Semiannual Report to Congress

April 1, 2021 – September 30, 2021
OIG-CA-22-004

Office of Inspector General
Department of the Treasury

Highlights

During this semiannual reporting period, the Office of Audit issued 17 products. Work by the Office of Investigations resulted in 19 indictments and 19 convictions. Some of our more significant results for the period are described below:

- We identified the following lessons learned from monitoring and overseeing the $150 billion Coronavirus Relief Fund (CRF) for Treasury's consideration in implementing and administering American Rescue Plan Act of 2021 programs: (1) the need for clear and timely guidance, (2) the need for agreements with terms and conditions, (3) balancing data reporting & transparency and recipient burden, (4) conducting outreach, and (5) the need for performance measures.
- We issued updates to the *CRF Prime Recipient Quarterly GrantSolutions Submissions Monitoring and Review Procedures Guide* pertaining to CRF reporting.
- Seven of our Office of Investigations agents are assigned to the Pandemic Response Accountability Committee (PRAC) Fraud Task Force on a part-time basis through a memorandum of understanding with the PRAC. The agents are assigned to the Paycheck Protection Program cases while continuing to work their existing caseload.
- Our joint investigation with the Federal Bureau of Investigation, Homeland Security Investigations, and U.S. Postal Inspection Service revealed that five subjects conspired to defraud several financial institutions in a scheme using fraudulent debit card returns resulting in an initial estimated loss of $1.1 million to those institutions. The U.S. Attorney's Office (USAO) for the Eastern District of Virginia sentenced the subjects to 13 months in prison, 13 years of probation, and $1.2 million in criminal restitution.
- Our joint investigation with the Department of Homeland Security Office of Inspector General, the Federal Protective Service, U.S. Customs and Border Protection (CBP), and the Office of Professional Responsibility determined that two subjects stole iPhones that had been seized by CBP. The subjects were sentenced by the USAO, District of New Jersey to 82 months of probation and $225,872 in restitution.

Message from the Acting Inspector General

As we approach the 2-year mark of the declaration of the Coronavirus Disease 2019 (COVID-19) pandemic, the challenges facing the Department of the Treasury (Treasury or the Department) continue to rise, making our oversight more important than ever. Treasury is responsible for leading and implementing economic relief and recovery programs to address the economic challenges precipitated by the COVID-19 pandemic, and we are auditing multiple aspects of Treasury's response to the pandemic.

We also continue to work closely with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and its Pandemic Response Accountability Committee to ensure transparency and accountability of COVID-19 spending, as well as Diversity, Equity, and Inclusion (DE&I) in the Department's programs and operations.

The Treasury OIG team's conduct of rigorous and valuable oversight of Treasury's programs and operations, while carrying out its greatly increased responsibilities in a fully remote work environment, is particularly impressive. This organization has met every challenge it has encountered, served as a responsible steward of the public's funds, and improved Treasury's performance of its missions.

Richard K. Delmar
Acting Inspector General

This page intentionally left blank.

Contents

Treasury Office of Inspector General Overview

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

Treasury OIG performs independent, objective reviews of Treasury programs and operations, except for those of the Internal Revenue Service (IRS), the Troubled Asset Relief Program (TARP), and certain pandemic-related loans, loan guarantees, and other investments, and keeps the Secretary of the Treasury and Congress fully informed of problems, deficiencies, and the need for corrective actions. The Treasury Inspector General for Tax Administration (TIGTA) and the Government Accountability Office (GAO) perform oversight related to the IRS. A Special Inspector General and GAO perform oversight related to TARP. The Special Inspector General for Pandemic Recovery and GAO perform oversight of loans, loan guarantees, and other investments under the Coronavirus Economic Stabilization Act of 2020.

Treasury 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, Treasury 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, Treasury 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.

Treasury OIG has four components: (1) Office of Audit; (2) Office of Investigations; (3) Office of Counsel; and (4) Office of Management. Treasury OIG is headquartered in Washington, DC. Treasury OIG also has an audit office in Boston, Massachusetts.

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, resource management, procurement, alcohol and tobacco excise tax revenue collection activities, SBLF programs, and the State Small Business Credit Initiative (SSBCI) authorized by the American Rescue Plan Act of 2021 (ARP). The second deputy is primarily responsible for financial management and transparency audits to include financial audits of Treasury and the Council performed by Treasury OIG staff and contractors; audits of Government-wide collection, payment, and debt programs and operations; audits of anti-money laundering/terrorist financing, foreign sanctions, and intelligence programs and operations; and audits of Emergency Rental Assistance (ERA) and Homeowners Assistance Fund (HAF) programs authorized by the Consolidated Appropriations Act, 2021 (CAA, 2021) and ARP. The third deputy is primarily responsible for cybersecurity and financial assistance audits to include audits of Treasury and the Council information systems performed by Treasury OIG staff and contractors; RESTORE Act programs and operations; the Coronavirus Relief Fund (CRF) and the Air Carrier Worker Support programs authorized by the CARES Act (as amended); the Emergency Capital Investment Program and the Community Development Financial Institutions Rapid Response Program authorized by the CAA, 2021; and the new State and Local Fiscal Recovery Funds authorized by ARP.

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 within Treasury OIG's jurisdictional boundaries, and investigates threats against Treasury personnel and assets in designated circumstances as authorized by the Inspector General Act. The Office of Investigations also manages the Treasury OIG Hotline to facilitate reporting of allegations involving these programs and operations.

The Office of Counsel, under the leadership of the Counsel to the Inspector General, provides legal advice to the Inspector General and all Treasury OIG components. The office represents Treasury OIG in administrative legal proceedings and provides a variety of legal services, including (1) processing Freedom of Information Act and *Giglio*[1] 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

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

General's signature, cease and desist letters and monetary assessments against persons and entities misusing the Treasury seal and name. The Office of Counsel also responds to media and Congressional inquiries and serves as the Whistleblower Protection Coordinator for Treasury.

The Office of Management, under the leadership of the Assistant Inspector General for Management, provides administrative services to maintain the Treasury OIG administrative infrastructure, including facilities, human resources, information technology, procurement, records management, and security.

Treasury OIG's fiscal year 2021 appropriation was $41 million, which included up to $2.8 million of 2-year funding for the RESTORE Act programs. Treasury OIG's oversight of SSBCI and SBLF programs was funded on a reimbursable basis. In addition to the annual fiscal year appropriation, Treasury OIG received additional multi-year and no-year funding for oversight of pandemic relief programs, which included $35 million for CRF, $9.5 million for ERA, and $2.6 million for HAF programs. As of September 30, 2021, Treasury OIG had 205 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 or the Department) Inspector General annually provide information on the most serious management and performance challenges facing Treasury and the Gulf Coast Ecosystem Restoration Council (Council). The following is a synopsis of our annual assessments which are available, in their entirety, on the Treasury Office of Inspector General (OIG) website.

Treasury

In an October 14, 2021, memorandum to Secretary of the Treasury, Janet Yellen, Acting Inspector General Richard Delmar reported the following six challenges facing the Department, of which one was new.

- Coronavirus Disease 2019 (COVID-19) Pandemic Relief
- Transition of New Administration (new)
- Cyber Threats
- Anti-Money Laundering/Terrorist Financing and Bank Secrecy Act Enforcement
- Efforts to Promote Spending Transparency and To Prevent and Detect Improper Payments
- Information Technology Acquisition and Project Management

Gulf Coast Ecosystem Restoration Council

In an October 8, 2021, letter to the Honorable Michael Regan, Administrator of the U.S. Environmental Protection Agency, as Chairperson of the Council, we reported three challenges, all of which are repeat challenges.

- Loss of Key Leadership Over Administration of Gulf Coast Restoration Activities
- Federal Statutory and Regulatory Compliance
- Grant and Interagency Agreement Compliance Monitoring

.

This page intentionally left blank.

Office of Audit – Significant Audits and Other Products

CARES Act Compliance Monitoring and Oversight

Title VI of the Social Security Act, as amended by Title V of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), established the Coronavirus Relief Fund (CRF) for Treasury to make $150 billion in payments to each of the 50 States, qualifying units of local government, the District of Columbia, U.S. Territories, and Tribal Governments for necessary expenditures due to the public health emergency with respect to the Coronavirus Disease 2019 (COVID-19).The Consolidated Appropriations Act, 2021, extended the covered period for recipients of CRF payments to use funds between March 1, 2020 and December 31, 2021. The CARES Act assigned the Department of the Treasury (Treasury or the Department) Office of Inspector General (OIG) with responsibility for monitoring and oversight of the receipt, disbursement, and use of CRF proceeds.[2] To carry out our monitoring responsibilities, we developed a portal via GrantSolutions, a grants management system under U.S. Department of Health and Human Services, for CRF recipients to report expenditure data on a quarterly basis. To date, CRF data has been collected up to and through September 30, 2021. This data is displayed on the Pandemic Response and Accountability Committee's website (https://www.pandemicoversight.gov/). During this reporting period, we also issued updates to the *CRF Prime Recipient Quarterly GrantSolutions Submissions Monitoring and Review Procedures Guide* pertaining to CRF reporting. **(OIG-CA-20-029R**).

Through our CRF monitoring and oversight work, we identified certain lessons learned with respect to the implementation and administration of the CRF program for Treasury management's consideration in implementing American Rescue Plan Act (ARP) programs.

American Rescue Plan- Application of Lessons Learned From the Coronavirus Relief Fund

We identified certain lessons learned that included, (1) the need for clear and timely guidance, (2) the need for agreements with terms and conditions, (3) balancing data reporting & transparency and recipient burden, (4) conducting outreach, and (5) the need for performance measures.

[2] CRF was established under Title VI of the Social Security Act, as amended by Title V of Division A of the CARES Act, P.L. 116-136 (March 27, 2020)

Accordingly, we recommended that Treasury management (1) finalize guidance concurrent with funds distribution in order to facilitate efficient administration of programs and minimize recipient confusion and misuse of funds; (2) document its analysis of the applicability of grant requirements under 2 CFR [*Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards, 2 CFR Part 200*] for each ARP program in its implementation plan as required by Office of Management and Budget's (OMB) Memorandum M-21-20, *Promoting Public Trust in the Federal Government through Effective Implementation of the American Rescue Plan and Stewardship of the Taxpayer Resources* (March 2021); (3) apply the requirements of 2 CFR to Federal financial assistance funded through the ARP to the maximum extent authorized by law; (4) require signed agreements documenting standard terms and conditions before disbursing ARP funds to recipients; (5) conduct and document an Information Technology investment analysis as required by OMB's M-21-20, OMB Circular No. A-130, *Managing Information as a Strategic Resource* (July 2016) and Circular No. A-11, *Preparation, Submission, and Execution of the Budget* (March 2021) before making the decision to implement the grants Quality Services Management Offices system,[3] GrantSolutions, Salesforce, or another solution for the execution of ARP programs; (6) develop performance metrics to measure the effectiveness of ARP program funding in assisting with pandemic relief goals; and (7) include recipient reporting requirements in written agreements to facilitate this process and ensure that needed information is collected quarterly. Management concurred with our recommendations. **(OIG-CA-21-020)**

[3] OMB's M-19-16, *Centralized Mission Support Capabilities for the Federal Government* (April 26, 2019), describes the process and desired outcomes for shared services and establishes a process for designating agencies as Quality Services Management Offices (QSMO). An agency QSMO offers solutions that, over time, will standardize processes, reduce the technology footprint, and reduce Government-wide operating costs. Once an opportunity for centralization or sharing is identified, OMB will designate a lead agency as the QSMO to take responsibility for establishing and/or managing such capabilities.

Manufacturing

We conduct audits of Treasury's coin programs. We issued the following report during this semiannual period.

Survey of Project Management at the United States Mint

In our survey, we found that it was premature to devote resources to conduct an audit of project management at the United States Mint (Mint) as Treasury had not yet established any Program Management Improvement Accountability Act (PMIAA)[4] guidance for its bureaus and policy offices. PMIAA is intended to improve the quality and effectiveness of program and project management in Federal agencies. There is a 5-year implementation plan from fiscal years (FY) 2018 through 2022 to fulfill the requirements of PMIAA across Treasury, including the development of project management guidance that is scheduled for the first part of FY 2022. After the issuance and implementation of Treasury-wide PMIAA guidance, we plan to reexamine the Mint's project management controls and processes, including compliance with any applicable PMIAA guidance. **(OIG-CA-21-023)**

[4] P.L.114-264, PMIAA (December 14, 2016)

Financial Management

PIIA

An independent certified public accounting firm, RMA Associates (RMA), under a contract monitored by our office, performed an audit of Treasury's compliance with the Payment Integrity Information Act of 2019 (PIIA) for FY 2020. In its audit, RMA also assessed Treasury's compliance with additional improper payment reporting requirements set forth in Executive Order 13520, *Reducing Improper Payments and Eliminating Waste in Federal Programs*, OMB Circular No. A-123, *Appendix C, Requirements for Payment Integrity Improvement*, and OMB Circular No. A-136, *Financial Reporting Requirements*. Our office performed the audit of the Gulf Coast Ecosystem Restoration Council's (Council) compliance with PIIA for FY 2020.

Treasury Compliance with PIIA Fiscal Year 2020

RMA reported that Treasury was not in compliance with PIIA for FY 2020 due to the Internal Revenue Service (IRS) not reporting an improper payment rate of less than 10 percent for three of its programs identified as susceptible to significant improper payments: the (1) Earned Income Tax Credit, (2) American Opportunity Tax Credit, and (3) Additional Child Tax Credit programs. RMA also reported that Treasury complied with 5 of the 6 PIIA requirements: (1) published an Agency Financial Report, (2) conducted a risk assessment, (3) published an improper payment estimate, (4) published corrective action plans, and (5) published and is meeting reduction targets. In addition, RMA noted that the Bureau of the Fiscal Service (Fiscal Service) was unable to provide sufficient documentation to support the quantitative risk assessment performed for the Treasury fund, Fiscal Service – Interest on the Public Debt. RMA also identified that Fiscal Service and Mint managements' responses to some risk assessment questions in several fund group qualitative risk assessments were inaccurate in determining the payment types' susceptibility to significant improper payments.

Accordingly, RMA recommended that (1) Treasury's Risk and Control Group (RCG) works with Fiscal Service management to revise its controls over the review and approval process to verify the quantitative risk assessment includes sufficient supporting documentation to substantiate Fiscal Service's improper payment amount derived from its non-statistical sampling methodology, and that (2) RCG works with Fiscal Service and Mint management to provide evidence of sufficient review and approval on the program-specific risk

assessments indicating management responses to risk assessment questions are complete and accurate. Management concurred with RMA's recommendations. **(OIG-21-028)**

Gulf Coast Compliance with PIIA Fiscal Year 2020

We determined that the Council was compliant with all of the applicable requirements of PIIA for FY 2020. Accordingly, we made no recommendations in this report. **(OIG-21-027)**

Attestation Engagements

Independent certified public accounting firms, Sagger & Rosenburg, P.C. (S&R) and KPMG LLP (KPMG), under contracts monitored by our office, completed the reports described below in support of the audit of Treasury's FY 2021 Consolidated Financial Statements and the financial statement audits of certain other Federal agencies.

Reports on the Processing of Transactions by Treasury Enterprise Business Solutions

S&R examined Treasury Enterprise Business Solutions' description of controls for processing user entities' human resource transactions in its HRConnect system, and the suitability of the design and effectiveness of these controls for the period beginning July 1, 2020 and ending June 30, 2021. S&R found, in all material respects, the controls were fairly presented in the description of controls for this system, suitably designed, and controls tested operated effectively throughout the period. **(OIG-21-029)**

Reports on the Processing of Transactions by Fiscal Service

KPMG examined the accounting and procurement processing and general computer controls related to financial management services provided to various Federal agencies by Fiscal Service's Administrative Resource Center for the period beginning July 1, 2020 and ending June 30, 2021. KPMG found, in all material respects, that the controls were fairly presented in the description of controls for these activities and suitably designed. KPMG also found that controls tested operated effectively throughout the period. **(OIG-21-030)**

Federal Financial Management Improvement Act

The following instances of noncompliance with the Federal Financial Management Improvement Act of 1996 were reported in connection with the audit of Treasury's FY 2020 Consolidated Financial Statements.

Condition	Type of noncompliance
Treasury continues to have deficiencies in IRS financial management systems. Specifically, Treasury did not consistently design, implement, and operate information system controls and security programs over its financial systems in accordance with the Federal financial management systems requirements. (first reported in FY 1997)	Federal financial management system requirements
Treasury has deficiencies in Fiscal Service government-wide cash and Federal debt management information systems. Specifically, Fiscal Service did not consistently design, implement, and operate information system controls and security programs over its cash and Federal debt systems in accordance with the Federal financial management systems requirements. (new reporting in FY 2018)	Federal financial management system requirements

The status of these instances of noncompliance, including progress in implementing remediation plans, will be evaluated as part of the audit of Treasury's FY 2021 Consolidated Financial Statements.

Office of Investigations – Significant Investigations

CARES Act Investigations

Departmental Offices Employee Forwarded Sensitive CARES Act Tribal Data to Another Agency Without Encryption or Confidential Warnings

Our investigation, which was initiated upon receipt of information from Congress and the Department of the Interior Office of Inspector General (OIG), revealed that unencrypted Coronavirus Aid, Relief, and Economic Security Act (CARES Act) tribal data was emailed, without confidential warnings to another Government agency, which contributed to a leak of tribal data. Criminal prosecution was presented and declined by the U.S. Attorney's Office (USAO) for the District of Columbia. Our office provided a report of investigation to Departmental Offices (DO), Office of the Assistant Secretary for Management, and to the concerned members of Congress.

Other Significant Investigations

Debit Card Fraud Conspirators Prosecuted

Our joint investigation with the Federal Bureau of Investigation, Homeland Security Investigations, and U.S. Postal Inspection Service (USPIS) revealed that five subjects conspired to defraud several financial institutions in a scheme using fraudulent debit card returns resulting in an initial estimated loss of $1.1 million to those institutions. The USAO for the Eastern District of Virginia sentenced the subjects to 13 months in prison, 13 years of probation, and $1.2 million in criminal restitution.

Subject Sentenced for Theft of Government Funds and Defrauding a Financial Institution

A final subject in our joint investigation with Internal Revenue Service-Criminal Investigation (IRS-CI), and USPIS was sentenced to 26 months in prison, 96 months of probation, restitution of $283,224, a special assessment of $200, and forfeiture of $60,619. The subject conspired with others and deposited a stolen Department of the Treasury (Treasury or the Department) check, in the amount of $993,176, into a bank account opened in the name of a fictitious business with false identification

documents, and laundered the funds through various other fraudulent business accounts. The USAO for the District of Maryland prosecuted the case.

Subject Sentenced for Theft of Government Property

Our joint investigation with the Department of Homeland Security OIG, the Federal Protective Service, U.S. Customs and Border Protection (CBP), and the Office of Professional Responsibility determined that two subjects stole iPhones that had been seized by CBP. The subjects were sentenced by the USAO, District of New Jersey to 82 months of probation and $225,872 in restitution.

Subject Sentenced for Theft of Thrift Savings Plan Retirement Account Funds

Our joint investigation with the Anne Arundel County Police Department revealed that a subject made a fraudulent $121,000 withdrawal from a victim's Thrift Savings Plan retirement account and directed it into the subjects' own bank account. The subject was sentenced to 10 months in prison, all but 3 months suspended, 60 months of probation, and $86,800 in restitution. The Office of the State's Attorney, Anne Arundel County, Maryland, prosecuted the case.

Honolulu Subject Sentenced for Impersonating a Treasury Agent

Our investigation revealed that an individual participated in an investment fraud scheme and pretended to be a Treasury agent to build credibility with the scheme's victims. The USAO for the District Court of Hawaii sentenced the individual to 60 months of probation, 150 hours of community service, a $100 special assessment, and $7,000 in criminal fines.

Cyber Assist with Stolen OCC Laptop Recovered During Prince Georges County Police Department Search Warrant

Our office, at the request of the Prince Georges County Police Department (PGPD), conducted a forensic examination of a stolen Office of the Comptroller of the Currency (OCC) laptop that PGPD recovered during a search warrant. Our office determined that information on the laptop was not accessed after it was stolen, and subsequently returned the laptop to PGPD for retention in their criminal investigation. PGPD will return the laptop to OCC upon completion of their criminal investigation.

Mismanagement of Loans by Bank Officials

Our joint investigation with the Federal Deposit Insurance Corporation and the Board of Governors of the Federal Reserve OIGs substantiated an allegation received by OCC that bank officials used inaccurate record keeping and diverted loan proceeds to pay other troubled non-performing loans and unrelated parties. Due to the age of the case and repaid loans, the USAO, Northern District of Illinois declined prosecution.

Allegations of Circumventing Policies and Practices Related to OCC Redlining Investigations Were Unsubstantiated

Our investigation, initiated upon receipt of information from members of Congress, that OCC engaged in a pattern of scuttling investigations related to civil rights and redlining in violation of its statutory responsibility determined that the allegations were unsubstantiated. Our office provided a response to the concerned members of Congress.

Allegation of Fraudulent Billing of Hours by Government Contractor Was Unsubstantiated

Our office initiated an investigation of an anonymous complaint involving the fraudulent billing of hours by a government contractor. It was alleged that the contractor's employees frequently showed up late for work and took long lunches. Our investigation determined that the contractor's employees were not full-time employees, but part-time and were only paid for the hours they worked.

Cease and Desist Letter Issued for Fraudulent Treasury Website

Our office initiated an investigation after being notified of a fraudulent Treasury website. Our investigation did not conclusively reveal the positive identity of the subscriber. Criminal prosecution was presented and declined by the USAO for the District of Maryland. Treasury sent a Cease and Desist letter to the domain registrant to take down the domain.

Prosecution of Former Departmental Offices Employee for Removing and Transmitting Classified Information Declined

Our office initiated an investigation after being notified of an allegation that a former DO employee removed classified documents from a Sensitive Compartmented

Information Facility without authorization, and emailed the classified documents to an individual without a need to know or clearance to access the information over an unsecured means of communication. The alleged disclosure occurred several months after DO removed the former employee for misconduct. Criminal prosecution of the former employee was declined by both the USAOs for the District of Columbia and the Eastern District of Virginia.

Bureau of the Fiscal Service Defended Against Automated Data Mining of Its Treasury Check Verification System Web Application by Implementing CAPTCHA

Our office investigated suspicious activities associated with the Bureau of the Fiscal Service (Fiscal Service) Treasury Check Verification System (TCVS). TCVS is a public website used to query Treasury check serial numbers and amounts. Our review of 7.5 million TCVS requests over a 3-week time period found that computer scripted queries appear to have targeted dollar amounts associated with Economic Impact Payments. The majority of the requests came from non-U.S. Internet Protocol addresses. Fiscal Service added an additional security feature called CAPTCHA, which is a computer test to determine whether or not the requestor is a human, effectively mitigating the automated data mining of TCVS.

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

Final Subjects Sentenced for Conspiracy to Defraud the Government and Aggravated Identity Theft

As reported in a previous semiannual period, our joint investigation with the IRS-CI determined a subject in Pennsylvania was involved in a fraud scheme to illicitly procure and negotiate Treasury checks. The subject, who owned two money service businesses, was linked to approximately $10 million in potential fraud related to stolen Treasury checks and a stolen identity refund fraud scheme. The subject pled guilty to Conspiracy to Defraud the Government in the U.S. District Court of the Middle District of Pennsylvania, and forfeited $2 million. Investigative efforts continued and the remaining three co-conspirators were located and arrested. The three additional subjects pled guilty to Conspiracy to Defraud the Government with respect to claims

and aggravated identity theft in the U.S. District Court of the Middle District of Pennsylvania.

Update: The final three subjects were charged by the USAO in the U.S. District Court of the Middle District of Pennsylvania, with conspiring to defraud Treasury by producing multiple fraudulent Federal income tax returns using stolen identities and receiving over $5 million in fraudulent funds. The subjects were sentenced to 16 years in prison, 9 years of probation, and $5 million in restitution and civil judgments

This page intentionally left blank.

Treasury OIG Accomplishments and Activities

PRAC Fraud Task Force

Earlier this year, the Pandemic Response Accountability Committee (PRAC) stood up a Fraud Task Force to serve as a resource for the Inspectors General (IG) community by merging investigative resources into those areas where the need is the greatest, currently pandemic loan fraud. Agents from Offices of Inspectors General (OIG) across the Government are detailed to work on Task Force cases. These agents have partnered with prosecutors at the Department of Justice's Fraud Section and at United States Attorneys' Offices across the country.

The idea behind the PRAC Fraud Task Force is to harness the expertise of the oversight community and attack this problem with every tool available: criminal, civil, forfeitures of money and property, suspension and debarments. The Task Force works closely with other initiatives to combat pandemic fraud such as the Department of Justice Coronavirus Disease 2019 (COVID-19) Fraud Enforcement Task Force.

Department of the Treasury (Treasury or the Department) OIG has seven agents who are assigned to the PRAC Fraud Task Force on a part-time basis. The PRAC has extended its authority to investigate pandemic-related fraud to Treasury OIG through a memorandum of understanding. The agents are assigned Paycheck Protection Program cases while continuing to work their existing Treasury OIG caseload. This initiative allows Treasury OIG to make a broader contribution to the IG community by assisting with investigations that might otherwise remain unstaffed.

Treasury OIG Leadership Roles

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

Deborah Harker, Assistant Inspector General for Audit, serves as the Co-Chair of the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Federal Audit Executive Council's Digital Accountability and Transparency Act (DATA Act) Working Group Governance Committee. **Ms. Harker** also represents CIGIE on the Chief Financial Officers Council, Leveraging Data as a Strategic Asset Working Group. In addition, **Ms. Harker** represents Treasury OIG on the National Association of State Auditors, Comptrollers, and Treasurers COVID-19 Accountability Work Group.

Pauletta Battle, Deputy Assistant Inspector General for Financial Management and Transparency Audits, chairs the Federal Audit Executive Council's DATA Act Working Group, which educates Inspectors General and Government financial communities on the DATA Act oversight process. The Working Group consists of approximately 200 members representing at least 48 OIGs.

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 American Institute of Certified Public Accountants' (AICPA) National Governmental Accounting and Auditing Update Conference planning committee. **James Hodge,** Audit Director, also serves with **Ms. Joseph** on the AICPA National Governmental Accounting and Auditing Update Conference planning committee.

Statistical Summary

Summary of Treasury OIG Activities

April 1, 2021 through September 30, 2021

OIG Activity	Number or Dollar Value
Office of Counsel Activities	
Regulation and legislation reviews	29
Instances where information was refused	0
Office of Audit Activities	
Reports issued and other products	17
Disputed audit recommendations	0
Significant revised management decisions	0
Management decision in which the Inspector General disagrees	0
Monetary benefits (audit)	
Questioned costs	$0
Funds put to better use	$0
Total monetary benefits	$0
Office of Investigations Activities*	
Criminal and judicial actions (including joint investigations)	
Investigative reports issued	164
Cases referred for prosecution and/or litigation	33
Individuals referred for criminal prosecution to the Department of Justice	36
Individuals referred for criminal prosecution to state and local authorities	2
Cases accepted for prosecution and/or litigation	5
Arrests	1
Indictments/informations	19
Convictions (by trial and plea)	19

**During the reporting period defendants were sentenced to 683 months of prison time, 1,272 months of probation, 7 months suspended, 108 months of home detention, 19 days of community service and ordered to pay fines, restitution, and court fees in the amount of $5.1 million, and seizures and forfeitures in the amount of $500,114.*

Metrics Used for Office of Investigations Activities

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

Reports with Unimplemented Recommendations

Issued prior to April 1, 2021

The following list of Treasury OIG reports with unimplemented recommendations is based on information in Treasury's automated audit recommendation tracking system, which is maintained by Treasury management officials, and recommendations tracked by other Federal organizations related to Treasury 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.

Treasury OIG is reporting 138 open and unimplemented recommendations for 25 reports issued prior to April 1, 2021, with $2,550 in potential monetary benefits. Treasury OIG considers all unimplemented recommendations for reports issued over 6 months to be significant.

Treasury Programs and Operations

Fiscal Year	Report Number	Report Title	Date Issued
2016	OIG-16-059	***General Management: Treasury Has Policies and Procedures to Safeguard Classified Information but They Are Not Effectively Implemented***	09/16
1.	The Assistant Secretary for Intelligence and Analysis should direct the Deputy Assistant Secretary for Security to update the Treasury Security Manual to include procedures requiring the Office of Security Programs to follow up and obtain all bureau self-inspection reports. Management agreed with the recommendation.		

Fiscal Year	Report Number	Report Title	Date Issued
2018	OIG-18-018	*Terrorist Financing/Money Laundering: OFAC Human Resources Practices Need Improvement*	11/17
1.	The Office of Foreign Assets Control (OFAC) Director should ensure that legacy employees' current position descriptions are evaluated to ensure that the documented promotion potential of these non-supervisory employees is consistent with OFAC's current promotion practices. Management agreed with the recommendation.		
Fiscal Year	**Report Number**	**Report Title**	**Date Issued**
2018	OIG-18-043	*Terrorist Financing/Money Laundering: OFAC's Licensing Program Would Benefit From System Enhancements*	04/18
1.	The Director of OFAC should develop performance measures specific for the licensing division. Management agreed with the recommendation.		
Fiscal Year	**Report Number**	**Report Title**	**Date Issued**
2018	OIG-18-044	*Terrorist Financing/Money Laundering: Audit of the Office of Intelligence and Analysis' Authorities and Actions Related to U.S. Persons' Financial Information*	04/18
1.	The Under Secretary for Terrorism and Financial Intelligence, as expeditiously as possible, should ensure that the Office of Intelligence and Analysis's (OIA) U.S. Persons Procedures are finalized and submitted for approval to the Attorney General of the United States.		
2.	Implement a compliance monitoring program to assess whether intelligence analysts' activities are conducted in accordance with OIA authorities, and electronic searches and other queries are performed in a manner that fully protects the rights of U.S. persons. Management agreed with the		

	recommendations.		
Fiscal Year	**Report Number**	**Report Title**	**Date Issued**
2019	OIG-19-007	***Information Technology: Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2018 Performance Audit***	10/18
1.	Treasury Inspector General for Tax Administration (TIGTA) management should establish a current enterprise baseline of software and related configurations for the TIGTA System.		
2.	Develop and disseminate to TIGTA personnel a TIGTA System Information System Contingency Plan that addresses purpose, scope, roles, responsibilities, management commitment, coordination, and compliance to facilitate the implementation of the contingency planning policy and associated contingency planning controls. TIGTA should conduct disaster recovery and business continuity testing for the TIGTA System on the frequency stipulated by a Business Impact Analysis. Management agreed with the recommendations.		
Fiscal Year	**Report Number**	**Report Title**	**Date Issued**
2019	OIG-19-040	***DATA Act: Treasury's Efforts to Increase Transparency Into Federal Spending Continue, But Further Refinement is Needed***	07/19
1.	The Fiscal Assistant Secretary should enhance generic disclaimers on USAspending.gov and expand the use of limitation statements on pages with known and potential display issues so that the public has a clear understanding of known limitations when using the data as displayed and available for download. Management agreed with the recommendation.		

Fiscal Year	Report Number	Report Title	Date Issued
2020	OIG-20-002	***Information Technology: Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2019 Performance Audit for Collateral National Security Systems (Sensitive but Unclassified)***	10/19
1.	This recommendation is Sensitive But Unclassified. Management agreed with the recommendation.		

Fiscal Year	Report Number	Report Title	Date Issued
2020	OIG-20-003	***Information Technology: Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2019 Performance Audit***	10/19
1.	The Bureau of Engraving and Printing (BEP) management should assess and remediate vulnerabilities identified during Security Content Automation Protocol configuration baseline compliance and vulnerability scanning within the required timeframes specified in the BEP Minimum Standard Parameters.		
2.	Departmental Offices (DO) management should develop and implement a process to ensure that periodic user access reviews are completed for DO System 2, documented, and all unnecessary access is removed in accordance with National Institute of Standards and Technology Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53, Rev. 4) and Treasury Directive Publication 85-01, *Department of the Treasury Information Technology Security Program* (TD P 85-01).		
3.	Bureau of the Fiscal Service (Fiscal Service) management should protect the confidentiality and integrity of transmissions by encrypting Fiscal Service System 2 data in transit as required by NIST 800-53, Rev. 4.		
4.	United States Mint (Mint) management should establish a quality control		

	process to ensure that user access to Mint System 1 and other Mint information systems follow the access management process requiring the completed background investigations, signed non-disclosure agreements, signed rules of behavior, and completion of the security awareness training.
5.	Mint management should clearly document and formally approve exemptions to the Mint's access authorization process when a business justification exists. Management agreed with the recommendations.

Fiscal Year	Report Number	Report Title	Date Issued
2020	OIG-20-007	***DATA Act: Treasury Continues to Make Progress in Meeting its DATA Act Reporting Requirements***	11/19
1.	Treasury's Assistant Secretary for Management (ASM), working as needed with Treasury's Senior Accountable Official, the Senior Procurement Executive, reporting entities, the Program Management Office, and the Office of Management and Budget (OMB) should develop and implement a method and procedures to submit Treasury Forfeiture Fund financial assistance award data to the Financial Assistance Broker Submission in accordance with the reporting submission specifications established by the Digital Accountability and Transparency Act (DATA Act) Information Model Schema. Management agreed with the recommendations.		

Fiscal Year	Report Number	Report Title	Date Issued
2020	OIG-20-022	***Financial Management: Management Report for the Audit of the Department of the Treasury's Consolidated Financial Statements for Fiscal Years 2019 and 2018***	12/19
1.	Fiscal Service management should address the mainframe operating system vulnerabilities noted in the condition as soon as possible.		
2.	Develop a tailored mainframe operating system security configuration baseline that specifies how security configuration options are to be set based on the selected industry guidance.		

3.	Ensure that the chief information security officer assign specific responsibility for providing controls over operating system security, including access permissions to all system datasets and all security-related option settings.
4.	Develop and document controls over changes and monitor update access to all key system datasets.
5.	Develop and document controls and baseline documentation of mainframe operating system options specified in the configuration files.
6.	Establish which techniques are to be used to control update access to key system datasets and to control read access to sensitive system datasets (such as the security software database and the page files), whether a third-party tool is to be used, or tailored change control mechanisms, and develop procedures and documentation to support their use.
7.	Develop procedures to provide assurance that programs installed with the privileges of the operating system (whether purchased from software vendors or internally developed) do not introduce security weaknesses.
8.	Develop, document, and implement policies, procedures, and controls to conduct periodic reviews of actual mainframe security software settings against the security baseline.
9.	Develop a mainframe security software risk assessment process using the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) as a guideline.
10.	Develop a tailored mainframe security software configuration baseline that specifies how security configuration options should be set based on the industry guidance. As part of this action, management should develop and document a baseline specifying for each possible setting in the security software control file how the option should be set and who is responsible for approving the setting.
11.	Use the mainframe security software configuration baseline to harden the mainframe environment, including the Payment Authorization Manager and Payments, Claims, and Enhanced Reconciliations production.

12.	Remove duplicate and excessive permissions in the mainframe security software database.
13.	Perform an annual comparison of each actual setting in the mainframe security software control file to each setting specified in the baseline to verify compliance with the baseline.
14.	Develop and document procedures for controlling updates to the mainframe security software control file.
15.	Define and document the segregation of functions and privileges based on the principle of least privilege for mainframe security software and operating system.
16.	Review and establish access permissions to the mainframe system and security software based on the principle of least privilege access.
17.	Review and re-assess each access permission in the mainframe security software dataset and resource rules on a periodic basis.
18.	Develop procedures and documentation to establish the following for each dataset permission, resource permission, and mainframe security software privilege: a. Responsibility for approving access and enforcing compliance with the principle of least privilege; b. Actual access meets the principle of least privilege; and c. Any discrepancy from approved access will be identified and corrected.
19.	Develop, document, and implement policies, procedures, and controls for comprehensive logging and monitoring of events. Procedures and controls should include an annual re-assessment of whether logging and reporting is adequate.
20.	Review and determine which profiles, applications, databases, and other processes on the mainframe will be logged and reviewed.
21.	Assess all mainframe logs to determine which logs should be evaluated by the incident management tool.
22.	Establish appropriate alerts and event thresholds for those mainframe logs required to be evaluated by the external tracking tool.

23.	Develop and implement data and analysis tools and processes for identifying event trends, patterns, spikes, and exceptions.
24.	Identify non-security related purposes for logging and monitoring (including performance tuning, problem management, capacity planning, and management of service level agreements); assign responsibility for addressing and integrating them with security uses of logging and monitoring.
25.	Identify the possible sources of log information; determine how each is to be used for security monitoring; and develop procedures to ensure that each type of logging which is necessary for effective security monitoring is activated.
26.	Annually assess the effectiveness of security logging and monitoring, ensuring that the volume of logged events is limited to just those that are needed for security, and ensuring that monitoring results include effective identification and response for any violations and for any significant trends (such as an increase in the number of password resets for a given group of users or repetition of the same attempted but failed attempt to access a productions dataset or resource).
27.	Identify, document, and assess the mainframe security controls affecting the system software to fully describe how mainframe security is provided. These Fiscal Service management controls should include: a. Specific assignment of responsibility for maintaining operating security, b. Skill assessment and remediation for operating system security maintenance, c. Baseline documents for mainframe configuration files, d. Standard procedures for review and maintenance of operating system security, and e. Standard procedures to compare actual configuration settings to baseline documents.
28.	Update mainframe documentation to be consistent with Fiscal Service and TD P 85-01.
29.	Develop procedures and documentation to establish who is responsible and how effective security is achieved for controls.
30.	Implement an oversight process to determine that designated Fiscal Service personnel review and reevaluate privileges associated with the UNIX

	production environment semiannually for privileged accounts.
31.	Configure the systems-management software agents to include all UNIX servers, databases, and users' accounts within the UNIX environment when generating the users' lists for the semiannual review and recertification process so that all privileged and non-privileged users' access is reviewed.
32.	Update UNIX semiannual account review and recertification procedures to include quality control steps to validate that systems-management software is generating complete and accurate account listings for all UNIX servers and databases privileged and non-privileged user accounts within the UNIX environment prior to completing the review and recertification process.
33.	Finalize policies and procedures to review audit logs of production DB2 servers.
34.	Implement an oversight process to ensure that designated Fiscal Service personnel: a. Review the security logs for the UNIX and DB2 servers hosting the Payment Information Repository (PIR), Judgment Fund Internet Claim System (JFICS), and Security Payment System (SPS) applications on a pre-defined frequency, as indicated in the Fiscal Service Baseline Security Requirements (BLSR). b. Formally document completion of their reviews and any escalations to the Information System Security Office, and c. Retain the audit logs and documentation of their reviews for 18 months, as required by the BLSR.
35.	Periodically review Fiscal Service management's implementation and operation of the review of the security audit logs for the UNIX and DB2 servers hosting the PIR, JFICS, and SPS applications to determine that Fiscal Service management completes the reviews on a pre-defined basis, documents completion of the reviews and escalations, and maintains such documentation.
36.	Establish an effective enforcement process or mechanism to ensure that (a) UNIX and DB2 events and monitoring controls are followed and (b) Fiscal Service management has confidence it consistently reviews for potential unauthorized or inappropriate activity.
37.	Update its current PIR security procedures to require that management obtain current PIR developer access requirement listings from the service provider and use them when validating the appropriateness of PIR developer

	access during the semiannual access reviews and recertification of the PIR and UNIX environments.
38.	Maintain the documentation used to review and recertify the access of the known PIR service provider developers evidencing that their access to the UNIX environments is commensurate with their job functions and responsibilities.
39.	Ensure that developers do not have the ability to make changes to the PIR production environment.
40.	Remove users' access once validated by the Federal Program Agency (FPA) during the SPS annual user access review.
41.	Retain evidence of recertification of all users.
42.	Oversee the recertification process and ensure that access corrections are processed once received from the FPA.
43.	Review and enhance the manual processes and procedures to ensure that user access to all resources, as defined for Treasury Web Application Infrastructure (TWAI) users, is accurately and completely identified and evaluated during the course of the General Support System 1 (GSS1) and General Support System 2 (GSS2) TWAI User Privilege Recertification cycles.
44.	Complete the GSS1 TWAI User Access Recertification cycle within the time intervals set by Fiscal Service BLSR requirements.
45.	Remove and disable the two users' access immediately.
46.	Implement a quality control process to ensure that PIR application accounts defined to the PIR production environment that have been inactive for over 120 days are disabled.
47.	Review and update the Enterprise Information Technology Infrastructure System Security Plans (SSP), Attachment A-Security Control Matrix, to be consistent with the Fiscal Service BLSR and the Chief Information Officer Publication Information System Security Internal Standard Operating Procedure 8.3.6.60 UNIX/LINUX Account Management.

48.	Configure the six UNIX servers to enforce the minimum password as stated in the Fiscal Service BLSR and ensure that the default password configuration settings for the production UNIX environments comply with the minimum requirements specified in the BLSR.
49.	Develop and implement a quality control process to ensure that PIR emergency change approvals are consistently obtained, documented, and retained by the Change Control Board prior to implementing changes into the PIR production environment.
50.	Develop and implement documentation to assign responsibility for ensuring adequacy of UNIX and database security and baseline settings.
51.	Update existing UNIX and database configuration security baseline documents to ensure that these documents fully incorporate and enforce the components of the DISA STIG. Management should document any deviations from the STIG and note compensating controls that mitigate the security risk to an acceptable level.
52.	Develop, document, and implement policies, procedures, and controls to conduct periodic reviews of actual UNIX and database settings against the security configuration baselines.
53.	Provide logging and monitoring of security related events to include the retention of evidence of reviews performed.
54.	Develop a baseline of essential security settings and specify that baseline as the standard to be observed.
55.	Implement corrective actions to address all vulnerabilities associated with the baseline enforcement to include removing the three default user accounts on UNIX servers. Management agreed with the recommendations.

Fiscal Year	Report Number	Report Title	Date Issued
2020	OIG-20-023	*BILL AND COIN MANUFACTURING: BEP Improved Governance and Oversight over Note Development and Production But Challenges Remain*	12/19
1.	The Director of the BEP should finalize the required 5 year update of the memorandum of understanding with the Board of Governors of the Federal Reserve System (Board) to formalize BEP and the Board's responsibilities and authorities related to notes including activities, procedures, and obligations related to the annual production, destruction, and research and development of notes. Management agreed with the recommendation.		
Fiscal Year	**Report Number**	**Report Title**	**Date Issued**
2020	OIG-20-027	*Resource Management: Audit of the Department of the Treasury Departmental Offices Executive Pay Adjustments, Bonuses, and Awards*	02/20
1.	The ASM should ensure that the Office of the Deputy Assistant Secretary for Human Resources and Chief Human Capital Officer (DASHR/CHCO) and the Office of Executive Resources (OER) develop, implement, and include effective internal controls within its policies and standard operating procedures (SOP) to ensure Treasury's Senior Executive Service (SES) basic pay rates are in compliance with 5 CFR 534.403(a)(3)(b), *Suspension of certification of performance appraisal system* and 5 CFR 534.404 (h)(2), *Setting pay upon transfer*.		
2.	DASHR/CHCO and OER calculate the overpayment amounts for the two DO SES members whose pay was set higher than allowed by regulation.		
3.	DASHR/CHCO and OER seek recovery of the overpayment amounts or exercise the authority to waive any claim in accordance with applicable Federal regulations and Treasury's Directive 34-01, *Waiving Claims Against Treasury Employees for Erroneous Payments.*		

4.	DASHR/CHCO and OER complete Office of Personnel Management (OPM) data calls in accordance with OPM's applicable instructions and guidance to ensure all required employees, such as those who have left Treasury, are properly reported.
5.	DASHR/CHCO finalizes and approves Treasury's SES Pay and Awards policy, and then periodically reviews it for continued relevance, effectiveness, and transparency in making pay decisions and awarding bonuses, assesses staffing levels, workforce skills, and respective budgets to determine whether additional personnel should and can plausibly be incorporated into future strategic planning to ensure OER can meet its goals and mission.
6.	DASHR/CHCO finalizes and approves Treasury's SES Pay and Awards policy, and then periodically reviews it for continued relevance, effectiveness, and transparency in making pay decisions and awarding bonuses.
7.	OER documents the processes and SOP, with appropriate detail, followed in administering Treasury DO SES member performance ratings, pay adjustments, and bonuses.
8.	OER oversees the process regarding exceptions to the 12-month rule.
9.	OER includes information regarding the approval process for waiver requests for exceptions to the 12-month rule in the instructions provided to bureau heads and DO policy offices. This information should be consistent with Federal regulations and Treasury's SES Pay and Awards policy.
10.	OER submits Treasury's respective data call report to OPM by the due dates established by 5 CFR 534.405, *Performance awards*, and before any established deadlines per OPM's annual data call memorandum. Management agreed with the recommendations.
Questioned Cost	$2,550

Fiscal Year	Report Number	Report Title	Date Issued
2020	OIG-20-029	*Gulf Coast Restoration: Jefferson Parish's Internal Control over Federal Awards*	03/20
1. & 2.	The Fiscal Assistant Secretary should ensure that deficiencies identified in Jefferson Parish, Louisiana's (Jefferson Parish) controls over Federal awards are considered as part of the Treasury's oversight of future awards as well as risk assessments of Jefferson Parish as required by the *Uniform Administrative Requirements, Cost Principals, and Audit Requirements for Federal Awards* (2 CFR Part 200) (Uniform Guidance). This recommendation is counted as two recommendations because it applies to both findings in the report. Management agreed with the recommendations.		
Fiscal Year	**Report Number**	**Report Title**	**Date Issued**
2020	OIG-20-030	*Bill and Coin Manufacturing: The United States Mint Numismatic Order Management System is Meeting User Needs But Improvements to Oversight are Needed*	03/20
1.	The Mint Director ensures the Numismatic and Bullion Directorate retains evidence of its monitoring activities outlined in the contract's Quality Assurance Surveillance Plan to better document the Mint's oversight of the contractor's compliance with contract requirements.		
2.	Perform an assessment regarding the impact of not having language accessibility for Mint's numismatic program services and considers adding these services to the Mint's Order Management System.		
3.	Perform analyses to determine the feasibility and potential impact of proposed actions to improve numismatic sales, perform additional studies to enhance future sales, and report the results to stakeholders. Management agreed with the recommendations.		

Fiscal Year	Report Number	Report Title	Date Issued
2020	OIG-20-036	*Interim Audit Update – Coronavirus Relief Fund Recipient Reporting*	05/20
1.	Treasury management should support our office in accomplishing our monitoring and oversight responsibilities in the following ways: (1) assist in communications with Coronavirus Relief Fund (CRF) recipients on matters that include, but are not limited to, communications of reporting and record keeping requirements and other audit inquiries, as needed; (2) ensure that Treasury maintains communication channels with recipients to obtain and address post payment inquiries regarding specific payments; and (3) continue to update CRF guidance and disseminate to recipients as needed. Management agreed with the recommendation.		
Fiscal Year	Report Number	Report Title	Date Issued
2020	OIG-20-040	*BILL AND COIN MANUFACTURING: Audit of Bureau of Engraving and Printing's Implementation of Security Features and Meaningful Access for the Blind and Visually Impaired into New Note Design*	06/20
1.	The Director of BEP in collaboration, as necessary, with members of the United States Currency Program: Continue to improve the Banknote Development Process and Technology Development Process guidance, including refining procedures to reflect lessons learned during its Catalyst note series redesign.		
2.	Ensure the Advanced Counterfeit Deterrence Steering Committee charter is updated in a timely manner, and as needed, to ensure roles, responsibilities, and current practices, such as the attendance of Advanced Counterfeit Deterrence Steering Committee monthly meetings by appropriate personnel, are clearly defined and communicated to its members. Management agreed with the recommendations.		

Fiscal Year	Report Number	Report Title	Date Issued
2020	OIG-20-042	*MANUFACTURING AND REVENUE: Mint Controls Over Raw Materials and Coin Exchange Programs Need Improvement*	08/20
1.	The U.S. Mint Director should conduct regular reviews of the suppliers' quality systems to ensure that the suppliers are acting in the best interest of the Mint. This includes regular site visits or periodic reviews of the suppliers' quality system documentation.		
2.	Develop and implement SOPs that are consistent among Mint facilities to ensure quality assurance processes over sampling, inspection, and testing of materials for circulating coinage are standardized and documented; and that materials received meet the specifications required in the contracts and by U.S. law.		
3.	Consider sampling and testing the material after blanking in order to assess the material quality throughout the coil.		
4.	Verify incoming raw material weights to ensure that the Mint is receiving the raw materials paid for.		
5.	Strengthen and finalize SOPs for all coin exchange programs before accepting any redemptions. This would include using tests and subject matter experts to authenticate the genuineness of coins redeemed, as well as working with the Board to develop appropriate interagency procedures to assure the integrity of the coin redemption process for uncurrent coins.		
6.	Follow all SOPs, including but not limited to, procedures related to sampling, inspecting, and testing coins; and appropriately document redemptions. Additionally, ensure that adequate background investigations are conducted on bulk redeemers and decisions to allow participation into the Mutilated Coin Redemption Program are based on relevant data from the background investigation. The Mint should add criteria, such as obtaining financial statements for analyses of the potential bulk redeemers and performing site visits at their premises, as part of the background investigation process for entry into the program. The Mint should document how this criteria was met, and if these steps were not performed, the		

	reasons why.		
7.	Ensure that all coins returned to the Mint and removed from circulation are destroyed timely and sufficiently accounted for. Management agreed with the recommendations.		
Fiscal Year	**Report Number**	**Report Title**	**Date Issued**
2021	OIG-21-009	***INFORMATION TECHNOLOGY: Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2020 Performance Audit (Sensitive But Unclassified)***	11/20
1.	This recommendation is Sensitive But Unclassified.		
2.	This recommendation is Sensitive But Unclassified.		
3.	This recommendation is Sensitive But Unclassified.		
4.	This recommendation is Sensitive But Unclassified. Management agreed with the recommendations.		
Fiscal Year	**Report Number**	**Report Title**	**Date Issued**
2021	OIG-21-010	***INFORMATION TECHNOLOGY: Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2020 Performance Audit for Collateral National Security Systems (Sensitive But Unclassified)***	11/20
1.	This recommendation is Sensitive But Unclassified.		
2.	This recommendation is Sensitive But Unclassified.		
3.	This recommendation is Sensitive But Unclassified.		
4.	This recommendation is Sensitive But Unclassified.		

5.	This recommendation is Sensitive But Unclassified.
6.	This recommendation is Sensitive But Unclassified.
7.	This recommendation is Sensitive But Unclassified.
8.	This recommendation is Sensitive But Unclassified.
9.	This recommendation is Sensitive But Unclassified. Management agreed with the recommendations.

Fiscal Year	Report Number	Report Title	Date Issued
2021	OIG-21-012	***FINANCIAL MANAGEMENT: Management Letter for the Audit of the United States Mint's Financial Statements for Fiscal Years 2020 and 2019***	12/20
1.	Mint management should re-enforce requirements to control performers to ensure that new or modified user accounts are approved prior to being enabled and that documentation supporting the approval is retained.		
2.	Enforce termination and transfer procedures to remove system access of terminated or transferred employees and contractors in a timely manner from the network and applications managed by the Mint or by its service providers.		
3.	Implement and enforce procedures that include a timeframe requirement for notifying service providers, such as the Administrative Resource Center, of terminated or transferred Mint employees and contractors, so that their access can be removed from applications hosted or managed by the service organizations in a timely manner. Management agreed with the recommendations.		

Fiscal Year	Report Number	Report Title	Date Issued
2021	OIG-21-013	*FINANCIAL MANAGEMENT: Audit of the Office of D.C. Pensions' Financial Statements for Fiscal Years 2020 and 2019*	12/20
1.	Office of D.C. Pensions management should fully develop existing policies and procedures to document a process for reviewing, investigating, and resolving unusual or suspicious activity identified during the audit log review, as well as maintaining evidence of such review, investigation, and resolution. Management agreed with the recommendation.		
Fiscal Year	**Report Number**	**Report Title**	**Date Issued**
2021	OIG-21-019	*FINANCIAL MANAGEMENT: Audit of the Department of the Treasury's Consolidated Financial Statements for Fiscal Years 2020 and 2019*	12/20
1.	The ASM and Deputy Chief Financial Officer should ensure that Fiscal Service implement requisite corrective actions to resolve control deficiencies over its cash management and debt information systems.		
2.	Ensure that the Internal Revenue Service (IRS) implements corrective actions to resolve its control deficiencies.		
3.	Ensure that IRS and Fiscal Service develop and implement remediation plans outlining actions to be taken to resolve noncompliance with the Federal financial management system requirements and the resources and responsible organizational units for such planned actions. Management agreed with the recommendations.		

Fiscal Year	Report Number	Report Title	Date Issued
2021	OIG-21-020	***FINANCIAL MANAGEMENT: Management Letter for the Audit of the Department of the Treasury's Financial Statements for Fiscal Years 2020 and 2019***	12/20
1.	DO Information Technology management should ensure that the configured schedule/frequency of Financial Analysis and Reporting System backups is implemented in accordance with the minimum backup frequency required by DO and Treasury policy.		
2.	Ensure that system-generated logs of backups, including failures, are retained for the examination period and can be provided upon request.		
3.	Management should strengthen control procedures to ensure policies, procedures, and related control activity documentation are timely updated for continued relevance and effectiveness of key controls based on changes in legislation, policies, and agreements related to Government Sponsored Enterprises' activities.		
4.	Assist management in mitigating the risk of potential noncompliance with the Federal Managers Financial Integrity Act (FMFIA) if (1) results of testing were not documented or (2) controls were not consistently tested by the components, management should enforce guidance on how to improve A-123 documentation and implementation of internal controls. Additionally, management should perform a more detailed review of the sufficiency of the component submissions, follow up with all inconsistencies, and have documentation readily available to substantiate the conclusion that was reached. Management agreed with the recommendations.		
Fiscal Year	Report Number	Report Title	Date Issued

2021	OIG-21-021	*FINANCIAL MANAGEMENT: Management Report for the Audit of the Department of the Treasury's Consolidated Financial Statements for Fiscal Years 2020 and 2019*	02/21
1.	Fiscal Service management should complete its periodic review of the PIR user access within the annual timeframe in accordance with the PIR SSP.		
2.	Address resource constraints and prioritize efforts to perform reviews within the annual timeframe in accordance with the PIR SSP.		
3.	Re-enforce established audit logging policy and procedures.		
4.	Retain evidence to demonstrate PIR auditable events are reviewed on a weekly basis as required by the PIR Security Log SOP.		
5.	Consider resource constraints and prioritize efforts to perform timely audit logging reviews in accordance with policy and procedures.		
6.	Review the current population of JFICS accounts and disable application user access that has been inactive for greater than 120 days.		
7.	Design and implement a control to automatically disable the JFICS application user accounts after 120 days of inactivity.		
8.	Retain evidence to demonstrate that access is disabled in a timely manner in accordance with the JFICS SSP.		
9.	Perform a review of the current system environment against the Configuration Management Database (CMDB) to ensure that all information system components are inventoried.		
10.	Perform a risk assessment over the subject matter and determine the appropriate personnel to be responsible for monitoring and updating the CMDB.		
11.	Update policy and procedures related to the above recommendations and disseminate the documentation to enforce such policy and procedures.		

12.	Conduct a review of the UNIX Mid-Tier production servers to validate that backups are scheduled for all servers based on the frequency defined in the Enterprise Information Technology Infrastructure (EITI) SSP for the full fiscal year.
13.	Perform a risk assessment over the subject matter and determine the appropriate personnel to be responsible for developing a Plan of Action & Milestones (POA&M) or formal risk acceptance for vulnerabilities identified.
14.	Disseminate policy and procedures related to the use of a POA&M or formal risk acceptance to the appropriate personnel determined above to enforce the respective vulnerability management requirements.
15.	Update the contingency plan at a minimum of every three years or after a major change, in accordance with BLSR and EITI SSP.
16.	Assign responsible points of contact to prioritize efforts to perform updates to the contingency plan every three years or when there is a significant change, in accordance with the BLSR and EITI SSP. Management agreed with the recommendations.

Fiscal Year	Report Number	Report Title	Date Issued
2021	OIG-21-025	***Interim Audit Update - Air Carrier and Contractor Certifications for Payroll Support Program***	03/21
1.	As expeditiously as possible, Treasury management should review payments issued under Payroll Support Program 1 (PSP1) to ensure awarded amounts are allowable per the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) and Treasury guidance.		
2.	As expeditiously as possible, Treasury management should remedy the incorrect amounts awarded under PSP1. Management agreed with the recommendations.		

Closed Investigations of Senior Government Employees Not Publicly Disclosed

April 1, 2021 through September 30, 2021

Treasury OIG closed six investigations involving senior Government employees during the period that were not publicly disclosed. In four of these investigations, an instance of misconduct was substantiated against a senior Government employee.

Case Number	Allegation/Disposition
UST-20-0074-I	At the request of the Integrity Committee of the Council of the Inspectors General on Integrity and Efficiency (CIGIE), Treasury OIG investigated allegations related to (1) violating Freedom of Information Act laws, (2) changing administrative rules to target a single employee, and (3) surreptitiously monitoring protected employee communications with the Office of Special Counsel and the Congress by a senior Government official. Treasury OIG's investigation determined the allegations were unsubstantiated due to lack of sufficient evidence. On January 22, 2021, Treasury OIG submitted its Report of Investigation to CIGIE for information and appropriate action. This matter was not referred to the Department of Justice (DOJ). *Unsubstantiated*
USM-21-0050-I	Treasury OIG initiated an investigation upon notification that senior Government officials pressured a subordinate to rescind a hiring selection based on the selectee's race. The allegation was unsubstantiated based on conflicting statements, and on the unanimous approval of the subordinate's selection by a hiring panel and the senior officials. On July 22, 2021, a report was provided to DOJ, but this matter was not referred to DOJ. *Unsubstantiated*
OCC-20-0012-I	Treasury OIG initiated an investigation upon notification a senior Government official from the Office of the Comptroller of the Currency (OCC) released confidential supervisory information during a presentation at a financial services forum. Prosecution of the employee was declined by the U.S.

Attorney's Office (USAO) for the District of Columbia. On May 24, 2021, Treasury OIG provided a report to OCC.
Substantiated

FinCEN-20-0011-I Treasury OIG substantiated an allegation that a senior Government official at the Financial Crimes Enforcement Network (FinCEN) was hired before the bureau received a required drug test in violation of bureau policy. On April 6, 2021, Treasury OIG provided its report of investigation to the Departmental Offices (DO) and FinCEN. The senior Government official resigned.
Substantiated

DO-19-0025-I Upon receipt of information from DO, Treasury OIG initiated an investigation regarding suspicious financial activity between unknown foreign individuals and a senior Government official. The employee allegedly received, laundered, and structured significant funds from foreign sources. The investigation did not substantiate structuring banking transactions to evade reporting requirements; however, Treasury OIG found the senior Government official did not handle and store classified documents properly. Prosecution of this senior Government official was declined by the USAO for the District of Columbia. On June 16, 2021, a report was provided to Departmental Offices for their information and appropriate administrative action.
Substantiated

BFS-21-0001-I	Treasury OIG initiated an investigation upon notification from the Bureau of the Fiscal Service (Fiscal Service), alleging a senior Government official used their position to hire their spouse. The investigation did not substantiate these allegations; however, the investigation revealed that the senior Government official used official Government email to conduct business for an outside business activity. Fiscal Service management counseled the employee on the proper use of Government email and the prohibition on conducting an outside business activity while on Government time. This matter was not referred to DOJ. *Substantiated*

Summary of Instances of Whistleblower Retaliation

April 1, 2021 through September 30, 2021

There were no cases of possible whistleblower retaliation opened or established to report for the period.

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

April 1, 2021 through September 30, 2021

There were no attempts made to resist, delay, or restrict Treasury 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, 2021 through September 30, 2021

Office of Audit

BILL AND COIN MANUFACTURING: Audit of Physical Security at U.S. Mint Production Facilities (OIG-21-026, 04/07/2021) **Sensitive But Unclassified, Not Publicly Disclosed**

CRF Prime Recipient Quarterly GrantSolutions Submissions Monitoring and Review Procedures Guide (Revised April 19, 2021) (OIG-CA-20-029R, 4/19/2021)

FINANCIAL MANAGEMENT: Audit of the Gulf Coast Ecosystem Restoration Council's Compliance with PIIA of 2019 for Fiscal Year 2020 (OIG-21-027, 05/14/2021)

American Rescue Plan - Application of Lessons Learned From the Coronavirus Relief Fund (OIG-CA-21-020, 05/17/2021)

Quarterly Summary Memorandum for the Lead Inspector General, Department of Defense: Operation Inherent Resolve - Summary of Work Performed by the Department of the Treasury Related to Terrorist Financing, ISIS, and Anti-Money Laundering for Second Quarter Fiscal Year 2021 (OIG-CA-21-021, 05/19/2021)

FINANCIAL MANAGEMENT: Audit of Treasury's Compliance with PIIA Requirements for Fiscal Year 2020 (OIG-21-028, 05/28/2021)

Memorandum for the Honorable Richard K. Delmar, Treasury Deputy Inspector General: Joint Purchase and Integrated Card Violation Report (October 1, 2020–March 31, 2021) (OIG-CA-21-022, 07/14/2021) **Internal Memorandum, Not Publicly Disclosed**

Survey Results Memorandum – Survey of Project Management at the United States Mint (OIG-CA-21-023, 07/20/2021)

Termination Memorandum – Audit of the Office of the Comptroller of the Currency's Supervision Related to Banks' Compliance with the Bank Secrecy Act, Anti-Money Laundering Regulations, Office of Foreign Assets Control Sanctions and Other Applicable Laws and the Impact on the De-risking Trend (OIG-CA-21-024, 7/27/2021)

Apache Tribe of Oklahoma's Use of Coronavirus Relief Fund Payment (OIG-CA-21-025, 7/28/2021) **Not Publicly Disclosed**

Termination Memo - Audit of Office of the Comptroller of the Currency's Human Capital Policies and Resource Planning (OIG-CA-21-026, 8/12/2021)

Quarterly Summary Memorandum for the Lead Inspector General, Department of Defense: Overseas Contingency Operations - Summary of Work Performed by the Department of the Treasury Related to Terrorist Financing and Anti-Money Laundering for Third Quarter Fiscal Year 2021(OIG-CA-21-027, 8/17/2021)

Termination Memorandum – Audit of Air Carrier Worker Support Certifications – West Air, Inc. (Redacted) (OIG-CA-21-028, 9/9/2021)

FINANCIAL MANAGEMENT: Financial Management: Report on the Enterprise Business Solutions' Description of its HRConnect System and on the Suitability of the Design and Operating Effectiveness of its Controls for the Period July 1, 2020, to June 30, 2021 (OIG-21-029, 9/17/2021)

Termination Memorandum – Audit of the Community Development Financial Institutions Fund's Administration of the Healthy Food Financing Initiative (OIG-CA-21-029, 9/21/2021)

FINANCIAL MANAGEMENT: Report on the Bureau of the Fiscal Service Administrative Resource Center's Description of its Shared Services and the Suitability of the Design and Operating Effectiveness of its Controls for the Period July 1, 2020 to June 30, 2021 (OIG-21-030, 9/27/2021)

Council of Inspectors General on Financial Oversight

Annual Report of the Council of Inspectors General on Financial Oversight (07/30/2021)

Audit Reports Issued With Questioned Costs

April 1, 2021 through September 30, 2021

Category	Total No. of Reports	Total Questioned Costs	Total Unsupported Costs
For which no management decision had been made by beginning of reporting period	1	$2,550	$0
Which were issued during the reporting period	0	$0	$0
Subtotals	1	$2,550	$0
For which a management decision was made during the reporting period	0	$0	$0
Dollar value of disallowed costs	0	$0	$0
Dollar value of costs not disallowed	0	$0	$0
For which no management decision was made by the end of the reporting period	1	$2,550	$0
For which no management decision was made within 6 months of issuance	1	$2,550	$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, 2021 through September 30, 2021

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

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.

Reports for Which No Management Comment was Returned Within 60 Days

As of September 30, 2021

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

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

As of September 30, 2021

There was one report as of the end of this reporting period with no management decision, *RESOURCE MANAGEMENT: Audit of the Department of the Treasury Departmental Offices Executive Pay Adjustment, Bonuses, and Awards*, OIG-20-027, issued on February 5, 2020, with $2,550 in questioned cost. Management agreed with our recommendations, but has not entered the planned corrective actions in the audit follow-up system, JAMES, to address the 10 recommendations made in the report.

Significant Revised Management Decisions

April 1, 2021 through September 30, 2021

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

Significant Disagreed Management Decisions

April 1, 2021 through September 30, 2021

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

Peer Reviews

April 1, 2021 through September 30, 2021

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 U.S. Department of Health and Human Services (HHS) OIG. In its report dated September 27, 2021, HHS OIG rendered a *Pass* rating for our system of quality control in effect for the year ended March 31, 2021. External audit peer review reports of our office are available on Treasury OIG's website. Treasury 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 its report dated January 5, 2021, the Federal Housing Finance Agency OIG found our office to be in compliance with all relevant guidelines for fiscal year 2020. During this reporting period, our office did not perform a peer review of another OIG.

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 banks 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 the 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.

There were no banks supervised by the OCC that failed during this reporting period.

Operation Inherent Resolve and Overseas Contingency Operations Quarterly Summary Memoranda to the Department of Defense OIG

During this reporting period, we issued two summary memoranda to the Department of Defense OIG regarding information we obtained on the Department of the Treasury's (Treasury or the Department) activities with respect to disrupting the Islamic State of Iraq and Syria's (ISIS) finances. The memoranda included specific examples of activities to disrupt ISIS's financing, information on Treasury programs that combat terrorist financing, and work we

performed or plan to perform to review these programs. **(OIG-CA-21-021, OIG-CA-21-027)**

References to the Inspector General Act

Section	Requirement	Page
Section 4(a)(2)	Review of legislation and regulations	21
Section 5(a)(1)	Significant problems, abuses, and deficiencies	7-17
Section 5(a)(2)	Recommendations with respect to significant problems, abuses, and deficiencies	7-17
Section 5(a)(3)	Significant unimplemented recommendations described in previous semiannual reports	22-43
Section 5(a)(4)	Matters referred to prosecutive authorities	21
Section 5(a)(5)	Summary of instances where information was refused	46
Section 5(a)(6)	List of audit reports	47-48
Section 5(a)(7)	Summary of significant reports	7-17
Section 5(a)(8)	Audit reports with questioned costs	49
Section 5(a)(9)	Recommendations that funds be put to better use	50
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	51
Section 5(a)(10)(B)	Summary of each audit, inspection, and evaluation report issued for which no management comment was returned within 60 days	51
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	22-43
Section 5(a)(11)	Significant revised management decisions made during the reporting period	51
Section 5(a)(12)	Management decisions with which the Inspector General is in disagreement	51
Section 5(a)(13)	Instances of unresolved Federal Financial Management Improvement Act noncompliance	12
Section 5(a)(14)	Results of peer reviews conducted of Treasury OIG by another OIG	52
Section 5(a)(15)	List of outstanding recommendations from peer reviews	52
Section 5(a)(16)	List of peer reviews conducted by Treasury OIG, including a list of outstanding recommendations from those peer reviews	52
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	21
Section 5(a)(18)	Description of metrics used to develop investigative statistics in Section 5(a)(17)	21
Section 5a(19)	Summary of each investigation involving a senior Government employee where allegation of misconduct was substantiated	44-46
Section 5a(20)	Instances of whistleblower retaliation	46
Section 5a(21)	Summary of attempts to interfere with Treasury OIG independence	46
Section 5a(22)(A)	Description of each inspection, evaluation, and audit that was closed and not publicly disclosed	47-48
Section 5a(22)(B)	Description of each investigation closed, involving a senior Government employee, that was not publicly disclosed	44-46
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	46

This page intentionally left blank.

Abbreviations

ARP	American Rescue Plan Act of 2021
BEP	Bureau of Engraving and Printing
BLSR	Baseline Security Requirements
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CBP	Customs and Border Protection
CIGIE	Council of the Inspectors General on Integrity and Efficiency
Council	Gulf Coast Ecosystem Restoration Council
COVID-19	Coronavirus Disease 2019
CRF	Coronavirus Relief Fund
DASHR/CHCO	Office of the Deputy Assistant Secretary for Human Resources and Chief Human Capital Officer
DATA Act	Digital Accountability and Transparency Act
DE&I	Diversity, Equity, and Inclusion
DO	Departmental Offices
DOJ	Department of Justice
Fiscal Service	Bureau of the Fiscal Service
FY	fiscal year
IRS	Internal Revenue Service
JFICS	Judgment Fund Internet Claim System
KPMG	KPMG LLP
Mint	United States Mint
OCC	Office of the Comptroller of the Currency
OFAC	Office of Foreign Assets Control
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PGPD	Prince Georges County Police Department
PIIA	Payment Integrity Information Act of 2019
PIR	Payment Information Repository
PMIAA	Program Management Improvement Accountability Act
PRAC	Pandemic Response Accountability Committee
RESTORE Act	Resources and Ecosystems Sustainability, Tourist Opportunities, and Revived Economies of the Gulf Coast States Act of 2012
RMA	RMA Associates
SES	Senior Executive Service
SSP	system security plan
SOP	standard operating procedures
TCVS	Treasury Check Verification System

TIGTA	Treasury Inspector General for Tax Administration
Treasury or the Department	Department of the Treasury
Trust Fund	Gulf Coast Restoration Trust Fund
USAO	U.S. Attorney's Office

View From Above of the Treasury Building at Night, Washington, DC
Source: Treasury Graphics

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

Report Waste, Fraud, and Abuse

Submit a complaint regarding Treasury OIG Treasury Programs and Operations and Gulf Coast Restoration using our online form: https://oig.treasury.gov/report-fraud-waste-and-abuse

Treasury Whistleblower Ombudsman

For information about whistleblowing and reprisal and about your rights and responsibilities as a Treasury employee or contractor, please contact the OIG Whistleblower Ombudsman Program at 202-927-0650 or Email: OIGCounsel@oig.treas.gov

Treasury OIG Website

Access Treasury OIG reports and other information online: https://oig.treasury.gov/