DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

October 15, 2019

INFORMATION MEMORANDUM FOR SECRETARY MNUCHIN

FROM: Richard K. Delmar /s/
Acting Inspector General

SUBJECT: Management and Performance Challenges Facing the Department of the Treasury (OIG-CA-20-005)

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 (hereinafter Treasury or the Department). In this year's memorandum, my office is reporting five challenges of which one is new and four are repeated and updated from last year.

- Operating in an Uncertain Environment (Repeat)
- Cyber Threats (Repeat)
- Anti-Money Laundering/ Terrorist Financing and Bank Secrecy Act Enforcement (Repeat)
- Efforts to Promote Spending Transparency and to Prevent and Detect Improper Payments (Repeat)
- Information Technology Acquisition and Project Management (New)

We identified challenges based on the threat they pose to Treasury's mission and stakeholders' interests. That said, we acknowledge the Department's accomplishments and efforts over the past year to address the most critical matters as noted within each challenge discussed. In addition to the above challenges, we are reporting our elevated concerns about the following matters: (1) the coin redemption program at the United States Mint (Mint) and (2) managerial cost accounting.

2020 Management and Performance Challenges

Challenge 1: Operating in an Uncertain Environment (Repeat)

As reported in the prior year's memorandum, we remain mindful of external factors and future uncertainties that affect the Department's programs and operations. Among the most notable was the 35-day partial Federal government shutdown from December 22, 2018 through January 25, 2019 that affected all of government including Treasury. Like other components of Treasury subject to a lapse in appropriation, the Bureau of the Fiscal Service (Fiscal Service) developed its 2019 Lapse Plan as directed by the Office of Management and Budget (OMB). According to Fiscal Service officials, its 2019 Lapse Plan was based on assumptions that the shutdown would be of a short duration consistent with OMB's guidelines. Assumptions included a shutdown that would (1) last one week at most including weekend operations because 7 of the last 10 shutdowns were 5 days or less; and (2) be a full operational shutdown and not a partial one. Fiscal Service's 2019 Lapse Plan did not contemplate a shutdown of the nature and duration as that of the fiscal year 2019 shutdown. Given the central role that Fiscal Service serves in providing financial and administrative services government-wide and to the American public, management had to make adjustments to meet the bureau's obligations.

Fiscal Service only avoided impacts to its services through proactive and decisive management and the support of the Department. Since the fiscal year 2019 shutdown was partial, many Federal agencies required ongoing support. According to Fiscal Service officials, this increased the workload for Fiscal Service's government-wide operations above those planned in the approved Lapse Plan and required modifications to the plan during the appropriation lapse. Fiscal Service officials stated that they revised the 2019 Lapse Plan to provide critical government-wide support services under different scenarios (e.g. short vs. long-term shutdown, partial vs. full shutdown).

Also reported in prior years, the Department continues to await discussions with OMB and Congress on the proposed changes included in OMB's comprehensive "Government–wide Reform Plan and Reorganization Recommendations" (Government–wide Reform Plan) to reorganize the Executive Branch.[1] In the plan, OMB made agency-specific recommendations that would merge functions with similar missions across agencies. Specific to Treasury, OMB proposed the transfer of alcohol and tobacco responsibilities from the Bureau of Alcohol, Tobacco, Firearms and Explosives within the Department of Justice to the Alcohol and Tobacco Tax and Trade Bureau (TTB) in order to leverage the expertise and resources of TTB. Other potential impacts on Treasury include OMB's recommendations to increase coordination between agencies and avoid duplication of roles in the areas of small business programs, the housing finance market, and financial literacy and education. Furthermore, the plan also includes a proposal to privatize the United States Postal Service, which is estimated to be insolvent, yet continues to hold a $15 billion unfunded liability to the Treasury's Federal Financing Bank. Although no decisions have been made, Treasury started to prepare for the potential long-term restructuring of certain functions of offices/bureaus and expected budget cuts.

Tackling OMB's proposed reformations and other critical matters at hand could be more challenging as Senate confirmed leadership positions and other key senior level positions within the Department remain vacant. As of this writing, there are several vacant positions. Even though some positions in the nomination process have been confirmed, other key positions such as the Chief Financial Officer (vacant since July 2013) and the Under Secretary for Domestic Finance (vacant since September 2014) remain unfilled. Although progress was made in filling other positions, it is important that any remaining vacancies and new ones across Treasury be filled as quickly as possible to avoid potential skill gaps. This could pose risks to Treasury meeting key program missions and impact succession planning. Human capital management overall remains a high risk area as the lengthy security clearance process and backlog of background investigations cause significant delays onboarding highly-skilled individuals to fill critical positions across Treasury. Due to substantial increases in appropriation and staffing levels, the two offices most impacted are the Office of International Affairs, which is working to increase its staffing level from 22 to 65 employees by the end of calendar year 2019 and to 90 employees by the end of calendar year 2020; and the Office of Terrorism and Financial Intelligence (TFI), which requested approximately 50 new positions for fiscal year 2020. These positions could be difficult to fill if

[1] OMB, *Delivering Government Solutions in the 21st Century, Reform Plan and Reorganization Recommendations* (June 2018)

approved because of the expertise required for these positions and length of time to process required security clearances.

Most recently, Treasury has had to manage the increasing demands placed on the Committee on Foreign Investments in the United States[2] (CFIUS), which is charged with reviewing transactions involving foreign investments in the United States to determine national security risks. There is an anticipated increase in both volume and complexity of transactions. The Office of International Affairs carries out the Secretary's role as Chair of CFIUS and coordinates the interagency review process. While the Foreign Investment Risk Review Modernization Act of 2018[3] modernized the review process, it also expanded CFIUS's jurisdiction to address growing concerns over certain investment structures that were not within CFIUS's jurisdiction such as investments involving U.S. businesses in close proximity to U.S. military bases and investments with impacts to critical infrastructure and personally identifiable information (PII). Treasury estimated that the number of transactions for review will increase from 200 to over 1,000 transactions per calendar year. It will be a challenge onboarding personnel with the specialized skills to review complex investment structures as the security clearance process continues to be a contributing factor in recruiting highly skilled personnel that require access to programs and information systems dealing with national security. As the office builds staff capacity, it plans to utilize contractor support.

The lengthy security clearance process continues to hamper the recruitment of cybersecurity personnel government-wide. Our previous audits of select Treasury bureaus found that the cause for many of our findings related to information systems' security measures involved a lack of resources and/or management oversight, which echoed the Government Accountability Office's (GAO) observations of agencies' impairments. In its April 3, 2019 letter to the Department regarding its top open recommendations, GAO included a recommendation from 2016 that emphasized the need for Treasury to address shortfalls in information technology (IT) workforce planning. While GAO acknowledged that some progress was made, Treasury had yet to develop an IT workforce plan that contained the key actions to address workforce skill gaps.[4] The security clearance process is still a culprit in the recruiting process and remained on GAO's 2019 high-risk list.[5]

Effective June 24, 2019, the responsibility for conducting background investigations was transferred from OPM's National Background Investigations Bureau to the Department of Defense's (DOD) Defense Counterintelligence and Security Agency. Although the intent of this transfer was to develop a unified approach for the security clearance process, there is uncertainty as to whether the transfer will reduce the delays in the clearance process for Treasury. In an effort to reduce the wait time for onboarding new personnel to fill special- sensitive and critical-sensitive positions, the Department implemented an investigative waiver request. If approved on a case by case basis, the Department may grant secret level clearance with the conditions that the employee has access to information at the secret level only. Employment is also conditioned on the favorable

[2] CFIUS is an interagency committee comprised of the departments of Commerce, Defense, Energy, Homeland Security, Justice, State, Treasury and the Office of the U.S. Trade Representative and the Office of Science and Technology.

[3] Public Law 115-232 (August 13, 2018).

[4] GAO, *Treasury Priority Recommendations* (GAO-19-325SP; April 3, 2019),

[5] GAO, *High-Risk Series, Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas* (GAO-19-157SP: March 2019).

completion of an investigation and issuance of an approved clearance. While this may bring staff on faster, it will not address the delay in the clearance process and meet the mission critical need to fill positions dealing with programs and materials of the highest sensitivity.

To further complicate matters, Treasury must also operate in the repeated cycle of budget and debt ceiling stopgaps. Legislation was passed in February 2018 to suspend the statutory debt limit through March 1, 2019.[6] Because no long-term solution had been found, the U.S. debt limit was reinstated at $22 trillion on March 2, 2019. When the statutory debt limit was reinstated, Treasury immediately implemented extraordinary measures to prevent the United States from defaulting on its obligations. Measures included (1) suspending State and Local Government Series securities sales, (2) declaring a "debt issuance suspension period" which suspended additional investments in the Civil Service Retirement and Disability Fund and Postal Retiree Health Benefits Fund, and (3) suspending investment in the Government Securities Investment Fund of the Federal Employees' Retirement System Thrift Savings Plan. In July 2019, Treasury informed Congress that these extraordinary measures would be exhausted before September 2019. Consequently, legislation was passed to suspend the statutory debt limit through July 31, 2021.[7] While the debt ceiling has been lifted, it is only temporary as Congress has yet to resolve unfinished business when it comes to the Nation's debt, and the long-term sustainability of the large programs. Although not included as a top open recommendation in its April 2019 letter to the Department, GAO raised the same concerns to Congress in its July 2015 report[8] with the approach to managing the federal debt limit and its impact on Treasury's borrowing costs and the need for alternative approaches.

The impact of this challenge and the uncertainties require the Department to focus its resources on programs that are in the highest need to citizens and/or where there is a unique federal role. It is essential that new programs and reforms be managed and communicated effectively for achieving performance and accountability.

Challenge 2: Cyber Threats (Repeat)

Cybersecurity remains a long-standing and serious challenge facing the Nation. A reliable critical infrastructure, including information systems and networks, is vital to our national security and economic stability. Cyber threats are a persistent concern as Treasury's information systems are critical to the core functions of government and the Nation's financial infrastructure. As cyber threats continue to evolve and become more sophisticated and subtle, they pose ongoing challenges for Treasury to fortify and safeguard its internal systems and operations along with the financial sector it oversees. Attackers frequently exploit vulnerable networks or systems in a string of trusted connections to gain access to government systems. Attempted cyber-attacks against Federal agencies, including Treasury, and financial institutions continue to increase in frequency and severity, in addition to continuously evolving. 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

[6] Public Law 115-123 (February 8, 2018).

[7] Public Law 116-37 (August 2, 2019).

[8] GAO, *Debt Limit: Market Response to Recent Impasses Underscores Need to Consider Alternative Approaches* (GAO-15-476; July 9, 2015).

systems and maintain a presence to enable future actions. Through cyber information sharing, Federal agencies are better prepared to thwart potential attacks to the cyber infrastructure of the Federal government and the financial sector that it serves. Ensuring the nations' cybersecurity continues to be reported as a government-wide issue on GAO's 2019 high-risk list.

As the tools used to perpetrate cyber-attacks become easier to use and more widespread, the less technological knowledge and fewer resources that are needed to launch successful attacks of increasing sophistication. Such attacks include distributed denial of service attacks, phishing or whaling attacks, fraudulent wire payments, malicious spam (malspam), ransomware, and compromise of supply chains. There has been growing concern with foreign adversaries creating and exploiting vulnerabilities in information and communication technology and services. To secure the supply technology and services chain, an Executive Order was issued on May 15, 2019 that bans 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.[9] 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 monitor developments in this area closely and plan for the possibility that its current supply chain may no longer be available in the near future.

In addition to Treasury's own networks and systems, management must be cognizant of, and mitigate, the risks posed by attacks made against other agencies and Treasury contractors and subcontractors. Treasury frequently enters into interconnection agreements with other Federal, State, and local agencies, and service providers, to conduct its business. Treasury management must exercise due care when authorizing such internetwork connections and verify that third parties comply with Federal policies and standards. Management is also challenged with ensuring that critical data and information maintained by third-party cloud service providers are properly protected. Issues related to management of cloud systems have been reported in four consecutive *Federal Information Security Modernization Act of 2014* [10] audits (fiscal years 2015, 2016, 2017, and 2018).

Additionally, effective public-private coordination continues to be required to address the cyber threat against the Nation's critical infrastructure. In this regard, 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. The Office of Critical Infrastructure Protection and Compliance Policy 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. The National Institute of Standards and Technology (NIST) updated its guidance to assist Federal agencies in managing cybersecurity risks.[11] In its 2018 report on adoption of the NIST framework by critical infrastructure sectors, GAO reported that the extent of adoption was unknown since agencies were not measuring framework

[9] *Executive Order on Securing the Information and Communications Technology and Services Supply Chain* (May 15, 2019).

[10] Public Law 113-283 (December 18, 2014).

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

implementation. With respect to Treasury, GAO 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 its April 2019 letter regarding its top open recommendations, GAO noted that Treasury had begun discussion with NIST to identify and develop methods for determining the level and type of framework adoption; however the recommendation remained open.

The Department reported steady progress over the past year to implement higher security settings for websites, web services, and e-mail. The Department also reported that it completed the first phase of implementing the Federal government-wide Continuous Diagnostics and Mitigation program aimed at providing agencies with the capabilities and tools needed to identify and prioritize cybersecurity risks on an ongoing basis and mitigate the most significant risks first. While progress was reported, resource constraints were noted. For example, the Department reported that evaluating and prioritizing remediation activities related to cybersecurity assessments of High Value Assets [12] had funding constraints. In response to our prior year memorandum, the Department acknowledged that six of its High Value Assets reside at Fiscal Service which is an inherent concentrated risk of cyber-attacks for Treasury. As discussed in challenge 1, we reported in prior audits that the cause for many of our information systems' findings involved a lack of resources and/or management oversight.

As an ongoing challenge, Treasury will need to balance cybersecurity demands while modernizing and maintaining IT systems. To this end, Treasury must ensure that cyber security is fully integrated into to its IT investment decisions as discussed in challenge 5.

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

Over the past year, TFI has remained dedicated to countering the ability of the 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 the financial networks that support rogue regimes, terrorist organizations, transnational criminal organizations, and other threats to the national security of the United States and our allies continues to be challenging as TFI's role to counter these financial networks and threats has grown because its economic authorities are key tools to carry out U.S. policy. In 2018, the Office of Foreign Assets Control (OFAC) designated approximately 1,500 persons to the list of Specially Designated Nationals and Blocked Persons (SDN)[13] which is approximately 50 percent more than it has ever added to the list in any single year. Additionally, criminals and other bad actors evolve and continue to develop more sophisticated money laundering methods in

[12] 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.

[13] SDN list includes individuals and entities designated in connection with activity involving sanctioned countries. It also lists individuals, groups, and entities such as terrorists and narcotics traffickers designated under sanctions programs that are not country-specific. Unless an exemption from regulation applies or OFAC authorizes a transaction under a license, all transactions by U.S. persons, including U.S. depository institutions, or transactions in or involving the United States are prohibited if they involve an individual or entity on the SDN list. U.S. persons must also block designated persons' property and interests in property within their possession or control.

an attempt to avoid detection. As noted in challenge 1, TFI requested approximately 50 new positions for fiscal year 2020 to address this growing demand.

TFI's authorities are key tools in implementing U.S. policy to pressure foreign countries and regimes, such as North Korea, Russia, and Iran, and terrorist groups, such as the Islamic State of Iraq and Syria (ISIS) through the use of designations and economic sanctions. TFI has significantly increased sanctions against North Korea for missile testing and it serves a critical role in the U.S.'s maximum economic pressure campaign. TFI also increased sanctions against Russia related to malign activities, such as interfering with the 2016 U.S. election, and support of the Government of Syria. As a result of the U.S. decision to withdraw from the Joint Comprehensive Plan of Action (JCPOA),[14] TFI re-imposed nuclear related primary and secondary sanctions, subject to certain 90 and 180 day wind-down periods for activities involving Iran. TFI continues to designate Iranian individuals and entities related to its ballistic missile program, terrorist activities, and human rights violations.

TFI's counter-terrorism designations disrupt the financial networks that support terrorist organizations. Disrupting terrorist financing depends on a whole-of-government approach and requires collaboration and coordination within Treasury and with other Federal agencies. Collaboration and coordination are key to successfully identifying and disrupting all of these 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.

Effective coordination and collaboration and TFI's ability to effectively gather and analyze intelligence information requires a stable cadre of experienced staff. As of this writing, TFI management stated that 81 of the 100 positions approved in fiscal year 2019 were filled. The office requested another 50 new positions for fiscal year 2020. The security clearance process has significantly impacted Treasury's human capital management as noted in our first challenge and is a systemic issue government-wide. If approved, the additional TFI positions may be difficult to fill because of the expertise needed and length of time to process required security clearances. As of this writing, it remains unknown if the transfer of background investigations from OPM to DOD's Defense Counterintelligence and Security Agency will decrease Treasury's wait time for onboarding skilled personnel to fill special- sensitive and critical-sensitive positions.

Data security and information sharing are challenges for the Financial Crimes Enforcement Network (FinCEN), which has experienced unauthorized disclosures of Bank Secrecy Act information. FinCEN is required to maintain a highly secure database for financial institutions to report suspicious activity. FinCEN has previously identified that the success of that system depends on the financial sector's confidence that those reports are adequately protected, but recent data breaches threaten to undermine that confidence. FinCEN is also required to maintain a government-wide data access service to make information available and useful to Federal, State,

[14] In July 2015, an international coalition, comprised of China, France, Germany, Russia, the United Kingdom, and the United States, reached the JCPOA to ensure that Iran's nuclear program would be exclusively peaceful. The JCPOA provides a long-term, multiphase commitment that deters Iran's path to build a nuclear weapon and imposes rigorous inspections and transparency measures to verify that Iran cannot pursue a nuclear weapon. In May 2018, it was announced that the United States would cease participation in the JCPOA.

local, and foreign law enforcement agencies and appropriate regulators and to support intelligence and counterintelligence activities and anti-money laundering initiatives. The challenge for FinCEN is to ensure the Bank Secrecy Act data remains secure in order to maintain the confidence of the financial sector while meeting the access needs of law enforcement, regulatory, and intelligence partners.

Given the criticality of Treasury's 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.

Challenge 4: Efforts to Promote Spending Transparency and to Prevent and Detect Improper Payments (Repeat)

Given the broad implications and critical roles assigned to Treasury by the Digital Accountability and Transparency Act of 2014 (DATA Act), we consider this project a management challenge. Since last year's memorandum, the Department continued to align its systems and execute a comprehensive governance framework to meet the submission and certification requirements of the DATA Act. Treasury's DATA Act Project Management Office continued to refine its processes to address Government-wide implementation challenges through corrective actions to improve data quality for Federal spending transparency.

In its efforts to promote spending transparency and use of federal financial data in order to strengthen government-wide decision-making, Treasury launched the Data Lab. The Data Lab is designed to increase the public understanding of Federal spending using interactive data visualizations and analyses on USASpending.gov. Further, Treasury's Office of the Deputy Chief Financial Officer, working together with the Office of the Procurement Executive, developed and executed remediation efforts focused on training and other related activities, including the development of a more comprehensive remediation plan. In May 2019, the Department released its Data Quality Plan which outlines the control environment for DATA Act reporting, provides a framework for remediating data quality issues, and documents initial remediation strategies and targeted timeframes for implementing such strategies to improve its reporting of Federal spending and award data.

Since 2014, we have engaged in a series of ongoing audits of Treasury's efforts to meet its responsibilities under the DATA Act. As of this writing, we are performing an audit focusing on the Department's continued efforts to report financial and award data and address data quality concerns we identified in our November 2017 report.[15]

Within the next fiscal year, the Department must implement government-wide reforms for making data accessible and useful for decision-making as authorized by the *Foundations for Evidence-Based Policymaking Act of 2018* [16] (Evidence Act). Among several requirements, departments and agencies must submit annually to Congress and OMB, an evidence-building plan for identifying and addressing policy questions relevant to programs, policies, and regulations. In addition, agencies must develop a plan to evaluate the activities pursuant to their evidence-based plans.

[15] OIG, *Treasury Continues to Make Progress in Meeting DATA Act Reporting Requirements, But Data Quality Concerns Remain* (OIG-18-010R; November 8, 2017).

[16] Public Law 115-435; (January 14, 2019).

Under Title II of the Evidence Act, also known as the *Open, Public, Electronic, and Necessary Government Data Act* or the "*OPEN Government Data Act*," Federal agencies must develop a strategic information resources management plan that includes, among other things, an open data plan that requires agencies to develop processes and procedures making data collection mechanisms created on or after enactment to be available in an open format. The strategic information resources management plan and open data plan must be updated annually and made publicly available on agency websites. Federal agencies must also develop and maintain a data inventory to be included in the Federal Data Catalogue[17] (www.Data.gov) developed and maintained by the General Services Administration.

The Evidence Act is a comprehensive government-wide undertaking with several moving parts to implementation that requires Treasury to work closely with OMB.

Detect Improper Payments

In light of the continuing government-wide problem with improper payments (estimated at $151 billion or 3.7 percent of all program outlays for fiscal year 2018),[18] the Federal Government intensified efforts to reduce improper payments in major Federal programs. The Do Not Pay (DNP) Initiative and the Fiscal Service's DNP Business Center are chief components of efforts designed to prevent and detect improper payments to individuals and entities.

The DNP Business Center provides two services to agencies: the DNP Portal and the DNP Data Analytics Service. The DNP Portal is intended to provide users with a single entry point to search data sources such as the Social Security Administration's (SSA) publicly available Death Master File, the Department of Health and Human Service Office of Inspector General's List of Excluded Individuals/Entities, the General Services Administration's System for Award Management, and Treasury's Debt Check Database. However, as we reported in November 2014, the effectiveness of the DNP Business Center as a tool to prevent and detect improper payments is hindered because the center does not have access to, among other things, SSA's full death data.[19] Since our May 2016 report, that challenge continues to exist in obtaining better death information.[20] In October 2016, GAO reported that restrictions on the center's access to SSA's full death data remained in place.[21]

In response to the *Federal Improper Payments Coordination Act of 2015*,[22] Fiscal Service entered into agreements with DOD and the Department of State in 2016 to incorporate death data collected by these agencies into the DNP Business Center Working System, which began receiving data in September 2017. In November 2017, OMB designated six additional databases for inclusion in the DNP Business Center Working System to help agencies address a broader range of improper

[17] A single public interface on-line as a point of entry for sharing data assets with the public.
[18] GAO, *The Nation's Fiscal Health*: *Action Is Needed to Address the Federal Government's Fiscal Future* (GAO-19-314SP; April 10, 2019); percentage based on total Government outlays of 4.1 billion (https://www.fiscal.treasury.gov/files/reports-statements/mts/mts0918.pdf).
[19] OIG, *Fiscal Service Successfully Established the Do Not Pay Business Center But Challenges Remain* (OIG-15-006; November 6, 2014).
[20] OIG, *Fiscal Service Faces Challenges in Obtaining Better Death Information for the Do Not Pay Business Center, but Alternatives Exist* (OIG-16-042; May 18, 2016)
[21] GAO, *Improper Payments, Strategy and Additional Actions Needed to Help Ensure Agencies Use the Do Not Pay Working System as Intended* (GAO-17-15; October 14, 2016).
[22] Public Law 114-109 (December 18, 2015).

payments beyond what can be detected through DNP Business Center's previously existing data sources.[23] There have been legislative proposals in January 2017, February 2017, February 2018, and May 2019 to obtain authorization to use both the SSA's full death file as well as the National Directory of New Hires. [24]

The DNP Data Analytics Service supports agencies' efforts to identify and prevent improper payments by identifying trends and patterns in agency payment and other information that may be indicative of improper payments. The results of these analyses are provided to agencies at no cost for further study so they can prevent future improper payments. We have an audit in progress to assess the services provided to agencies by the DNP Data Analytics Service.

With its potential to reduce improper payments, the DNP Business Center is a major and important undertaking by Treasury. As part of our ongoing audit work in this area, we will continue to monitor the steps taken by Fiscal Service to improve the effectiveness of the DNP Business Center.

Challenge 5: Information Technology Acquisition and Project Management (New)

The *Federal Information Technology Acquisition Reform Act* (FITARA), enacted in December 2014, was the first major overhaul of Federal IT management since the passage of the *Clinger-Cohen Act of 1996* [25] which was designed to improve the Federal Government's acquisition and management of its resources to include IT investment. Among other things, it expanded the involvement of Chief Information Officers (CIO) of Federal agencies in IT decision making, including annual and multi-year planning, programming, budgeting, execution, reporting, management, governance, and oversight functions.[26] FITARA was intended to improve how Federal agencies acquire and manage IT, as well as, enable Congress to monitor progress and hold Federal agencies accountable for reducing duplication and achieving cost savings. FITARA includes specific requirements related to seven areas: (1) the Federal data center consolidation initiative, (2) enhanced transparency and improved risk management, (3) agency CIO authority enhancements, (4) portfolio review, (5) expansion of training and use of IT acquisition cadres, (6) government-wide software purchasing, and (7) maximizing the benefit of the Federal strategic sourcing initiative.

While FITARA was intended for agencies to better manage their IT investments, implementation continues to be a government-wide challenge. Since February 2015, GAO has included the management of IT acquisitions and operations on its high-risk list as cost overruns and schedule delays impact mission related outcomes government-wide.[27] In its March 2019 high risk report, GAO acknowledged that the executive branch has undertaken numerous initiatives to better

[23] The following databases were added: (1) Treasury's Office of Foreign Assets Control's SDN list (OFAC List), (2) the General Services Administration's System for Award Management (SAM), (3) the Internal Revenue Service's (IRS) Automatic Revocation of Exemption List, (4) the IRS's Exempt Organizations Select Check, (5) the IRS's e-Postcard database, and (6) the commercial database American InfoSource (AIS) Deceased Data.

[24] The National Directory of New Hires (NDNH) is a national database of wage and employment information operated by the Federal Office of Child Support Enforcement (OCSE). OCSE uses the NDNH primarily to assist states administering programs that improve States' abilities to locate parents, establish paternity, and collect child support. The information in this database is only available to authorized persons or entities for authorized purposes.

[25] Public Law 104-106 (February 10, 1996).

[26] Public Law 113-291 (December 19, 2014).

[27] GAO, *High- Risk Series*, *An Update* (GAO-15-290; February 11, 2015).

manage the more than $90 billion that is invested annually in IT. However, GAO reported that more needed to be done to improve overall management of IT acquisitions and operations and recommended that, in general, agencies needed to improve CIO's authorities, establish action plans to modernize and replace obsolete IT investment, and address weaknesses in IT Dashboard[28] reporting of IT investment risk and incremental development implementation. [29] For example, none of the 24 major Federal agencies, including Treasury, had IT management policies that fully addressed the role of their CIOs. Further, the majority of the agencies did not assess the CIO role in assessing agency IT workforce needs, and developing strategies and plans for meeting those needs.

The House Oversight and Reform Committee worked with GAO to develop a biannual scorecard to assess Federal agencies' efforts in implementing FITARA by assigning a grade from A to F based on self-reported data at the agency level. Agencies are scored on areas of CIO authority enhancements, transparency and risk management, portfolio review, data optimization, software licensing and modernizing government technology. Since the first scorecard was issued in November 2015 Treasury's overall FITARA score has wavered between a D- and C-. Areas needing most improvement were enhanced transparency and risk management (i.e. IT investment risk) and improved cybersecurity. The *FITARA Enhancement Act of 2017* [30] extended the sunset date for full implementation of the data center optimization requirements of FITARA from October 1, 2018 to October 1, 2020. As of the end of fiscal year 2018, Treasury met its data center closure target, but did not achieve its other targets in the data center optimization initiative.

In fiscal year 2019, Treasury reported $1.8 billion in non-Internal Revenue Service (IRS) IT investment, which is expected to increase in fiscal year 2020. Given this sizable investment, we are reporting the Department's IT acquisition and project management as a new management and performance challenge distinct from challenge 2 that addresses cybersecurity concerns.

A more recent initiative to manage and monitor IT investments includes the government-wide adoption of the Technology Business Management (TBM) framework as reported in the fiscal year 2018 *President's Management Agenda: Modernizing Government for the 21st Century* (March 20, 2018). The goal is to improve outcomes through Federal IT spending transparency with the adoption of TBM government-wide by fiscal year 2022. TBM is expected to improve IT spending data accountability and transparency, empowering agency executive suite leadership from across the enterprise to drive mission value and improve customer experience through technology. This initiative will be led by OMB with General Services Administration's Office of Government-Wide Policy team and with Executive Councils.

In fiscal year 2019, Treasury's non-IRS bureaus reported 23 major IT projects. Treasury's CIO assessed 20 projects as having moderately low or low risk to accomplishing their goals. The

[28] IT Dashboard was launched in June 2009 to provide agencies and the public the ability to view details of Federal IT investments and track progress over time.
[29] GAO, *High-Risk Series, Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas* (GAO-19-157SP: March 2019).
[30] Public Law 115-88 (November 21, 2017).

remaining three IT projects, which reside at Fiscal Service, were assessed as having medium risk[31] to accomplishing their goals:

- Electronic Federal Tax Payment System (EFTPS),
- Post Payment Services (PPS), and
- Wholesale Securities Services (WSS).

Select projects within EFTPS and PPS were behind schedule and over budget, while WSS had select projects that were behind schedule. Although projects identified with medium overall risk in cost and scheduling require special attention from the highest level of agency management, they are not necessarily at risk for failure. We plan to initiate an audit of these IT acquisitions. Overall, 80 percent of Treasury's total IT projects were on schedule and 56 percent were on budget. During fiscal year 2019, Treasury spent 33 percent of its total IT spending on 41 major investments.

Non-IT related acquisitions also require attention to ensure timely delivery and minimize cost overruns for achieving cost savings. The *Program Management Improvement Accountability Act*[32] was intended to improve program and project management practices across the Federal Government. Similar to IT projects, other major acquisitions need to be monitored so that the project goals are met in a timely manner and costs are not allowed to significantly exceed established budgets. In prior years, we have reported our ongoing concern over the Bureau of Engraving and Printing's (BEP) outdated Washington D.C. facility with limited capabilities to produce $100 notes and the need for a new facility to ensure continuity of operations at the bureau. With recent passage of the Agriculture Act of 2018, the Secretary of Agriculture will transfer to the Secretary of the Treasury administrative jurisdiction over a parcel of real property in Beltsville, Maryland, for a new BEP facility. The Secretary of Agriculture entered into a binding memorandum of agreement with the Secretary of the Treasury regarding the responsibilities, including financial responsibilities, of each party for evaluating and, if necessary, remediating or otherwise addressing hazardous substances, pollutants, or contaminants found at the parcel. BEP has requested $30 million in its FY 2020 budget to begin preparation of the site for BEP's new facility. This money is for BEP to provide to the General Services Administration for surveys, environmental studies, transportation, and employment of construction and management contractors. BEP will need to ensure it employs effective contract and project oversight for preparation of the land, construction of the building, purchase of equipment and machinery, and employment of a workforce to ensure continuity of operations at the bureau. We have included an audit of BEP's management of this large construction project in our Annual Plan for Fiscal Year 2020.

Other Matters of Concern

Although we are not reporting these as management and performance challenges, we are highlighting two areas of concern: (1) coin redemption and (2) managerial cost accounting.

[31] IT Dashboard, "the Agency CIO rates each investment based on his/her judgment using a set of pre-established criteria. As a rule the evaluation should reflect the CIO's assessment of risk and the investment's ability to accomplish goals." Evaluation ratings are based on five-point risk scale as follows: 5-low risk, 4= moderately low risk, 3= medium risk, 2= moderately high risk, and 1=high risk.

[32] Public Law 114-264 (December 14, 2016).

Coin Redemption

On January 19, 2018, the Mint recommenced its mutilated coin redemption program, which was suspended in 2016, with procedures to enhance the validation of the sources of these coins. However, as of April 24, 2019, the Mint temporarily ceased processing applications and material submitted to its mutilated coin redemption program pending the development of additional program safeguards to mitigate risks identified in our current audit. The Mint's internal control related to safeguarding and ensuring the integrity of U.S. coinage is a concern. As of this writing, the Director of the Mint confirmed that plans are being implemented to address this concern.

Managerial Cost Accounting

Managerial cost accounting is a fundamental part of a financial performance management system. It involves the accumulation and analysis of financial and nonfinancial data, resulting in the allocation of costs to organizational pursuits, such as performance goals, programs, activities, and outputs. As of this writing, we are auditing Departmental Offices' (DO) Office of Budget and Travel's (OBT) controls over its overhead [33] process and compliance with the *Economy Act*.[34] Early in our audit, we communicated with OBT management our concerns related to internal control weaknesses identified within OBT's overhead process used to charge reimbursable customers. That is, OBT's methodology to accumulate, allocate, and charge overhead costs to reimbursable customers was not appropriate or consistently followed. Therefore, we expressed concern of a potential *Economy Act* violation in fiscal year 2015 by OBT not recovering actual costs from reimbursable customers. Further, OBT potentially augmented its fiscal year 2015 appropriation by recovering indirect costs in excess of actual costs from reimbursable customers. OBT followed the same overhead process for fiscal years 2015 through 2018, which was recently changed in fiscal year 2019. Our office has an ongoing audit that is reviewing this new process.

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: David Eisner
Assistant Secretary for Management

[33] Overhead, also known as indirect costs, are items which are commonly recognized as elements of cost that may not have resulted in direct expenditures. It covers the cost of administrative expenses associated with financial management, human resources, information technology, general counsel and other support related to providing reimbursable services to customers.

[34] Public Law 73-2 (March 20, 1933)