



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

October 15, 2026

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-27-004)

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 reiterating the five challenges identified last year, incorporating updates as appropriate.

The challenges discussed in detail below are as follows:

- Resource Optimization (Repeat)
- Evolving Cyber Landscape (Repeat)
- Super Intelligence Adoption (Repeat)
- 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) preventing and reducing improper payments, (2) ongoing management of Coronavirus Disease 2019 (COVID-19) pandemic relief programs, and (3) administration of federal student assistance programs.

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: Kevin Henneken, Acting Assistant Secretary for Management

Contents

Challenge 1: Resource Optimization (Repeat).....	2
Challenge 2: Evolving Cyber Landscape (Repeat)	2
Challenge 3: Super Intelligence Adoption (Repeat)	3
Challenge 4: Anti-Money Laundering/Terrorist Financing and Bank Secrecy Act Enforcement (Repeat).....	4
Challenge 5: Crypto and Digital Assets Growth (Repeat).....	5
Other Matters of Concern	6
Appendix: Acronyms and Abbreviations	10

Challenge 1: Resource Optimization (Repeat)

In response to our 2025 Management Challenges memorandum, Treasury noted that it has taken several steps to modernize and strengthen the Treasury workforce, including implementing targeted workforce reduction programs, enhancing Treasury's human resource management system with position budget management capabilities, developing the fiscal year 2026 Agency Staffing Plan, and establishing the Treasury Common Services Center (TCSC). These initiatives are aimed at modernizing workforce management and aligning with Administration goals to enhance efficiency and reduce waste.

Despite these initiatives, resource optimization remains a significant challenge for the Department. As Treasury streamlines internal processes to address critical staffing needs, it still faces challenges recruiting skilled talent in such areas as information technology, cybersecurity, manufacturing trades and crafts, and law enforcement (primarily within the Bureau of Engraving and Printing and the United States Mint). As such, reduced funding and personnel may continue to limit the Department's ability to meet mission demands, implement new initiatives, address audit recommendations, and maintain oversight functions. Furthermore, while TCSC service consolidations may generate cost savings, it requires ongoing oversight to ensure service levels are maintained or improved and not adversely affected.

The Department faces the ongoing task of finding ways to reduce costs while maintaining high-quality and timely government services. Given persistent resource constraints, it is imperative to adopt strategies that improve efficiency without compromising mission standards or accountability. Accordingly, Treasury must remain intensely committed to strategic workforce planning and continue investing in tools and processes that facilitate resource optimization. Continued assessment and adaptation are essential to meeting evolving Administration priorities, supporting workforce needs, and ensuring efficient use of Treasury resources. My office will continue to monitor the Department's progress in enhancing operational efficiencies, while balancing limited resources with competing mission demands and executing the Administration's priorities.

Challenge 2: Evolving Cyber Landscape (Repeat)

Treasury operates in a rapidly evolving cyber landscape, where both technology and the threat environment change quickly, and the Department must continually adapt to new or updated regulations and requirements. Because Treasury's information systems underpin both core government operations and the nation's financial infrastructure, the Department must continuously strengthen and modernize its cybersecurity posture while optimizing its resources. Threat actors, including criminal groups and nation-states, use increasingly sophisticated methods to take advantage of vulnerabilities in trusted connections and supply chains to infiltrate federal systems. While managing known risks is an ongoing challenge, Treasury must remain agile to address new requirements and unforeseen events as they arise. Additionally, the rise of Super Intelligence (SI)¹ tools has continued to lower the barrier for launching successful cyber-attacks.

¹ EO 14434, "Inaugurating the Era of Super Intelligence" (September 29, 2026)

In response to last year's memorandum, the Department noted it has implemented a series of initiatives to address cyber risks across the financial sector and within Treasury, such as expanding Project Fortress, an effort centered around enhancing the security and resilience of the financial services sector. The Department also reported that TCSC continued to streamline cybersecurity operations, including migrating web properties to a secure enterprise hosting platform with integrated controls.

Our ongoing yearly Federal Information Systems Modernization Act work will continue to monitor Treasury's progress in maintaining its overall cybersecurity posture while balancing its resource constraints.

Challenge 3: Super Intelligence Adoption (Repeat)

SI (formerly referred to as Artificial Intelligence or AI), is rapidly changing how organizations across government and the private sector operate. For the Department, SI 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 SI can sometimes be biased, incomplete, or potentially fabricated. Risks related to information security and privacy increase as agencies adopt and scale SI infrastructure and usage. In addition, SI technology is evolving at a pace that can create challenges for existing policies and oversight structures. These realities make responsible and effective use of SI a significant management challenge for the Department.

Federal leaders have made clear that SI is a national priority and the President has issued several executive orders (EOs) on SI adoption,² education,³ workforce readiness,⁴ unbiased SI principles,⁵ and protection of American innovation abroad.⁶ More recent guidance, including EO 14365, "Ensuring a National Policy Framework for Artificial Intelligence" and EO 14409, "Promoting Advanced Artificial Intelligence Innovation and Security" further emphasizes accelerating SI innovation and adoption while strengthening governance, oversight, and security. EO 14409 also positions Treasury as the lead, in consultation with other agency directors, in creating an SI cybersecurity clearinghouse. Together, these actions underscore that SI is a core responsibility that demands sustained attention.

In response to last year's memorandum, Treasury noted it established an SI Governance Board, chaired by the Deputy Secretary, and an SI Council, comprised of SI and technical leads from Treasury's bureaus and departmental offices. In June 2025, the Secretary also advanced formalizing SI adoption by naming the Department's first Chief SI Officer. Treasury's Chief SI Officer is leading the Department's strategic use of SI to enhance mission delivery and strengthen the resilience of the U.S. financial system, while also establishing baseline processes for assessing and managing the risks associated with SI technologies. As part of the Department's SI strategy, Treasury reported that its Office of the Chief Information Officer oversees Treasury's broader SI

² EO 14179, "Removing Barriers to American Leadership in Artificial Intelligence" (January 23, 2025)

³ EO 14277, "Advancing Artificial Intelligence Education for American Youth" (April 23, 2025)

⁴ EO 14278, "Preparing Americans for High-Paying Skilled Trade Jobs of the Future" (April 23, 2025)

⁵ EO 14319, "Preventing Woke AI in the Federal Government" (July 23, 2025)

⁶ EO 14320, "Promoting the Export of the American AI Technology Stack" (July 23, 2025)

advancement efforts, including infrastructure development, workforce training, and engagement with public and private sector partners. Moving forward, Treasury needs to remain vigilant, continue to strengthen its governance capacity, and adapt continuously to the rapid pace of technological change to ensure SI serves the public interest effectively and responsibly.

Challenge 4: Anti-Money Laundering/Terrorist Financing and Bank Secrecy Act Enforcement (Repeat)

The Office of Terrorism and Financial Intelligence (TFI) remains 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. 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 essential tools in implementing U.S. policy to pressure foreign countries, hostile regimes, and rogue actors, such as terrorists, narcotics traffickers, and malicious cyber groups. The Department leverages a range of targeted financial measures, such as economic sanctions, to achieve this objective. TFI authorities, including its Bank Secrecy Act (BSA) authorities,⁷ 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, also play an important role. Disrupting terrorist financing depends on a whole-of-government approach and requires collaboration and coordination within Treasury, and 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 previously experienced unauthorized disclosures of information. FinCEN is required to maintain a highly secure database for financial institutions to report BSA information. FinCEN recognizes that the success of that system depends on the financial sector's confidence that those reports are adequately protected, and that incidents of unauthorized disclosure pose a risk to that confidence. The challenge for FinCEN is to ensure the

⁷ Certain parts of the Currency and Foreign Transactions Reporting Act, its amendments, and the other statutes relating to the subject matter of that Act, have come to be referred to as the BSA. These statutes are codified at 12 U.S.C. 1829b, 12 U.S.C. 1951–1960, and 31 U.S.C. 5311–5314 and 5316–5336 and notes thereto, with implementing regulations at 31 CFR chapter X.

BSA information remains secure to maintain the confidence of the financial sector, while meeting the access needs of law enforcement, regulatory, and intelligence partners.

TFI and its components have a wide range of responsibilities in combatting terrorists, criminals, and other bad actors. As such, 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)

With the growth of crypto and digital assets, Treasury's challenges include managing rapid digital-asset expansion while implementing new legislative and regulatory requirements designed to safeguard the U.S. financial system. As interest in digital assets expands, so does the complexity of risks Treasury must address. In 2025, United States banking agencies experienced a surge in bank charter applications ranging from fintech companies and payment platforms to crypto and brokerage firms. Application types include traditional bank charters conferring full bank status and uninsured national trust bank charters that are non-depositories and thus exempt from Federal Deposit Insurance Corporation deposit insurance requirements. As of April 28, 2026, over 20 digital asset companies, lenders, payment providers, and neobanks⁸ had applied for or conditionally received bank charters from the Office of the Comptroller of the Currency (OCC).⁹

The U.S. financial system's strength, size, and reliability make it a notable target, and misuse by illicit actors affects matters of national security.¹⁰ Digital assets, similar to other mediums of exchange, enable rapid cross-border transfers and offer a perceived level of anonymity—features that illicit actors can exploit to facilitate money laundering and terrorist financing, as well as other predicate offenses, crimes, and fraud.¹¹ As digital-asset activity expands, gaps in oversight or regulatory safeguards increase opportunities for cyber actors, ransomware groups, traffickers, sanctions evaders, and fraudsters to use cryptocurrencies and other digital assets to transfer and launder illicit funds. The borderless nature of digital asset markets, combined with a developing legal and regulatory framework, further complicates efforts to counter money laundering and terrorist financing.

Volatility in the crypto-asset market also poses risks to the traditional financial system. As of June 2026, the crypto-asset market reached a combined market capitalization of \$2.2 trillion, down from approximately \$3.9 trillion in August 2025.¹² Financial institutions that develop concentrations in or build their business models around partnering with or providing traditional

⁸ Neobanks are financial technology companies that typically offer banking accounts through mobile apps and web browsers. Some neobanks offer savings accounts, loans, credit cards and investing products.

⁹ EO 14405, "Integrating Financial Technology Innovation in Regulatory Frameworks" (May 19, 2026), directs regulators to take steps to encourage innovation by, and growth of, fintech firms and federally regulated institutions of all sizes.

¹⁰ 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

¹¹ [Financial Stability Oversight Council, 2025 Annual Report](#), p. 43

¹² [Cryptocurrency Prices, Charts, and Crypto Market Cap](#) (accessed June 10, 2026)

banking products and services to a single industry, including the crypto-asset market, may be adversely impacted by disruptions in that industry.¹³

The Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act)¹⁴ marked 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. Under the Act, the OCC gained regulatory or enforcement authority over certain permitted payment stablecoin issuers, including subsidiaries of national banks or federal savings associations, federal qualified payment stablecoin issuers, registered foreign payment stablecoin issuers, and certain state qualified payment stablecoin issuers.

In implementing the GENIUS Act, Treasury issued several notices of proposed rulemaking in 2026. For example, in February 2026, the OCC issued a Notice of Proposed Rulemaking (NPRM) addressing all the regulations the OCC is required to promulgate under the GENIUS Act, other than those related to the BSA, anti-money laundering, and Office of Foreign Asset Control sanctions. In April 2026, FinCEN and the Office of Foreign Assets Control issued a joint NPRM to implement the GENIUS Act's anti-money laundering and sanctions compliance program requirements. In June 2026, FinCEN and the OCC, together with the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the National Credit Union Administration, issued a joint NPRM to implement the GENIUS Act customer identification program requirements, which directs that permitted payment stablecoin issuers be treated as financial institutions under the BSA and be required to maintain effective customer identification programs. The OCC also issued an NPRM to implement the BSA and sanctions compliance standards applicable to OCC-supervised permitted payment stablecoin issuers. Collectively, these proposed rules aim to support innovation while establishing a risk-based regulatory framework that mitigates illicit-finance risks and protects the financial system and national security.

Given recent legislative changes, the speed at which these changes are being implemented, and continued growth and interest in digital assets, including cryptocurrencies, Treasury must find ways to leverage emerging opportunities while ensuring robust risk-mitigation frameworks that preserve 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 three areas of concern: (1) preventing and reducing improper payments, (2) ongoing management of COVID-19 pandemic relief programs, and (3) administration of federal student assistance programs.

¹³ 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). 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 Board of Governors of the Federal Reserve System.

¹⁴ P.L. 119-27, GENIUS Act (July 18, 2025)

Preventing and Reducing Improper Payments

Preventing and reducing improper payment remains a government-wide priority and a persistent challenge for Treasury. Treasury is working to improve payment integrity and to increase the use and effectiveness of the “Do Not Pay” (DNP) Working System. Notably, pursuant to the Ending Improper Payments to Deceased People Act,¹⁵ which established permanent access to the Death Master File, Treasury is supporting agency efforts to prevent improper payments to deceased individuals. Treasury has also implemented measures to comply with executive orders¹⁶ to ensure that agencies follow strict protocols for payment processing, which include regular reviews and audits to identify and address any potential issues related to improper payments. Other notable accomplishments include, but are not limited to, expanding risk-based screenings, identifying and prioritizing high-risk transactions, using SI to identify check fraud, improving payment processing schedules, and expanding pre-payment verification screening aimed at avoiding improper payments over the long term. Despite these efforts, improper payments persist¹⁷ and require continued attention from Treasury.

While screening for payments to deceased individuals is essential, these payments constitute only a minor portion of overall improper overpayments. Moreover, in January 2026, the adoption of the DNP Working System was limited to approximately 4 percent of eligible programs fully utilizing its functionalities. Since then, Treasury has significantly expanded access to DNP data, reporting in October 2026 that approximately 99 percent of federal programs can access all DNP data sources for which they are legally authorized. Treasury management must continue to promote effective use of the DNP Working System, work with federal agencies to expand data availability, enhance performance measurement, and focus on strengthening payment verification capabilities and program controls. Ongoing diligence will be vital in meeting expanded oversight responsibilities and reducing risks of improper payments.

Ongoing Management of COVID-19 Pandemic Relief Programs

Treasury’s ongoing management of pandemic programs to ensure compliance with funding requirements and its ability to identify and recover fraudulent or improper payments remains a challenge. The Department established the Office of Capital Access (OCA) to oversee and manage these programs to assist communities during the COVID-19 pandemic. The Department disbursed over \$650 billion in aid to more than 30,000 recipients supporting transportation industry workers, small businesses, renters and homeowners, states, and government entities. Treasury’s pandemic programs provided needed support to many people and businesses but were also subject to losses from fraud and other improper payments. OCA, as the program office, has authority and responsibility to recoup improper or fraudulent payments for all pandemic programs. Audits, reviews, and investigations conducted by my office identified fraud, questioned costs, and overpayments within Treasury’s pandemic programs. The Government Accountability Office also highlighted Treasury’s need to strengthen its post-payment controls over certain pandemic

¹⁵ P.L. 119-77, Ending Improper Payments to Deceased People Act (February 10, 2026)

¹⁶ See, e.g., EO 14249, “Protecting America’s Bank Account Against Fraud, Waste, and Abuse” (March 25, 2025)

¹⁷ Treasury OIG, *Fiscal Service’s Sensitive Payment Systems’ Controls are Generally Adequate but Weaknesses and Deficiencies Exist*, OIG-26-032 (June 8, 2026)

program funds to more effectively recover overpayments, adding that, until Treasury strengthens these controls, its ability to recover overpayments will be delayed or impossible. Considering OCA's resource constraints and the conclusion of many pandemic programs, Treasury's ability to recover overpayments is weakened.

In response to last year's memorandum, Treasury noted that more than \$902 million was recovered for the first Emergency Rental Assistance program and that it was conducting desk reviews for the second Emergency Rental Assistance program and the Homeowners Assistance Fund to ensure the proper use of funds. The Department plans to continue these desk reviews through fiscal year 2027. Further, Treasury is developing a system to collect information from recipients and other parties regarding implementation of financial assistance programs administered by the Department. Treasury may use the information to evaluate compliance with program requirements, including compliance with applicable federal laws, regulations, and executive orders; to support other audit and program oversight activities; to identify potential waste, fraud, and abuse; and for research and statistical purposes. My office will monitor how this system of records will assist Treasury with executing monitoring and oversight of the pandemic programs and the recovery of funds, recognizing that OCA continues to wind down most of its programs and dedicated resources.

Administration of Federal Student Assistance Programs

On March 19, 2026, the Department of Education (Education) signed an interagency agreement with Treasury to procure services supporting the administration of federal student assistance programs¹⁸—a \$1.7 trillion federal student loan portfolio. The agreement provides a three-phase approach. For the first phase, Treasury “will revoke its exemption for referral of defaulted student loan collections to Education and carry out default collections through integration of Federal Student Aid’s Default Resolution Group with its existing Cross-Servicing program.” During Phase 2, Treasury will take over “responsibility for administrative operations for servicing of Education’s non-defaulted debt, to the extent practicable, following Treasury’s assessment of the portfolio and its operations.” The third phase has Treasury “reviewing the programmatic and policy requirements that govern the eligibility for students to receive federal student financial assistance, including but not limited to the administration of the Free Application for Federal Student Aid and eligibility for institutions of higher education to gain and retain eligibility for federal student financial assistance, including but not limited to origination of loans, oversight, and enforcement activities.” The agreement outlines general roles and responsibilities to be executed for the first phase of the plan but lacks details on the other two phases and does not specify timelines for implementation. The agreement also allows for modification from “time to time” if agreed to by both Treasury and Education.

In an April 16, 2026, letter¹⁹ to Congress, Treasury stated that Treasury and Education began the early stages of implementing Phase 1 and achieved two milestones. First, on March 20, 2026, Treasury published a Request for Information to obtain input on draft solicitation for default

¹⁸ <https://www.ed.gov/media/document/ed-treasury-interagency-agreement-federal-student-assistance-partnership-march-19-2026-113468.pdf> (accessed August 2026)

¹⁹ https://www.warren.senate.gov/wp-content/uploads/media/doc/response_from_treasury.pdf (accessed August 2026)

resolution agents (previously referred to as private collection agencies). Second, on April 3, 2026, an agreement was signed to detail Education employees to Treasury and Treasury employees to Education with the initial focus on transitioning operational responsibility for the defaulted portfolio to Treasury. Subsequently, in August 2026, Treasury announced its intent to create a “Default Resolution Hub,” to help borrowers plan steps to get out of default, including guidance on repayment options and secure sharing of tax information. Given the size and complexity of the federal student loan portfolio, and Treasury’s efforts to optimize resources and reduce improper payments, managing all aspects of federal student assistance programs could become a significant challenge for Treasury.

Appendix: Acronyms and Abbreviations

BSA	Bank Secrecy Act
COVID-19	Coronavirus Disease 2019
Department	Department of the Treasury
DNP	Do Not Pay
Education	Department of Education
EO	Executive Order
FinCEN	Financial Crimes Enforcement Network
GENIUS Act	Guiding and Establishing National Innovation for U.S. Stablecoins Act
NPRM	Notice of Proposed Rulemaking
OCA	Office of Capital Access
OCC	Office of the Comptroller of the Currency
OIG	Office of Inspector General
SI	Super Intelligence (formerly Artificial Intelligence or AI)
TCSC	Treasury Common Services Center
TFI	Office of Terrorism and Financial Intelligence
Treasury	Department of the Treasury