OFFICE OF
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

December 4, 2025

INFORMATION MEMORANDUM FOR SECRETARY BESSENT

FROM: Loren J. Sciurba
Deputy Inspector General

SUBJECT: Management and Performance Challenges Facing the Department of the Treasury (OIG-CA-26-005)

In accordance with the Reports Consolidation Act of 2000, we are providing 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 five challenges, two new and three updated from last year.

The challenges discussed in detail below are as follows:

- Resource Optimization (New)
- Cyber Threats (Repeat)
- Artificial Intelligence Adoption (New)
- Anti-Money Laundering/Terrorist Financing and Bank Secrecy Act Enforcement (Repeat)
- Crypto and Digital Assets Growth (Repeat)

These challenges were identified based on the threats they pose to Treasury's mission and stakeholders' interests. We acknowledge within each challenge, if applicable, the Department's accomplishments and efforts over the past year to mitigate these risks.

In addition to the five challenges, we are reporting concerns about the following matters: (1) streamlining access to Do Not Pay (DNP) data sources, (2) ongoing management of Coronavirus Disease 2019 (COVID-19) pandemic relief programs, (3) United States Mint (Mint) gold acquisitions, and (4) Bureau of Engraving and Printing's (BEP's) construction of a new facility.

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: John W. York, Assistant Secretary for Management

Contents

Challenge 1: Resource Optimization (New)

In assessing the Department's most pressing challenges, it is essential to consider both external factors and future uncertainties that may significantly impact operations. These include, but are not limited to, staff reductions, funding cuts, challenges related to recruiting and retaining qualified personnel, and the ability to meet the Administration's priorities.

Staff and funding cuts have the potential to streamline processes and generate cost savings, but may also undermine the Department's operational resilience. The recent retirements and deferred resignations of many experienced personnel across Treasury bureaus and offices have created a significant human capital gap, including the loss of institutional knowledge and continuity, which threatens the Department's ability to fulfill its mission. This challenge is compounded by potential reductions in force and ongoing government-wide hiring restrictions.[1] Although hiring exemptions exist for certain critical positions in law enforcement and national security, the Department will operate under a reduced budget and will need to adapt to newly established staffing levels. These challenges and limitations may increase workloads, delay implementation of critical initiatives, and reduce Treasury's agility in addressing emerging issues.

The Department also continues to face significant difficulties in attracting and retaining skilled personnel, particularly in specialized areas such as financial analysis, information technology, cybersecurity, regulatory compliance, manufacturing trades and crafts, and police officers (for the BEP and the Mint). Contributing factors include competitive labor market conditions, federal compensation limitations, and constrained advancement opportunities. The lack of specialized expertise increases the risk of operational inefficiencies, security vulnerabilities, and non-compliance with laws and regulations. If these challenges are not addressed, the Department will continue to struggle with talent shortages that could hinder its ability to meet increasingly complex operational demands, adapt to evolving policy priorities, and maintain secure and efficient systems.

In the face of these challenges, the Department remains committed to advancing the Administration's goals and is focusing on efforts to improve the efficiency and effectiveness of operations, as it reshapes and optimizes the Treasury workforce by improving processes and enterprise decision-making, and streamlining human capital management through centralization and standardization. To this end, Treasury OIG will evaluate the Department's efforts to create operational efficiencies and generate cost savings while balancing limited resources, reduced staff, and competing mission demands as it executes the Administration's priorities.

Challenge 2: Cyber Threats (Repeat)

Cybersecurity remains a long-standing and serious challenge facing the Nation and continues to be reported by the Government Accountability Office (GAO) as a government-wide issue in its high-

[1] Presidential Memorandum, *Hiring Freeze* (January 20, 2025); Presidential Memorandum, *Extension of Hiring Freeze* (April 17, 2025); Presidential Memorandum, *Ensuring Accountability and Prioritizing Public Safety in Federal Hiring* (July 7, 2025); and Executive Order 14356, *Ensuring Continued Accountability in Federal Hiring* (October 15, 2025)

risk list published biennially.[2] A reliable critical infrastructure, including information systems and networks, is vital to our national security and economic stability. Cyber threats are an ever-present 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 these 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 be nimble and reinforce and/or redirect cybersecurity efforts to address unforeseen events when they arise, such as when serious flaws are discovered in software or systems that place Treasury's information and systems at risk of compromise.

Threat actors frequently probe trusted connections for weaknesses to exploit vulnerable networks or systems and gain access to government systems, leveraging vulnerabilities and varying their methods to disguise their attacks and make detection and prevention difficult. 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 establish a foothold to enable future actions against the Department or those connected to the Department. Through information sharing, federal agencies are better prepared to thwart potential attacks on the cyber infrastructure of the Federal Government and the financial sector.

As the tools used to perpetrate cyber-attacks continue to become easier to use and more widespread, the technological knowledge and resources needed to launch attacks decrease and the chances of successful attacks increase. Artificial Intelligence (AI) is increasingly used to support and create more realistic social engineering attacks (phishing emails, deepfake voices and videos) and programs that find and/or exploit vulnerabilities with minimal effort on the attacker's part. In addition, supply chain security remains a concern for both software and hardware.

Efforts to address these cybersecurity concerns at the federal level include Executive Order (EO) 13873, *Securing the Information and Communications Technology and Services Supply Chain*, 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 9, 2025, this EO was extended for 1 year.[3] Further, EO 14028*, Improving the Nation's Cybersecurity*, calls for federal agencies to, among other things, update existing plans to prioritize resources for adoption and use of cloud technology and to adopt a zero-trust architecture.[4] EO 14144, *Strengthening and Promoting Innovation in the Nation's Cybersecurity*, mandates software providers selling to the U.S. Government prove they are using secure development practices. These EOs were amended and enhanced by EO 14306, *Sustaining Select Efforts To Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144*. To achieve the goals outlined in EO 14028, the Office of Management and Budget (OMB) issued M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* to provide the strategy for achieving a

[2] GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness* (GAO-25-107743; February 25, 2025)

[3] *Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain* (May 9, 2025)

[4] 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.

zero-trust architecture, and require agencies to meet specific cybersecurity standards and objectives by the end of fiscal year (FY) 2024. OMB also issued M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* requiring agencies to only use software that complies with secure software development standards. The Department must not only stay on top of developments in cybersecurity, but also with federal requirements as those in turn adapt to the ever-shifting cybersecurity threat environment.

Furthermore, as part of prudent policy and as a cornerstone of implementing zero-trust architecture, Department 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 are also risks to Treasury's networks and systems, due to necessary interconnections to conduct business with service providers and federal, state, and local agencies. Management must continue to monitor the overall threat environment, exercise due care evaluating and authorizing internetwork connections, and verify that third parties comply with federal policies and standards including any guidance issued to address new and/or expanded threats and risks. Management must also ensure that critical data and information maintained by third-party service providers are properly protected.

The financial sector and its institutions look to Treasury for effective leadership in the fight against cyber threats. As such, effective public-private coordination is essential to the Nation's financial infrastructure 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's critical infrastructure and reduce operational risks including those 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.[5] In 2018, GAO reported[6] that the extent of adoption of the NIST framework by critical infrastructure sectors was unknown and 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. According to GAO, as of April 2025, Treasury's Financial Services Sector Risk Management Plan includes a line of effort aimed at promoting adoption of financial services sector-specific goals, which may correlate with aspects of the NIST cybersecurity framework; however, GAO noted Treasury did not identify steps it has taken in collaboration with sector partners to develop methods for determining adoption of NIST's cybersecurity framework or sector-specific goals that relate to the framework. Treasury's response to GAO stated that there are limitations on Treasury's ability to implement GAO's recommendation, as Treasury cannot compel entities to share cybersecurity framework adoption data and participation is voluntary.

In addition, quantum computing potentially permits hostile actors to attack the public-key cryptography used as the basis of financial services sector and Treasury signature, identity verification, and data encryption. NIST has released new Federal Information Processing

[5] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0, February 12, 2014; superseded by Version 1.1; April 16, 2018)

[6] GAO, *Critical Infatuation Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211 (February 15, 2018)

Standards for Post-Quantum Cryptography.[7] In coordination with the Office of Cyber Security and Critical Infrastructure Protection, the Department acknowledges that all elements of the financial services sector should be urged to transition to these new standards, preferably completing transition by FY 2035.

In response to our 2024 letter, Treasury noted progress towards its cybersecurity and compliance goals, such as encrypting data at rest for nearly all High Value Assets,[8] and all data in transit for Department-wide network traffic. The Department also reported advancements towards zero trust architecture, by expanding its enterprise-wide authentication platform and phishing-resistant multi-factor authentication. The Department plans to overhaul the cyber compliance program to streamline activities, reduce paperwork, and centrally manage risk.

In addressing increases in cyber threats, Treasury will need to continue to balance cybersecurity demands while maintaining and modernizing information technology systems.

Challenge 3: Artificial Intelligence Adoption (New)

AI is rapidly changing how organizations across government and the private sector operate. For the Department, AI represents both an opportunity and a risk. While it offers the potential to improve efficiency, refine analysis, and strengthen oversight, the technology remains an emerging and imperfect tool, with results that depend heavily on the quality of the data it uses. Results derived from AI can sometimes be biased, incomplete, or potentially fabricated. Risks related to information security and privacy increase as agencies adopt and scale AI infrastructure and usage. In addition, AI technology is evolving at a pace that can create challenges for existing policies and oversight structures. These realities make responsible and effective use of AI a significant management challenge for the Department.

Federal leaders have made clear that AI is a national priority. *America's AI Action Plan*[9] calls for innovation that reflects American values, while EO 14179, *Removing Barriers to American Leadership in Artificial Intelligence*, requires agencies to accelerate AI adoption by removing barriers and establishing consistent standards. Earlier guidance, such as EO 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, introduced principles of trustworthy AI, emphasizing accuracy, reliability, and transparency. More recent directives, including EOs on AI education,[10] workforce readiness,[11] unbiased AI principles,[12] and protection of American innovation abroad,[13] reflect how broad and fast-moving the government's priorities in

[7] The Federal Information Processing Standards are as follows: 203 entitled *Module-Lattice-Based Key-Encapsulation Mechanism Standard*, 204 entitled *Module-Lattice-Based Digital Signature Standard*, and 205 entitled *Stateless Hash-Based Digital Signature Standard*.

[8] 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.

[9] The White House, *Winning the Race: America's AI Action Plan* (July 2025) https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf

[10] EO 14277, "Advancing Artificial Intelligence Education for American Youth" (April 23, 2025)

[11] EO 14278, "Preparing Americans for High-Paying Skilled Trade Jobs of the Future" (April 23, 2025)

[12] EO 14319, "Preventing Woke AI in the Federal Government" (July 23, 2025)

[13] EO 14320, "Promoting the Export of the American AI Technology Stack" (July 23, 2025)

this area have become. Together, these actions underscore that AI is a core responsibility that demands sustained attention.

For Treasury, meeting this responsibility poses unique challenges. The Department must ensure that AI is introduced carefully and used in ways that strengthen, rather than compromise, its mission. That requires clear governance structures, careful oversight of contractors and vendors, and continuous monitoring to ensure AI systems remain accurate and reliable over time. It also means recognizing the limitations of AI and resisting the temptation to treat it as a replacement for human judgment in areas where accountability, fairness, and transparency are essential. Balancing these demands while AI technology continues to evolve will be an ongoing test for the Department.

Without a coordinated and cautious approach, Treasury risks relying on AI systems that produce unreliable results that can undermine public confidence. By following the direction set in *America's AI Action Plan*, related EOs, and OMB guidance,[14,15] the Department has an opportunity to shape AI adoption in a way that improves efficiency while maintaining accountability and trust. Moving forward, Treasury will need to remain vigilant, strengthen its governance capacity, and adapt continuously to the rapid pace of technological change to ensure AI serves the public interest effectively and responsibly.

Challenge 4: 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 national security through intelligence analysis, sanctions, and international private-sector cooperation. As previously reported, identifying, disrupting, and dismantling these networks continues to be challenging as criminals and other bad actors develop increasingly sophisticated money laundering methods to avoid detection.

TFI's authorities are key tools in implementing U.S. policy to pressure foreign countries and regimes, such as Russia and Iran, as well as rogue actors, such as terrorists, narcotics traffickers, and malicious cyber groups, by using a variety of targeted financial measures including economic sanctions. Over the past few years, TFI has significantly increased sanctions against Russia related to its actions against Ukraine and its other specified harmful foreign activities. TFI authorities, including its Bank Secrecy Act (BSA)[16] authorities, have supported Administration priorities, including countering narcotics trafficking and ensuring border security. 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,

[14] OMB M-25-21, "Accelerating Federal Use of AI through Innovation, Governance, and Public Trust" (April 3, 2025) www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf

[15] OMB M-25-22, "Driving Efficient Acquisition of Artificial Intelligence in Government" (April 3, 2025) www.whitehouse.gov/wp-content/uploads/2025/02/M-25-22-Driving-Efficient-Acquisition-of-Artificial-Intelligence-in-Government.pdf

[16] P.L. 91-508, Bank Secrecy Act of 1970 (October 26, 1970)

also play an important role. Disrupting terrorist financing depends on a whole-of-government approach and requires collaboration and coordination within Treasury, as well as with 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. Treasury officials stated that TFI continues to strengthen its collaborative approach to achieve its mission to effectively implement U.S. policy and disrupt these financial networks. 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 information in the past. 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.

The Office of Intelligence and Analysis (OIA), as a member of the Intelligence Community, is required to take steps to adopt AI to improve intelligence collection and analysis.[17] 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 resources, as well as necessary updates to the information technology infrastructure, have negatively affected OIA's ability to take further steps to adopt AI.[18]

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 5: Crypto and Digital Assets Growth (Repeat)

Interest in, and use of, digital assets including cryptocurrencies and stablecoins has increased rapidly over the past year. In January 2025, EO 14178, *Strengthening American Leadership in Digital Financial Technology*, established the President's Working Group on Digital Asset Markets to develop a federal regulatory framework for digital assets and prohibited federal agencies from undertaking any action to establish, issue, or promote central bank digital currencies

[17] P.L. 117-263, James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (December 23, 2022)
[18] Treasury OIG, *OIA Does Not Have Artificial Intelligence Capabilities and Faces Barriers to its Accelerated Adoption,* OIG-25-025 (April 2, 2025)

(CBDC),[19] except to the extent required by law. On July 14, 2025, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Board of Governors of the Federal Reserve System (FRB) issued a joint statement discussing general risk management considerations for engaging in fiduciary and non-fiduciary crypto-asset safekeeping activities.[20] Clarifying risk management considerations for crypto custody, stablecoin transactions, and blockchain networks facilitates institutional adoption and deeper financial integration with digital assets.

On July 18, 2025, the *Guiding and Establishing National Innovation for U.S. Stablecoins Act* (GENIUS Act)[21] was signed into law, marking the United States' first major legislative step towards federally regulating stablecoins. The GENIUS Act expands Treasury's authority and responsibilities related to cryptocurrencies and digital assets, including strengthening national security through enhanced sanctions and anti-money laundering enforcement, and requires the Secretary of the Treasury to issue regulations regarding illicit digital asset activity. With the Secretary chairing on the Stablecoin Certification Review Committee, Treasury will play a key role in certifying state stablecoin frameworks.

On July 30, 2025, the President's Working Group on Digital Asset Markets released a report containing recommendations to strengthen American leadership in digital financial technology.[22] The Working Group report requires regulators to coordinate on actions to modernize bank regulation for digital assets, and made a number of recommendations for rulemaking; however, the full impact of this report's findings depends on additional legislative action[23] and regulators' implementation of the recommendations.

While Treasury supports responsible innovation and the potential benefits of digital assets, the Financial Stability Oversight Council (FSOC)[24] reported that many crypto-asset firms may be acting outside of, or not in 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.[25] Insufficient oversight or regulatory safeguards could create opportunities for illicit actors, such as cyber actors, ransomware cybercriminals, drug traffickers, human traffickers, sanctions evaders, and fraudsters who may be using cryptocurrencies and digital assets to transfer and launder illicit monies. The U.S. financial

---

[19] A central bank digital currency or CBDC is generally defined as a digital liability of a central bank that is widely available to the 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.

[20] The Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Board of Governors of the Federal Reserve System. *Crypto-Asset Safekeeping by Banking Organizations* (July 14, 2025) Crypto-Asset Safekeeping by Banking Organizations

[21] P.L. 119-27, GENIUS Act (July 18, 2025)

[22] https://www.whitehouse.gov/crypto/

[23] H.R. 3633, the Digital Asset Market Clarity Act, passed the House of Representatives on July 17, 2025, and has been sent to the Senate for consideration. The bill seeks to clarify regulatory roles and provide consumer protections within the digital asset market.

[24] 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.

[25] FSOC, *2024 Annual Report*, pp. 45-49

system's strength, size, and reliability make it a notable target, and misuse by illicit actors affects matters of national security.[26] The borderless nature of digital asset markets, combined with a lack of consensus, standards, and practices among crypto industry participants with respect to regulations seeking to counter money laundering and terrorist financing exacerbate these issues.

Volatility in the crypto-asset market also poses risks to the traditional financial system. As of August 2025, the crypto-asset market reached a combined market capitalization of $3.9 trillion, up from approximately $2 trillion in September 2024.[27] Financial institutions that develop concentrations in, or build their business models around partnering with or providing traditional banking products and services to a single industry, including the crypto-asset market, may be adversely impacted by disruptions in that industry. This volatility was demonstrated in the spring of 2023, when 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).[28]

Given recent legislative changes and continued growth and interest in digital assets including cryptocurrencies, the Department must determine how to exploit the opportunities these technologies provide while also taking appropriate steps to mitigate risks to the safety and soundness of the U.S. financial system.

Other Matters of Concern

Although we are not reporting these as management and performance challenges, we are highlighting four areas of concern: (1) streamlining access to "Do Not Pay" (DNP) data sources, (2) ongoing management of COVID-19 pandemic relief programs, (3) Mint gold acquisitions, and (4) BEP's construction of a new facility.

Streamlining Access to DNP Data Sources

Reducing improper payments remains a government-wide priority and a persistent challenge for Treasury. EO 14249, *Protecting America's Bank Account Against Fraud, Waste, and Abuse,* requires executive branch agencies, in collaboration with Treasury, "to take action to defend against financial fraud and prevent improper payments." Such payments often result from incomplete or inaccurate data, insufficient eligibility verification, or weaknesses in program controls. The Payment Integrity Information Act of 2019 (PIIA)[29] further requires agencies to prevent, detect, and recover improper payments. Treasury supports agency compliance with PIIA through the DNP portal, a central resource for screening benefit recipients, vendors, and other payees against authoritative databases. The DNP portal has significantly expanded over time, incorporating critical data sources, such as the Social Security Administration's Death Master File

[26] President's Working Group on Digital Asset Markets. *Strengthening American Leadership in Digital Financial Technology* (July 30, 2025) Strengthening American Leadership in Digital Financial Technology – The White House, p. 100

[27] Cryptocurrency Prices, Charts, and Crypto Market Cap (accessed August 21, 2025)

[28] A crypto winter refers to a period when stocks and currencies in the crypto world lose popularity and value, becoming stagnant. The 2022 crypto winter was triggered, in part, by high inflation rates in the U.S., leading to aggressive interest rate increases by the FRB.

[29] P.L. 116-117, Payment Integrity Information Act of 2019 (March 2, 2020)

(DMF) to strengthen its ability to prevent improper payments. Treasury has also enhanced the portal with advanced analytics and system integration capabilities.

Despite these advancements, Treasury continues to face challenges. Agencies currently have access to the complete DMF, but that authority will expire on December 27, 2026,[30] without legislative action to make access permanent. Privacy, legal, and technical constraints also continue to slow integration of new federal and state data sources, limiting Treasury's ability to provide agencies with the full range of information needed to prevent improper payments. In addition, agencies vary in how effectively and consistently they use DNP tools, which reduces the overall government-wide impact of the system. To address these challenges and implement EO 14249, OMB issued M-25-32, *Preventing Improper Payments and Protecting Privacy Through Do Not Pay*. The guidance directs agencies to expand their use of DNP while ensuring strong privacy protections and provides new flexibility for sharing data with Treasury. In response, Treasury is developing a streamlined process for accessing additional data sources. Striking the right balance between modernization, data expansion, and privacy safeguards—while avoiding delays that could hinder agencies' ability to fully leverage DNP—remains a significant management challenge.

To strengthen the DNP portal and address challenges in expanding data access, Treasury should secure permanent legislative authority for the DMF, accelerate federal and state data-sharing agreements, and ensure robust privacy protections in coordination with OMB and oversight bodies. Simultaneously, Treasury should continue modernizing the DNP system through scalable technology and advanced data analytics, improving agency outreach and training to promote consistent use, and establishing performance measures to track impact on improper payments. Streamlining internal governance for onboarding new data sources will further reduce delays, enabling Treasury to maximize the DNP portal's effectiveness, protect privacy, enhance program integrity, and advance government-wide efforts to reduce fraud, waste, and abuse.

Ongoing Management of COVID-19 Pandemic Relief Programs

In response to legislation passed to address the COVID-19 pandemic,[31] Treasury was tasked with disbursing over $650 billion in aid to more than 30,000 recipients to support transportation industry workers; small businesses; renters and homeowners; and state, District of Columbia, local, territorial, and tribal government entities. The Department established the Office of Capital Access (OCA)[32] to implement and manage most of Treasury's COVID-19 pandemic programs. Treasury's pandemic programs provided needed support to many people and businesses, but were subject to losses from fraud and other improper payments. My office has performed audits, reviews,[33] and investigations into many of the more than 10,000 complaints and recipient-reported cases received. For the Coronavirus Relief Fund and the first Emergency Rental Assistance

[30] On December 27, 2020, Congress passed the Consolidated Appropriations Act of 2021, amending the Social Security Act to authorize the Social Security Administration to share its complete death data with the Do Not Pay program for a three-year period beginning no later than December 27, 2023.

[31] P.L. 116-136, Coronavirus Aid, Relief, and Economic Security Act (March 27, 2020); P.L. 116-260, Consolidated Appropriations Act, 2021 (December 27, 2020); P.L. 117-2, American Rescue Plan Act of 2021 (March 11, 2021); and P.L. 117-328, Consolidated Appropriations Act, 2023 (December 29, 2022)

[32] Formerly known as the Office of Recovery Programs.

[33] As of September 2025, Treasury OIG has identified approximately $4 billion in monetary impact ($4.2 million in recoupment and $4 billion in questioned costs) for pandemic programs under Treasury's purview.

program, Congress assigned the Treasury Office of Inspector General (OIG) the statutory authority to recoup funds if the Inspector General determined that a recipient failed to comply with the requirements related to the use of those funds. OCA is responsible for recouping ineligible payments and misuses of funds from other pandemic programs.

The Coronavirus State and Local Fiscal Recovery Fund (SLFRF) program is one of several programs for which OCA is responsible for recoupment. Under the SLFRF program, recipients were required to obligate all award funds by December 31, 2024, and must expend funds by December 31, 2026, with the exception of Surface Transportation projects and Title I projects that have an expenditure deadline of September 30, 2026.[34,35] In a recent report, GAO highlighted the compliance procedures and guidance for the SLFRF program.[36] GAO noted that since 2022, Treasury has required SLFRF recipients to submit project and expenditure reports to provide information on how recipients used their awards, including obligations and spending amounts. In each year from 2022 to 2024, thousands of SLFRF recipients did not meet the reporting deadline for project and expenditure reports. GAO recommended that Treasury develop and document, in its internal procedures and guidance for recipients, the timing and circumstances under which Treasury will initiate recoupment of awards for recipients that have not met SLFRF reporting requirements. To enhance accountability in the program, OCA needs to develop the procedures and guidance recommended in GAO's report.

As many of the pandemic programs under Treasury's purview wind down, OCA needs to ensure recipients continue to use funds responsibly. OCA also must continue to resolve audit findings of grantees and their subrecipients, including those with questioned costs, that are reported through required audits under the *Single Audit Act* (Single Audit).[37] We reported in our memorandum last year that while progress has been made, OCA was not timely in issuing management decisions for Single Audit findings and that remains the case. Prompt actions are needed because, as GAO stated in a recent letter to Treasury, "as more time passes, it is less likely overpayments will be recovered."[38]

United States Mint Gold Acquisitions

Despite purchasing over a half a billion dollars in gold annually, the Mint has limited engagement with its gold bullion suppliers or approved gold refineries to affirm 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.[39] For a little over 20 years, the Mint has not requested or

[34] Surface Transportation projects are funding projects eligible under specific Department of Transportation programs.

[35] Title I projects are funding projects eligible under Title I of the Housing and Community Development Act of 1974.

[36] GAO, *COVID-19 Relief: Treasury Could Improve Compliance Procedures and Guidance for State and Local Fiscal Recovery Funds*, GAO-25-107909 (July 22, 2025)

[37] P.L. 104-156, Single Audit Act Amendments of 1996 (July 5, 1996)

[38] GAO, *Priority Open Recommendations: Department of the Treasury,* GAO-25-108067 (August 12, 2025). GAO recommended that Treasury needs to develop processes, such as post-payment reviews or recovery audits, to strengthen its oversight of Emergency Rental Assistance funds. GAO also noted that implementing this priority recommendation could help Treasury more consistently identify and recover overpayments—including those resulting from potential fraud—for ineligible households.

[39] 31 U.S.C. § 5116

obtained documentation from gold refiners concerning the origin of the gold purchased. In a May 2024 report, we recommended that the Mint consider 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.[40] We also recommended that the Mint develop a plan that outlines the steps and controls the Mint will implement to comply with the law in the production of gold coins. Additionally, when purchasing gold for its coin program, the Mint's Basic Ordering Agreements with suppliers and representations to the public on its website need to reflect a validated methodology to ensure compliance with U.S law.

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

Built in 1914, the BEP's Washington D.C. facility is over 100 years old and restricts the bureau's ability to effectively implement modern currency production processes and security features required in the new family of bank notes. The BEP's project to replace its Washington, D.C. facility with a new facility in Beltsville, Maryland, is currently on hold and being re-evaluated for opportunities to decrease the overall cost. According to Treasury, trade tariffs being applied under the International Emergency Economic Powers Act have contributed to increases in costs since the BEP does not have an exemption (similar to the National Aeronautics and Space Administration's exemption). For example, in FY 2025 the BEP paid $5 million in tariffs for equipment alone and projects to incur in excess of an additional $100 million under the current rate structure. The costs of tariffs erode the budget planned for the project. Further this delay has necessitated additional investment in the existing century old DC facility to remain operational as a safe workplace. The BEP has requested over $650 million to mitigate long-standing deferred maintenance and improvements that are now necessary since the Bureau will remain in the existing facility for a longer time period. If the project resumes, the BEP will face ongoing challenges and will need to ensure effective project oversight for construction of the building and employment of a workforce to produce the new family of bank notes. Treasury OIG will coordinate with FRB 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.

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

Appendix: Acronyms and Abbreviations

AI	Artificial Intelligence
BEP	Bureau of Engraving and Printing
BSA	Bank Secrecy Act
CBDC	Central Bank Digital Currencies
COVID-19	Coronavirus Disease 2019
Department	Department of the Treasury
DMF	Death Master File
DNP	Do Not Pay
EO	Executive Order
FinCEN	Financial Crimes Enforcement Network
Fiscal Year	FY
FRB	Board of Governors of the Federal Reserve System
FSOC	Financial Stability Oversight Council
GAO	Government Accountability Office
GENIUS Act	Guiding and Establishing National Innovation for U.S. Stablecoins Act
Mint	United States Mint
NIST	National Institute of Standards and Technology
OCA	Treasury Office of Capital Access
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIIA	The Payment Integrity Information Act of 2019
Single Audit	Single Audit Act
SLFRF	State and Local Fiscal Recovery Funds
TFI	Office of Terrorism and Financial Intelligence
Treasury	Department of the Treasury