly Disclosed**

*Survey Results-Department of the Treasury's Activities to Implement the Cybersecurity Act of 2015* (OIG-CA-17-020, 6/15/2017)

*Quarterly Summary Memorandum for the Lead Inspector General, Department of Defense: Operation Inherent Resolve - Summary of Work Performed by the Department of the Treasury and Office of Inspector General Related to Terrorist Financing, ISIS, and Anti-Money Laundering* (OIG-CA-17-021, 7/5/2017)

*State Small Business Credit Initiative: Oklahoma's Use of Federal Funds for Its Venture Capital Programs* (OIG-17-048, 7/21/2017)

*State Small Business Credit Initiative: Oregon's Use of Federal Funds for Capital Access and Other Credit Support Programs* (OIG-17-049, 7/25/2017) **Questioned Costs \$6,750**

*Termination Memorandum—Audit of the Inventory Fulfillment Center in Plainfield, Indiana, Operated by Pitney Bowes Government Solutions* (OIG-CA-17-023, 7/28/2017)

*Termination Memorandum—Audit of the Mint's Controls Over the Sales of Limited-Production, Investment Grade Products* (OIG-CA-17-024, 7/28/2017)

*Memorandum for the Honorable Eric M. Thorson, Treasury Inspector General: Semiannual Joint Report on Purchase Card Violations for the Period of October 1, 2016 through March 31, 2017* (OIG-CA-17-025, 8/1/2017) **Internal OIG Memorandum, Not Publicly Disclosed**

*Financial Management: Report on the Bureau of the Fiscal Service Administrative Resource Center's Description of its Financial Management Services and the Suitability of the Design and Operating Effectiveness of its Controls for the Period July 1, 2016 to June 30, 2017 (OIG-17-050, 8/23/2017)*

*Contract Audit: Independent Examination Report of WaveFront Technology, Inc.'s Accounting System (OIG-17-051, 8/29/2017) Sensitive But Unclassified, Not Publicly Disclosed*

*Information Technology: 2017 Audit of Treasury's Compliance with the Federal Information Security Modernization Act for its Intelligence Systems (OIG-17-052, 9/13/2017) Classified, Not Publicly Disclosed*

*Financial Management: Report on the Bureau of the Fiscal Service Federal Investments and Borrowings Branch's Description of its Investment/Redemption Services and the Suitability of the Design and Operating Effectiveness of its Controls for the Period August 1, 2016 to July 31, 2017 (OIG-17-053, 9/18/2017)*

*Financial Management: Report on the Bureau of the Fiscal Service Funds Management Branch's Description of its Trust Funds Management Processing Services and the Suitability of the Design and Operating Effectiveness of its Controls for the Period August 1, 2016 to July 31, 2017 (OIG-17-054, 9/18/2017)*

*Terrorist Financing/Money Laundering: FinCEN's 314 Information Sharing Programs Are Useful But Need FinCEN's Attention (OIG-17-055, 9/18/2017)*

*State Small Business Credit Initiative: New York's Use of Federal Funds for Six of Innovate Fund's Venture Capital Funds (OIG-17-056, 9/18/2017)*

*State Small Business Credit Initiative: Rhode Islands' Use of Federal Funds for Its Betaspring Fund 100, LLC Venture Capital Program (OIG-17-057, 9/20/2017) Questioned Costs \$803,644*

*State Small Business Credit Initiative: New Hampshire's Use of Federal Funds for the Borealis Granite Fund, LP (OIG-17-058, 9/28/2017)*

*State Small Business Credit Initiative: Wisconsin's Use of Federal Funds for the Kegonsa Growth Fund, LP (OIG-17-059, 9/28/2017) Questioned Costs \$261,000*

**Council of Inspectors General on Financial Oversight Working Group**

*CIGFO's Corrective Action Verification on the Audit of the Financial Stability Oversight Council's Designation of Market Utilities (CIGFO-2017-002, 5/26/2017)*

*Annual Report of the Council of Inspectors General on Financial Oversight (7/26/2017)*

## Audit Reports Issued With Questioned Costs

April 1, 2017 through September 30, 2017

Category	Total No. of Reports	Total Questioned Costs	Total Unsupported Costs
For which no management decision had been made by beginning of reporting period	0	\$0	\$0
Which were issued during the reporting period	3	\$1,071,394	\$0
Subtotals	3	\$1,071,394	\$0
For which a management decision was made during the reporting period	3	\$1,071,394	\$0
Dollar value of disallowed costs	3	\$1,071,394	\$0
Dollar value of costs not disallowed	0	\$0	\$0
For which no management decision was made by the end of the reporting period	0	\$0	\$0
For which no management decision was made within 6 months of issuance	0	\$0	\$0
Questioned costs include expenditures: (1) that are questioned because of an alleged violation of a provision of a law, regulation, contract, or other requirement governing the expenditure of funds; (2) that, at the time of the audit, are not supported by adequate documentation (i.e., unsupported costs); or (3) used for the intended purpose that are unnecessary or unreasonable.			

## Audit Reports Issued With Recommendations that Funds Be Put to Better Use

April 1, 2017 through September 30, 2017

Category	Total No. of Reports	Total	Savings	Revenue Enhancement
For which no management decision had been made by beginning of reporting period	0	\$0	\$0	\$0
Which were issued during the reporting period	0	\$0	\$0	\$0
Subtotals	0	\$0	\$0	\$0
For which a management decision was made during the reporting period	0	\$0	\$0	\$0
Dollar value of recommendations agreed to by management	0	\$0	\$0	\$0
Dollar value based on proposed management action	0	\$0	\$0	\$0
Dollar value based on proposed legislative action	0	\$0	\$0	\$0
Dollar value of recommendations not agreed to by management	0	\$0	\$0	\$0
For which no management decision was made by the end of the reporting period	0	\$0	\$0	\$0
For which no management decision was made within 6 months of issuance	0	\$0	\$0	\$0
<p>A recommendation that funds be put to better use denotes funds could be used more efficiently if management took actions to implement and complete the recommendation including: (1) reduction in outlays; (2) de-obligations of funds from programs or operations; (3) costs not incurred by implementing recommended improvements related to operations; (4) avoidance of unnecessary expenditures noted in pre-award review of contract or grant agreements; (5) any other savings which are specifically identified; or (6) enhancements to revenues of the Federal Government.</p>				

---

## **Reports for Which No Management Comment was Returned Within 60 Days**

As of September 30, 2017

There were no such reports issued for comment over 60 days as of the end of this reporting period.

---

## **Reports Issued Over 6 Months for Which No Management Decision Has Been Made**

As of September 30, 2017

There were no such reports as of the end of this reporting period.

---

## **Significant Revised Management Decisions**

April 1, 2017 through September 30, 2017

There were no significant revised management decisions during the reporting period.

---

## **Significant Disagreed Management Decisions**

April 1, 2017 through September 30, 2017

There were no significant disagreed management decisions during the reporting period.

---

## Peer Reviews

April 1, 2017 through September 30, 2017

### Office of Audit

Audit organizations that perform audits and attestation engagements of Federal Government programs and operations are required by generally accepted government auditing standards to undergo an external peer review every 3 years. The objectives of an external peer review are to determine, during the period under review, whether the audit organization was complying with its quality control system to provide the audit organization with reasonable assurance that it was conforming to applicable professional standards. Federal audit organizations can receive a peer review rating of *Pass*, *Pass with Deficiencies*, or *Fail*.

The most recent peer review of our office was performed by the Department of Labor (DOL) OIG. In its report dated November 23, 2015, DOL OIG rendered a *Pass* rating for our system of quality control in effect for the year ended March 31, 2015. External audit peer review reports of our office are available on the Treasury OIG [website](#).

OIG did not perform any peer reviews of other Federal audit organizations during this reporting period.

### Office of Investigations

Council of the Inspectors General on Integrity and Efficiency (CIGIE) mandates that the investigative law enforcement operations of all OIGs undergo peer reviews every 3 years to ensure compliance with (1) CIGIE's investigations quality standards and (2) the relevant guidelines established by the Office of the Attorney General of the United States.

In August 2014, the General Services Administration OIG conducted a peer review of our office and found it to be in compliance with all relevant guidelines. The Department of Energy OIG is performing a peer review of our office for the period of April 2014 through July 2017. The review was in progress as of the end of the reporting period.

This page intentionally left blank.

## Other Reporting Requirements and Requests

This section addresses certain reporting requirements of our office that are separate from the reporting requirements in the Inspector General Act of 1978 (as amended).

### Reviews of Bank Failures With Nonmaterial Losses

We conduct reviews of failed bank supervised by the Office of the Comptroller of the Currency (OCC) with losses to the Federal Deposit Insurance Corporation's (FDIC) Deposit Insurance Fund (DIF) that do not meet the definition of a material loss in the Federal Deposit Insurance Act. The reviews are performed to fulfill the requirements found in 12 U.S.C. §1831o(k). The term "material loss" triggers a material loss review if a loss to the DIF exceeds \$50 million (with provisions to increase that trigger to a loss that exceeds \$75 million under certain circumstances). For losses that are not material, the Federal Deposit Insurance Act requires that each 6-month period, the Office of Inspector General (OIG) of the Federal banking agency must (1) identify the estimated losses that have been incurred by the DIF during that 6-month period and (2) determine the grounds identified by the failed institution's regulator for appointing the FDIC as receiver, and whether any unusual circumstances exist that might warrant an in-depth review of the loss. For each 6-month period, we are also required to prepare a report to the failed institutions' regulator and Congress that identifies (1) any loss that warrants an in-depth review, together with the reasons why such a review is warranted and when the review will be completed; and (2) any losses where we determine no in-depth review is warranted, together with an explanation of how we came to that determination.

During this reporting period, there were no failed banks supervised by the OCC with nonmaterial losses to the DIF. There was however, one bank that failed during the period with a material loss to the DIF. Guaranty Bank, Milwaukee, Wisconsin, (d/b/a BestBank in Georgia and Michigan) was closed on May 5, 2017, with an estimated loss to the DIF of \$146.4 million. As of September 30, 2017, the estimated loss to the DIF was \$148.5 million. Our material loss review was ongoing as of the end of the reporting period.

### Operation Inherent Resolve Quarterly Summary Memorandums to the Department of Defense OIG

During this reporting period, we issued two summary memorandums to the Department of Defense OIG regarding information we obtained on the Department of the Treasury's (Treasury) activities with respect to disrupting the Islamic State of Iraq and the Levant's (ISIL) finances. The memorandums included specific examples of activities to disrupt ISIL's financing, information on Treasury's programs that combat terrorist financing, and work we performed or plan to perform to review these programs. **(OIG-CA-17-016, OIG-CA-17-021)**

### Joint Purchase Card Violations Report

The Government Charge Card Abuse Prevention Act of 2012, Public Law 112-194, requires the head of each executive agency with more than \$10 million in purchase card spending annually, and each Inspector General of such an executive agency, on a semiannual basis, to submit to the Director of the Office of Management and Budget (OMB) a joint report on confirmed violations involving misuse of a purchase card by employees of such executive agency and the related disciplinary actions. OMB prescribed the format for the semiannual report, which is transmitted by Treasury to OMB via the OMB Max Portal. We reviewed the report, *Semi-Annual Report on Purchase Card Violations*, for the Department of the Treasury Non-Internal Revenue Service, prepared by Treasury's Office of the Procurement Executive (OPE) for the period of October 1, 2016 through March 31, 2017. The report showed that for the period, Treasury's non-Internal Revenue Service and non-Troubled Asset Relief Program Offices and Bureaus had two confirmed violations involving misuse of a purchase card.

One violation involved purchases made without the availability of funds; that is, the purchases were over the cardholder's monthly cycle limit. The disciplinary action taken was suspension of the cardholder's account until June 7, 2017 (approximately 6 months). In addition, the approving official, who is also the cardholder's supervisor, was informed of the suspension and of the required ratification process should the violation reoccur. The cardholder was also required to attend additional training. The other violation that was under OIG investigation during the reporting period was closed. The violation, which originally occurred in 2009, involved an inappropriate purchase. The cardholder was verbally counseled at the time of the violation in 2009.

The report also stated that there were no violations pending investigation, hearing, final agency action, or decision on appeal. As part of our work to verify the information reported, we inquired of OPE staff about their procedures to identify reportable matters. We also inquired of the OIG Office of Investigations and the Office of Counsel to obtain information on cases of OIG confirmed purchase card violations during the period. OIG Office of Investigations provided us with supplementary information relating to one of the confirmed violations. **(OIG-CA-17-025)**

### **CIGFO's Corrective Action Verification on the Audit of the Financial Stability Oversight Council's Designation of Financial Market Utilities**

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank) created a Council of Inspectors General on Financial Oversight (CIGFO), whose members include the Inspectors General with oversight authority for the majority of the Financial Stability Oversight Council's (FSOC) member agencies. Dodd-Frank authorizes CIGFO to convene a Working Group of its members to evaluate the effectiveness and internal operations of FSOC. In May 2016, CIGFO convened a Working Group to determine whether FSOC had taken corrective actions responsive to the recommendations in CIGFO's July 2013 report.<sup>10</sup>

The Working Group determined that FSOC had taken corrective actions responsive to each of the five recommendations made by CIGFO in its July 2013 report. The Working Group did not make any recommendations to FSOC in the corrective action verification report. **(CIGFO-2017-002)**

---

<sup>10</sup> *Audit of the Financial Stability Oversight Council's Designation of Financial Market Utilities*, (CIGFO-2016-001; issued July 12, 2013)

This page intentionally left blank.

## References to the Inspector General Act

Section	Requirement	Page
Section 4(a)(2)	Review of legislation and regulations	55
Section 5(a)(1)	Significant problems, abuses, and deficiencies	11-46
Section 5(a)(2)	Recommendations with respect to significant problems, abuses, and deficiencies	11-46
Section 5(a)(3)	Significant unimplemented recommendations described in previous semiannual reports	56-62
Section 5(a)(4)	Matters referred to prosecutive authorities	55
Section 5(a)(5)	Summary of instances where information was refused	63
Section 5(a)(6)	List of audit reports	64-67
Section 5(a)(7)	Summary of significant reports	11-46
Section 5(a)(8)	Audit reports with questioned costs	68
Section 5(a)(9)	Recommendations that funds be put to better use	69
Section 5(a)(10)(A)	Summary of each audit, inspection, and evaluation report issued before the beginning of the reporting period for which no management decision was made	70
Section 5(a)(10)(B)	Summary of each audit, inspection, and evaluation report issued for which no management comment was returned within 60 days	70
Section 5(a)(10)(C)	Summary of each audit, inspection, and evaluation report issued before the beginning of the reporting period for which there are outstanding unimplemented recommendations, including the aggregate potential cost savings	56-62
Section 5(a)(11)	Significant revised management decisions made during the reporting period	70
Section 5(a)(12)	Management decisions with which the Inspector General is in disagreement	70
Section 5(a)(13)	Instances of unresolved Federal Financial Management Improvement Act noncompliance	23
Section 5(a)(14)	Results of peer reviews conducted of Treasury OIG by another OIG	71
Section 5(a)(15)	List of outstanding recommendations from peer reviews	71
Section 5(a)(16)	List of peer reviews conducted by Treasury OIG, including a list of outstanding recommendations from those peer reviews	71
Section 5(a)(17)(A-D)	Statistics for the period related to the number of (A) investigative reports issued, (B) persons referred to the Department of Justice for criminal prosecution, (C) persons referred to state and local authorities for criminal prosecution, and (D) criminal indictments/informations	55
Section 5(a)(18)	Description of metrics used to develop investigative statistics in Section 5(a)(17)	55
Section 5a(19)	Summary of each investigation involving a senior Government employee where allegation of misconduct was substantiated	63
Section 5a(20)	Instances of whistleblower retaliation	63
Section 5a(21)	Summary of attempts to interfere with OIG independence	63
Section 5a(22)(A)	Description of each inspection, evaluation, and audit that was closed and not publicly disclosed	64-67
Section 5a(22)(B)	Description of each investigation closed, involving a senior Government employee, that was not publicly disclosed	63
Section 5(d)	Serious or flagrant problems, abuses, or deficiencies	N/A
Section 6(b)(2)	Report to Secretary when information or assistance is unreasonably refused	63

This page intentionally left blank.

## Abbreviations

ADFA	Arkansas Development Finance Authority
AVA	American Viticultural Area
BEP	Bureau of Engraving and Printing
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CISA	Cyber Information Sharing Act of 2015
Council	Gulf Coast Ecosystem Restoration Council
County	Gulf County, Florida
DATA Act	Digital Accountability and Transparency Act of 2014
DIF	Deposit Insurance Fund
FAEC	Federal Audit Executive Council
FinCEN	Financial Crimes Enforcement Network
Fiscal Service	Bureau of the Fiscal Service
FISMA	Federal Information Security Modernization Act of 2014
FSOC	Financial Stability Oversight Council
GAO	Government Accountability Office
IPERA	Improper Payments Elimination and Recovery Act of 2010
IRS	Internal Revenue Service
IRS-CI	Internal Revenue Service Criminal Investigations
Kegonsa	Kegonsa Growth Fund, LP
KPMG	KPMG LLP
McConnell& Jones	McConnell & Jones LLP
Mint	United States Mint
OCC	Office of the Comptroller of the Currency
OIG	Office of Inspector General
OMB	Office of Management and Budget
OSP	Office of Security Programs
Recovery Act	American Recovery and Reinvestment Act of 2009
RESTORE Act	Resources and Ecosystems Sustainability, Tourist Opportunities, and Revived Economies of the Gulf Coast States Act of 2012
RIH	Rhode Island Housing
SF	Standard Form
SSA	Social Security Administration
SSBCI	State Small Business Credit Initiative
TFFC	Office of Terrorist Financing and Financial Crimes
TIGTA	Treasury Inspector General for Tax Administration
Treasury	Department of the Treasury
TTB	Alcohol and Tobacco Tax and Trade Bureau
USPIS	U.S. Postal Inspection Service
USPS	U.S. Postal Service
USSS	U.S. Secret Service
1602 Program	Payments to States for Low-Income Housing Projects in Lieu of Low-Income Housing Tax Credits

This page intentionally left blank.

## **IN THE MIST**



**Pictured above is a view of the North Entrance to the Treasury Building in Washington, DC from the Treasury Annex Alleyway.**

**Source: Treasury Graphics Branch**

## **Treasury Office of Inspector General Locations**

1500 Pennsylvania Avenue, N.W., Room 4436  
Washington, DC 20220

875 15th Street, N.W., Suite 200  
Washington, DC 20005

408 Atlantic Avenue, Room 330  
Boston, Massachusetts 02110



### **Treasury OIG Website**

Access Treasury OIG reports and other information online:

<http://www.treasury.gov/about/organizational-structure/ig/Pages/default.aspx>

### **Report Waste, Fraud, and Abuse**

**OIG Hotline for Treasury Programs and Operations** – Call toll free: 1-800-359-3898

Email: [Hotline@oig.treas.gov](mailto:Hotline@oig.treas.gov)

**Gulf Coast Restoration Hotline** – Call toll free: 1-855-584.GULF (4853)

Email: [GulfCoastRestorationHotline@oig.treas.gov](mailto:GulfCoastRestorationHotline@oig.treas.gov)

Submit a complaint using our online form:

<https://www.treasury.gov/about/organizational-structure/ig/Pages/OigOnlineHotlineForm.aspx>