DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

October 15, 2024

INFORMATION MEMORANDUM FOR SECRETARY YELLEN

FROM: Richard K. Delmar
Acting Inspector General

SUBJECT: Management and Performance Challenges Facing the Department of the Treasury (OIG-CA-25-003)

In accordance with the Reports Consolidation Act of 2000, we are providing you with our perspective on the most serious management and performance challenges facing the Department of the Treasury (herein "Treasury" or "the Department"). In this year's memorandum, my office is reporting four challenges, one has been reframed, one is new, and two challenges are repeated and updated from last year. The reframed challenge focuses on Treasury's role in responsibly managing the financial assistance programs created in response to the Coronavirus Disease 2019 (COVID-19) global pandemic. A new challenge, Crypto and Digital Assets, considers factors beyond Treasury's control and their impact on Treasury's operations.

We removed two challenges from last year's memorandum, Climate Initiatives Risk and Information Technology Acquisition and Project Management. We recognize that Treasury continues to focus on meeting its responsibilities in these areas through various activities and initiatives.

The challenges discussed in detail below are as follows:

- Ongoing Management of COVID-19 Pandemic Relief Programs (Reframed from Previous Challenge, COVID-19 Pandemic Relief)
- Cyber Threats (Repeat)
- Anti-Money Laundering/Terrorist Financing and Bank Secrecy Act Enforcement (Repeat)
- Crypto and Digital Assets (New)

We identified challenges based on the threat they pose to Treasury's mission and stakeholders' interests. We also acknowledge the Department's accomplishments and efforts over the past year to address critical matters as noted within each challenge.

In addition to the challenges in this year's letter, we are reporting our concerns about the following matters: (1) U.S. Mint gold acquisitions, (2) Bureau of Engraving and Printing's construction of a new facility, and (3) Treasury's role with Customs revenue functions.

We are available to discuss our views on the management and performance challenges and the other matters expressed in this memorandum in more detail.

cc: Aditi Hardikar, Assistant Secretary for Management

Contents

Challenge 1: Ongoing Management of COVID-19 Pandemic Relief Programs (Reframed from Previous Challenge, COVID-19 Pandemic Relief)

While the national emergency declaration for the COVID-19 pandemic ended in May 2023, Treasury's responsibilities and workloads remain vastly expanded. Treasury needs to ensure these programs meet the economic needs and fiscal requirements of their respective constituencies responsibly. Specifically, Treasury is responsible for certain economic relief provisions in the *Coronavirus Aid, Relief, and Economic Security Act*[1] (CARES Act), the *Consolidated Appropriations Act, 2021*[2] (CAA, 2021), the *American Rescue Plan Act of 2021,*[3] and the *Consolidated Appropriations Act, 2023*[4] (CAA, 2023). In all, Treasury was tasked with disbursing over $650 billion in aid to more than 30,000 recipients, including state, local, territorial, and tribal government entities. As such, the Department established the Office of Capital Access (OCA)[5] to implement and manage most of Treasury's COVID-19 pandemic programs.

Our previous Management and Performance Challenges Memorandum (OIG-CA-24-001) provided the details of each program authorized by the legislation above and the associated challenge for each. Below is a list of those Treasury pandemic programs under our oversight.

- Coronavirus Relief Fund (CRF)
- Air Carrier Payroll Support Programs (PSPs)
- Emergency Rental Assistance Programs (ERA1 and ERA2)
- Homeowner Assistance Fund
- The Coronavirus State Fiscal Recovery Fund and the Coronavirus Local Fiscal Recovery Fund
- Coronavirus Capital Projects Fund (CPF)
- Local Assistance and Tribal Consistency Fund
- State Small Business Credit Initiative
- Emergency Capital Investment Program
- Community Development Financial Institutions Equitable Recovery Program

In this Management and Performance Challenges Memorandum, we are emphasizing the challenges faced by Treasury in management of these programs. Over the past year, turnover in OCA personnel and limited budgetary resources have resulted in operational weaknesses. Specifically, there has been a delay in carrying out certain required program functions, a lack of timely follow-through on implementing corrective action in response to Government Accountability Office (GAO) and Treasury Office of Inspector General (OIG) findings, and delays in responding to OIG requests. Taken together these deficiencies, if not corrected, may jeopardize the integrity of the operational effectiveness and efficiency, and compliance with regulations and guidance, for hundreds of billions of dollars of pandemic programs under Treasury's purview.

[1] Public Law 116-136 (March 27, 2020)
[2] Public Law 116-260 (December 27, 2020)
[3] Public Law 117-2 (March 11, 2021)
[4] Public Law 117-328 (December 29, 2022)
[5] Formerly known as the Office of Recovery Programs.

As discussed in our previous management and performance challenges memoranda dating back to October 29, 2020, we recognized that Treasury was initially challenged by resource and personnel constraints in standing up, in a short period of time, the multiple programs authorized by Congress in the various pandemic statutes. We also recognize that there have been changes in the leadership and the structure of OCA since my last memorandum. That said, these challenges and events do not relieve Treasury from its ongoing responsibility to ensure Congress and the American taxpayer that the pandemic funds entrusted to Treasury were, and are, being used prudently and properly.

A few examples of concerns noted follow.

- Single Audit Act[6] Report Follow-up – As part of the implementation of the multiple pandemic programs, Treasury is responsible to issue management decisions related to *Single Audit Act* (Single Audit) findings for a large number of financial assistance awardees (grantees) in compliance with the Office of Management and Budget's (OMB) Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance).[7] Among those responsibilities is the requirement to issue these management decisions on Single Audit findings timely (i.e., within 6 months). Although mostly late, in calendar years 2023 and 2024 Treasury has made some progress in issuing management decisions. However, Treasury is still behind the number of management decisions required and has yet to determine which grantees have failed to file or are late in filing Single Audit reports. This is a basic program responsibility.

- ERA1 Closeout Reports – The period of performance for ERA1 grantees ended in December 2022. After repeated requests from OIG since July 2023, OCA provided preliminary closeout data, in September 2024, for 619 out of 698 grantees. Final closeout reports for all grantees are critical because previously reported data by grantees to Treasury were determined by both OCA and OIG to be incomplete. In addition, this data is used by OIG to review thousands of ERA hotline complaints for identification of improper payments and fraud.

- The ERA and PSP programs have been identified as susceptible to significant improper payments.[8] OCA has been informed of the high risk of improper payments and other issues with these programs in multiple reports from GAO and OIG and meetings with OIG over several years but has yet to take sufficient corrective actions to fully address the issues. Treasury's inaction increases the risk

[6] P. L. 104-156 (July 5, 1996) The Single Audit Act of 1984, as amended in 1996, requires entities who receive Federal funds in excess of $750,000 to obtain an annual audit of those Federal funds. It was enacted for the purpose of promoting sound financial management, including effective internal controls, with respect to Federal awards administered by non-Federal entities and to establish uniform requirements for audits.
[7] Uniform Guidance, 2 C.F.R. § 200, Subpart F, Audit Requirements.
[8] Improper payments are payments that should not have been made, were made in incorrect amount, or were made to an ineligible recipient and are a long-standing and significant problem in the Federal government. As of May 2024, the estimated improper payments for both programs totaled over $200 million.

of significant improper payments within these programs and potential non-compliance with applicable laws and regulations.

In late August and early September 2024, I briefed Treasury's Acting General Counsel and the Deputy Secretary about our concerns with the challenges and weaknesses with the operations of the pandemic programs. Both these senior officials expressed their commitment to a resolution of these concerns and since that time, Treasury has been working with OIG and has resolved several issues and demonstrated progress towards resolving others. We will closely monitor the progress being made by OCA and look forward to continuing to work with Treasury management on these matters.

Challenge 2: Cyber Threats (Repeat)

Cybersecurity remains a long-standing and serious challenge facing the Nation and reported by GAO as a government-wide issue in its 2023 high-risk list published biennially.[9] A reliable critical infrastructure, including information systems and networks, is vital to our national security and economic stability. Cyber threats remain a persistent concern as Treasury's information systems are critical to the core functions of government and the Nation's financial infrastructure, along with the financial sector it oversees. As cyber threats continue to evolve and become more sophisticated, subtle, and easier to perform, Treasury must fortify and safeguard its internal systems and operations while modernizing and maintaining them. Although managing known risks is an ongoing challenge, Treasury must also be ready to reinforce and/or redirect cybersecurity efforts when unforeseen events occur, or when serious flaws are discovered in software or systems that increase potential risk of information compromise.

Threat actors frequently probe trusted connections for weaknesses to exploit vulnerable networks or systems and gain access to government systems. Organized hacking groups leverage published and unpublished vulnerabilities and vary their methods to make attacks hard to detect and even harder to prevent. Criminal groups and nation-states are constantly seeking to steal information; commit fraud; disrupt, degrade, or deny access to information systems; or infiltrate information systems and maintain a presence to enable future actions. Through information sharing, federal agencies are better prepared to thwart potential attacks to the cyber infrastructure of the Federal Government and the financial sector.

The tools used to perpetrate cyber-attacks continue to become easier to use and more widespread, lowering the technological knowledge and resources needed to launch successful attacks of increasing sophistication. Such attacks include distributed denial of service, phishing, fraudulent wire payments, business email compromise, malicious spam (malspam), ransomware, compromise of supply chains (both hardware and software), frequently used in combination to maximize attack effectiveness. Increasingly, artificial intelligence (AI) is being used to support attacks, from generating realistic looking phishing emails with minimal effort to creating programs to exploit vulnerabilities. Additionally, Treasury must remain cognizant of the increased risk profile a remote workforce presents, as it provides threat actors with a broader attack surface. Increased network traffic from remote sources provides cover for attackers to blend in with the federal workforce and

[9] GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas* (GAO-23-106203: April 20, 2023)

launch cyber assaults, and denial of service attacks upon a network or service can disrupt operations and prevent remote workers from performing their duties.

There is continuing concern over foreign adversaries creating and exploiting vulnerabilities in the Nation's supply chain for information and communication technology and services. Executive Order (EO) 13873, *Securing the Information and Communications Technology and Services Supply Chain*, was issued on May 15, 2019, to secure the supply technology and services chain by banning the import, use, or sale of technology or services designed, developed, manufactured, or supplied from persons or companies that are owned or controlled by governments defined as hostile to the United States. On May 8, 2024, this EO was extended again for 1 year.[10] There are risks that Treasury's systems and resources already in use, including critical infrastructure, contain components from sources that have yet to be designated as threats. Once a source is designated as such, repairs and/or upgrades of key system components may no longer be available. Therefore, there is risk of disruption of critical operations. The Department will need to continue to monitor developments in this area closely and plan for the possibility that its current supply chain may no longer be available.

Furthermore, EO 14028*, Improving the Nation's Cybersecurity*, issued on May 12, 2021, calls for federal agencies to update existing plans to prioritize resources for adoption and use of cloud technology and to adopt a zero-trust architecture,[11] among other things. To achieve the goals outlined in EO 14028, OMB issued M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*[12] to provide the strategy for achieving a zero-trust architecture, and require agencies to meet specific cybersecurity standards and objectives by the end of fiscal year 2024. OMB also issued M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*[13] to use only software that complies with secure software development standards. As mentioned above, Treasury management must be mindful that the efforts to secure Treasury's supply chain may hamper cloud adoption and the implementation of zero-trust architecture. In response to our fiscal year 2023 memorandum, Treasury reported progress towards implementing a zero-trust architecture by accelerating efforts to bring systems into compliance with federal mandates related to multi-factor authentication, encryption of data-at-rest, and encryption of data in-transit.

We continue to remind the Department that, in addition to Treasury's own networks and systems, management must be cognizant of, and mitigate, the risks posed by attacks made against other federal and non-federal agencies and Treasury contractors and subcontractors. Threats and risks to third parties' networks and systems also pose risks to Treasury's networks and systems, due to interconnections with other federal, state, and local agencies, and service providers to conduct its business. Management must continue thoughtful awareness of the wide threat environment and exercise due care evaluating and authorizing such internetwork connections and verify that third

[10] *Notice on the Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain* (May 8, 2024)
[11] Zero-trust architecture is a method of designing a system in which all actions are presumed dangerous until reasonably proven otherwise, thereby reducing the chance of a successful attack causing further damage.
[12] OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (January 26, 2022), (https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf)
[13] OMB M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (September 14, 2022), (https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf)

parties comply with federal policies and standards including any guidance issued to address new and/or expanded threats and risks. Management is also challenged with ensuring that critical data and information maintained by third-party service providers are properly protected.

Treasury is looked upon to provide effective leadership to financial institutions in particular, and the financial sector in general, to strengthen awareness and preparedness against cyber threats to the Nation's critical infrastructure. As such, effective public-private coordination is essential to the Nation's financial and national security. In this regard, the Office of Cybersecurity and Critical Infrastructure Protection coordinates Treasury's efforts to enhance the security and resilience of the financial services sector critical infrastructure and reduce operational risk including risks associated with cybersecurity. That said, Treasury and other federal agencies have yet to fully implement the National Institute of Standards and Technology (NIST) guidance to assist federal agencies in managing cybersecurity risks.[14] In 2018, GAO had reported that the extent of adoption of the NIST framework by critical infrastructure sectors was unknown since agencies were not measuring framework implementation.[15] With respect to Treasury, GAO had recommended that steps be taken to consult with respective sector partners to develop methods for determining the level and type of adoption by entities across the financial services sector. In 2020, GAO recommended that Treasury track the content and progress of sector wide cyber risk mitigation efforts and prioritize their completion according to sector goals and priorities in the sector-specific plan. Additionally, Treasury should update the financial services sector-specific plan to include specific metrics for measuring the progress of risk mitigation effects and information on the sector's ongoing and planned risk mitigation efforts.[16] However, as of April 2024, GAO reported Treasury needed to finalize steps to track the financial sector's risk mitigation efforts, and to prioritize the completion of efforts according to sector-wide goals and priorities. Treasury was planning to update the financial services sector-specific plan and was working on developing sector-specific cyber performance goals. Lastly, Treasury reported to GAO that it did not believe it would be beneficial to update the sector-specific plan until the Department of Homeland Security completes its updates to the national plan and provides guidance on sector-specific plans.[17] Additionally, Treasury reported in its response to our 2023 letter that it contributed to the development of the Cross Sector Cyber Performance Goals, with significant input from the financial sector and independent regulators. Treasury also noted that they were developing an effort focused on the benefits and challenges related to cybersecurity in the financial services sector, stemming from increased use of AI.

The Department reported in its response to last year's letter that it continues to focus on network defense efforts for its High Value Assets,[18] which includes an increased emphasis on risk/vulnerability assessments as well as accelerated compliance with logging, encryption, and multi-factor authentication

[14] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0, February 12, 2014; superseded by Version 1.1; April 16, 2018)
[15] GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption* (GAO-18-211; February 18, 2018)
[16] GAO, *Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts* (GAO-20-631; September 17, 2020)
[17] GAO, *Priority Open Recommendations: Department of the Treasury* (GAO-24-107324; June 5, 2024)
[18] High Value Assets are assets, information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the U S.' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety.

requirements. They also reported continued advocation for financial sector entities to participate in the Cybersecurity and Infrastructure Security Agency's Cyber Hygiene Vulnerability Scanning to receive timely notifications of vulnerable internet-facing systems.

While addressing increases in cyber threats, Treasury will need to continue to balance cybersecurity demands while maintaining and modernizing Information Technology systems.

Challenge 3: Anti-Money Laundering/Terrorist Financing and Bank Secrecy Act Enforcement (Repeat)

Over the past year, the Office of Terrorism and Financial Intelligence (TFI) has remained dedicated to countering the ability of financial networks that support terrorists, organized transnational crime, weapons of mass destruction proliferators, and other threats to international security through intelligence analysis, sanctions, and international private-sector cooperation. As previously reported, identifying, disrupting, and dismantling these networks continue to be challenging. Additionally, criminals and other bad actors evolve and continue to develop sophisticated money laundering methods in an attempt to avoid detection.

TFI's authorities are key tools in implementing U.S. policy to pressure foreign countries and regimes, such as Russia, by using a variety of targeted financial measures to include designations and economic sanctions. TFI has significantly increased sanctions against Russia related to its actions against Ukraine and its other malign activities. TFI's counter-terrorism designations disrupt the financial networks that support terrorist organizations. Other TFI tools, such as diplomatic and private sector engagement, regulatory oversight, and intelligence analysis, also play an important role. Disrupting terrorist financing depends on a whole-of-government approach and requires collaboration and coordination within Treasury, other federal agencies, the private sector, and international partners.

Collaboration and coordination are key to successfully identifying and disrupting illicit financial networks and meeting TFI's mission. This effort requires effective and efficient working relationships among components within TFI and the Intelligence Community. In an effort to effectively implement U.S. policy and disrupt these financial networks, officials stated that TFI is moving towards a more collaborative approach to achieve its mission. Given Treasury's critical mission and its role to carry out U.S. policy, we continue to consider anti-money laundering and combating terrorist financing programs and operations as inherently high-risk.

Data privacy, security, and information sharing are challenges for the Financial Crimes Enforcement Network (FinCEN), which has experienced unauthorized disclosures of *Bank Secrecy Act* (BSA) information.[19] FinCEN is required to maintain a highly secure database for financial institutions to report BSA information. FinCEN has previously identified that the success of that system depends on the financial sector's confidence that those reports are adequately protected, but unauthorized disclosures threaten to undermine that confidence. The challenge for FinCEN is to ensure the BSA information remains secure in order to maintain the confidence of the financial sector, while meeting the access needs of law enforcement, regulatory, and intelligence partners. FinCEN also faces an additional challenge to administer a secure database as required by the

[19] Public Law 91-508 (October 26, 1970)

Corporate Transparency Act.[20] This Act requires certain businesses to submit information about their beneficial owners such as legal name, date of birth, and address. That information may be shared with governmental authorities and financial institutions. FinCEN implemented the database in January 2024 and will need to securely store tens of millions of reports containing beneficial ownership information.

The Office of Intelligence and Analysis, as a member of the Intelligence Community, is required to take steps to adopt AI to improve intelligence collection and analysis.[21] The office appointed a Chief Artificial Intelligence Officer responsible for overseeing and coordinating efforts relating to AI, including the integration of acquisition, technology, human capital, and financial management aspects necessary for the adoption of AI solutions. However, various barriers, such as a lack of Office of the Director of National Intelligence guidance and Treasury's Office of Intelligence Analysis resources, as well as necessary updates to the information technology infrastructure have negatively affected their ability to take further steps to adopt AI.

TFI and its components have a wide range of responsibilities in combatting terrorists, criminals, and bad actors, Thus, it is critical that TFI has the resources and tools needed to stay ahead of sophisticated terrorists' financial networks and criminal money laundering schemes.

Challenge 4: Crypto and Digital Assets (New)

Interest in, and use of, digital assets, including cryptocurrencies, and stablecoins has increased rapidly over the past decade. Multiple jurisdictions are progressing with central bank digital currency[22] research and pilots which may be based on distributed ledger technology (DLT). [23] Experimentation with DLT continues, with numerous projects at various stages of proof-of-concept development. As of September 2024, the crypto-asset market reached a combined market capitalization of over $2 trillion, up from approximately $14 billion in late 2016 but down from $3 trillion in November 2021.[24]

Decentralized finance (DeFi) platforms increased total value locked (TVL)[25] during 2024, commensurate with overall growth in crypto market capitalization.[26] In April 2023, Treasury published a risk assessment on DeFi in which Treasury explored how illicit actors are abusing DeFi services as well as the vulnerabilities unique to DeFi services.[27] Treasury made several

[20] Public Law 116-283 (January 1, 2021)
[21] Public Law 117-263 (December 23, 2022)
[22] A central bank digital currency or CBDC is generally defined as a digital liability of a central bank that is widely available to the general public. A central bank is a national bank that provides financial and banking services for its country's government and commercial banking system, as well as implementing the government's monetary policy and issuing currency.
[23] Distributed ledger technology is a decentralized record of ownership of digital assets.
[24] Cryptocurrency Prices, Charts, and Crypto Market Cap, accessed September 9, 2024.
[25] TVL is an industry reported metric that is the amount of user funds deposited or "locked" in a DeFi service. TVL is used as a measure to gauge the size of the DeFi market or the degree of adoption or acceptance by users.
[26] There is currently no generally accepted definition of DeFi, even among industry participants. There is also no consensus on what characteristics would make a product, service, arrangement or activity "decentralized." The term broadly refers to virtual asset protocols and services that purport to allow for some form of automated peer-to-peer transactions.
[27] Treasury Report, *Illicit Finance Risk Assessment of Decentralized Finance* (April 2023)

recommendations in the report, including strengthening existing supervisory and enforcement functions to increase and harmonize compliance with regulatory requirements including those under the Bank Secrecy Act (BSA) such as the Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) program rule obligations.

While Treasury supports responsible innovation and the potential benefits of digital assets, the Financial Stability Oversight Council (FSOC)[28] reported that many crypto-asset firms may be acting outside of, or out of compliance with, applicable law(s) and may also lack sufficient risk governance and control frameworks. This increases the potential for fraud, illicit finance, sanctions evasion, operational failures, liquidity and maturity mismatches, and risk to investors and consumers, as well as contagion within the crypto-asset market.[29] Insufficient oversight or regulatory safeguards could create opportunities for illicit actors, such as cyber actors, ransomware cybercriminals, drug traffickers, and scammers who may be using digital assets and DeFi services to transfer and launder their illicit proceeds. The lack of consensus, standards, and practices among crypto industry participants regarding AML/CFT regulations as applied to digital assets or DeFi services exacerbate these issues.

Volatility in the crypto-asset market also poses risks to the traditional financial system. Financial institutions that partner with or provide traditional banking products and services to crypto-asset market participants may be impacted by this volatility. In 2023, in response to significant crypto-asset market volatility in 2022 (known as the "crypto winter"), the federal banking agencies, including the Office of the Comptroller of the Currency (OCC), issued two joint statements highlighting risks to banks involved with crypto-assets and crypto-asset participants. Shortly following the publication of these statements, in the Spring of 2023, residual risks adjacent to the 2022 "crypto winter" contributed to the failure of Silvergate, Silicon Valley, and Signature banks (e.g., liquidity and asset/liability risk management, concentration risk management).

Several Treasury offices, including the OCC's Office of Financial Technology continue to engage with digital asset industry stakeholders, including crypto-asset industry participants, and the agency's supervised institutions to understand developments and interest in the space, educate examiners and staff, and collaborate with other Treasury offices and federal agencies.

Taken together, the growth and continued interest in digital assets and DeFi services demands that the Department adopts a holistic approach to understanding the risks and opportunities these technologies present both within and outside the established financial system.

Other Matters of Concern

Although we are not reporting these as management and performance challenges, we are highlighting three areas of concern: (1) U.S. Mint gold acquisitions, (2) Bureau of Engraving and Printing's construction of a new facility, and (3) Treasury's role with Customs revenue functions.

[28] FSOC was established by the Dodd-Frank Wall Street Reform and Consumer Protection Act (P.L. 111-203). FSOC is charged with identifying risks to the nation's financial stability, promoting market discipline, and responding to emerging threats to the stability of the U.S. financial system. It is a collaborative body chaired by the Secretary of the Treasury.
[29] FSOC 2023 Annual Report, page 42

U.S. Mint Gold Acquisitions

Despite purchasing over a half a billion dollars in gold annually, the U.S. Mint (Mint) has limited engagement with its gold bullion suppliers or approved gold refineries to reaffirm that responsible sourcing requirements are met and that a majority of gold coins produced are minted from newly mined U.S. gold in compliance with U.S. law. For a little over 20 years, the Mint has not requested or obtained documentation from gold refiners concerning the origin of the gold purchased. In a May 2024 report, we recommended that the Mint considers additional procedures to oversee refiners including, but not limited to, obtaining and periodically reviewing documentation from the Mint's approved refineries to ensure that refineries are sourcing gold responsibly in accordance with U.S. law and the best interests of the U.S. Government.[30] We also recommended that the Mint develops a plan that outlines the steps and controls the Mint will implement to comply with the law in the production of gold coins. Additionally, the Mint's Basic Ordering Agreements with suppliers and representations to the public on its website need to reflect a validated methodology to ensure its compliance with U.S law in its purchase of gold for its coin programs.

As the Mint vets the options for improving the gold purchasing process, we will monitor the implementation of these controls to ensure they are sufficient to comply with U.S. law in the production of gold coins.

BEP's Construction of a New Facility

The Bureau of Engraving and Printing (BEP) project to replace its Washington, DC facility with a new facility in Beltsville, Maryland, is currently estimated to cost $1.78 billion. The FY 2024 and FY 2025 budget estimates include $1.5 billion and $63.9 million, respectively, for the next phases of this project. The U.S. Army Corps of Engineers will award a construction contract for the replacement facility during first quarter FY 2025 with construction expected to begin in late FY 2025. Until the estimated completion of the facility in 2027, BEP will need to ensure effective project oversight for construction of the building and purchase of equipment and machinery; proper accounting procedures; and employment of a workforce to produce the new family of secure notes. Treasury OIG will coordinate with the Federal Reserve Board OIG and the Department of Defense OIG, as necessary, to monitor the funding for, and construction of, the new facility and conduct related audit work.

Treasury's Role in Customs Revenue Functions

U.S. Customs and Border Protection is the second largest revenue collection agency in the United States. The Homeland Security Act of 2002 established the Department of Homeland Security (DHS) and dissolved the legacy United States Customs Service (Customs) in Treasury, transferring all its functions from Treasury to DHS, except Customs revenue functions, which were to be retained by Treasury. Treasury retained certain Customs revenue functions which include the approval of trade and duty related regulations and the authority to review, modify, or revoke any determination or ruling. Further, the Advisory Committee on Commercial Operations of the Customs Service is jointly appointed by the Secretary of the Treasury and the Secretary of

[30] OIG, Bill and Coin Manufacturing- The Mint Needs to Enhance Controls Over Gold Acquisitions (OIG-24-027; issued May 29, 2024)

DHS. In accordance with Treasury orders and directives, the Deputy Assistant Secretary for Tax, Trade and Tariff Policy has been delegated Customs revenue responsibilities; however, this position has been vacant for a little over 2 years. Treasury's Deputy Assistant Secretary for Tax Policy assumed Customs revenue responsibilities until his departure in February 2024. Treasury has not made any official delegations since the departure of the Deputy Assistant Secretary for Tax, Trade and Tariff Policy in 2022. This risks continuity of operations and assurance that Customs revenue responsibilities are being managed by the appropriate Treasury officials.

In an August 2024 memorandum, we recommended that Treasury's Acting Assistant Secretary for Tax Policy ensures that Treasury orders and directives are updated as necessary to accurately reflect the Treasury officials currently performing the Customs revenue functions. [31] This may include appointing an official to serve as the Deputy Assistant Secretary for Tax, Trade and Tariff Policy or issuing a revised Treasury Directive. Treasury officials have been working with colleagues at DHS to finalize an order that will delegate to the Secretary of Homeland Security authority related to Customs revenue functions not already delegated. Treasury officials are also working on revising delegations within Treasury to ensure that responsibility for the Customs revenue functions that will remain with Treasury is clearly delineated. We will continue to monitor Treasury operations to ensure the proper delegations are put in place and Customs revenue responsibilities are being fulfilled by designated Treasury officials. It is important that Customs revenue be protected and supported with responsible legislation and rulings.

[31] OIG, U.S. Treasury's Role with the Customs Revenue Function – Trade Facilitation and Trade Enforcement Act of 2015, Section 112 (OIG-CA-24-025; issued August 28, 2024)

Appendix: Acronyms and Abbreviations

AI	Artificial Intelligence
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
BSA	Bank Secrecy Act
CAA, 2021	Consolidated Appropriations Act, 2021
CAA, 2023	Consolidated Appropriations Act, 2023
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
COVID-19	Coronavirus Disease 2019
CPF	Coronavirus Capital Projects Fund
CRF	Coronavirus Relief Fund
Department	Department of the Treasury
DeFi	Decentralized Finance
DLT	Distributed ledger technology
EO	Executive Order
ERA	Emergency Rental Assistance
ERA1	Emergency Rental Assistance Program 1
ERA2	Emergency Rental Assistance Program 2
FinCEN	Financial Crimes Enforcement Network
FSOC	Financial Stability Oversight Council
GAO	Government Accountability Office
NIST	National Institute of Standards and Technology
OCA	Treasury Office of Capital Access
OCC	Office of the Comptroller of the Currency
OIG	Office of Inspector General
OMB	Office of Management and Budget
PSP	Air Carrier Payroll Support Program
Single Audit	Single Audit Act
TFI	Office of Terrorism and Financial Intelligence
TVL	Total value locked
Treasury	Department of the Treasury