DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

October 29, 2020

**INFORMATION MEMORANDUM FOR SECRETARY MNUCHIN**

**FROM:** Richard K. Delmar /s/
Deputy Inspector General

**SUBJECT:** Management and Performance Challenges Facing the Department of the Treasury (OIG-CA-21-006)

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 six challenges, one of which one is new and reports on Treasury's role in combatting the economic fallout of the Coronavirus Disease 2019 (COVID-19) global pandemic at the forefront of the Nation. Five challenges are repeated and updated from last year to include COVID-19 impacts on related workforce and work streams.

- COVID-19 Pandemic Relief (New)
- 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 (Repeat)

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), (2) managerial cost accounting, and (3) internal control matters at the Bureau of Engraving and Printing (BEP).

We identified challenges and concerns based on the threat they pose to Treasury's mission and stakeholders' interests. We also acknowledge the Department's accomplishments and efforts over the past year to address critical matters as noted within each challenge. That said, the COVID-19 pandemic has caused a global health emergency and an ensuing economic crisis that Treasury has spent the second half of fiscal year 2020 tackling. As noted throughout the challenges, Treasury had to act swiftly, and in some cases, draw on its existing resources to meet the more recent economic needs.

## 2021 Management and Performance Challenges

### Challenge 1: COVID-19 Pandemic Relief (New)

The COVID-19 pandemic has affected the health and economic stability of communities worldwide. In the United States alone, more than 8.7 million people have been infected with more

than 225,000 deaths[1] reported as of this writing. In March 2020, Congress passed three key pieces of legislation in succession to address the COVID-19 health crisis and the economic fallout affecting individuals, businesses, and other industry sectors. On March 6, 2020, the Coronavirus Preparedness and Response Supplemental Appropriation Act of 2020 was signed into law providing $8.3 billion in emergency funding to address health and medical care. [2] Shortly thereafter, the Families First Coronavirus Response Act was enacted on March 18, 2020 to address the financial stress of individuals and households with approximately $104 billion in funding.[3] The Coronavirus Aid, Relief, and Economic Security Act (CARES Act),[4] which is by far the largest relief funding to date, passed on March 27, 2020. The CARES Act provided over $2.4 trillion in health and economic relief to hospitals and healthcare providers, individuals and households, businesses and employees, as well as, states, local and tribal governments, and Federal agencies, among other things.

Treasury has been instrumental in implementing and/or supporting other Federal agencies in implementation of economic relief provisions of the CARES Act. To assist individuals and households, Treasury directed approximately $468 billion in Economic Impact Payments (EIP)[5] to workers and households through the Internal Revenue Service (IRS). Through the IRS, Treasury also implemented the Employee Retention Tax Credit and Payroll Tax Deferral CARES Act provisions to protect workers and jobs. Treasury also assisted the Small Business Administration (SBA) in carrying out the Paycheck Protection Program[6] and the Economic Injury Disaster Loans authorized by the CARES Act. SBA's Paycheck Protection Program authorized $349 billion to support payroll, benefits, and other operating costs of small businesses for up to 24 weeks[7] in order to keep workers on the payroll. The Economic Injury Disaster Loans provides authority for small businesses to receive an advance loan up to $10,000 to cover revenue loss due to COVID-19. In addition to all this, the Department established programs to preserve airline industry jobs, provide liquidity to the financial sector, and disbursed payments to other levels of government within the United States impacted by the increasing costs caused by the COVID-19 pandemic. The Emergency Relief and Taxpayer Protections (commonly referred to as Section 4003) provisions authorized Treasury to make up to $500 billion in loans, loan guarantees, and other investments to eligible businesses, Sates, and municipalities. Up to $46 billion of this amount was made available as loans and loan guarantees to air passenger carriers ($25 billion), air cargo carriers ($4 billion), businesses engaged in national security ($17 billion) and up to $454 billion was made available as loans, loan guarantees and other investments in programs and facilities of the Board of Governors of the Federal Reserve System to provide liquidity to the financial system. The Emergency Relief and Taxpayer Protections provisions also authorized the establishment of the Special Inspector General for Pandemic Recovery (SIGPR) within Treasury to oversee $500 billion in loans, loan guarantees, and other investments provided by Treasury.

---

[1] CDC COVID Data Tracker.
[2] Public Law 116-123 (March 6, 2020).
[3] Public Law 116-127 (March 18, 2020).
[4] Public Law 116-136 (March 27, 2020).
[5] IRS estimate as of April 24, 2020.
[6] The Payroll Protection Program received an additional $321 billion under the *Paycheck Protection Program and Healthcare Enhancement Act* (Public Law 116-139; April 24, 2020).
[7] The Paycheck Protection Program Flexibility Act of 2020 (Public Law 116-142, June 5, 2020), extended the covered period for loan forgiveness from 8 weeks after the date of loan disbursement to 24 weeks after the date of loan disbursement.

Although some of the aforementioned CARES Act provisions do not fall under the oversight jurisdiction of my office, the payment work streams and mechanisms administered by the Bureau of the Fiscal Service (Fiscal Service) do. In the context of this overarching challenge, we recognize the breadth and scope of Treasury's responsibilities as it impacts programs, operations, and activities regardless of jurisdictional oversight boundaries. The CARES Act provisions within the oversight purview of my office are those that support airline industry workers and state, local, territorial, and tribal government entities through direct financial assistance.

To maintain pay and benefits of airline industry workers, Treasury implemented the Air Carrier Worker Support (hereinafter referred to as the Payroll Support Program) provisions of the CARES Act that authorized up to $32 billion of direct financial assistance for passenger air carriers ($25 billion), cargo air carriers ($4 billion), and contractors ($3 billion). Financial assistance is to ensure the continuation of workers' payroll and benefits with the stipulation that employees are not involuntarily furloughed and do not receive reductions in pay and benefits. Many requirements for this program, such as program procedures, were implemented within days of the CARES Act enactment. Using existing resources and contractor support, Treasury quickly stood up the Payroll Support Program to establish, among other things, the application requirements for requesting financial assistance, terms and conditions for receiving financial assistance, and subsequent compliance monitoring of air carriers and contractors. Treasury also consults with the Department of Transportation (DOT) on the larger air carriers that report financial information to DOT on a regular basis (referred to as 241 carriers[8]). As you are aware, the CARES Act requires my office to audit the certifications of sworn financial data submitted to Treasury by passenger and cargo carriers and contractors that do not report to DOT (referred to as non-241 carriers). While my office has ongoing audits of Treasury's program implementation and non-241 carriers' certifications submitted to Treasury, it is incumbent upon the Department to establish and maintain strong internal control over recipients' compliance with signed terms and conditions for receiving financial assistance. That is, Treasury's compliance monitoring function is essential to ensuring that recipients use funds for the continuation of salaries and benefits as intended.

The $150 billion Coronavirus Relief Fund, established under Title VI of the Social Security Act, as amended by Title V of the CARES Act, has been a large endeavor for both the Department and my office. The Department was responsible for making direct payments to States, units of local government, the District of Columbia, U.S. Territories, and Tribal governments. Disbursement of funds was a complicated undertaking given the number of recipients at varying levels of government and other payment requirements of the CARES Act. That is, payments to States and local units of government were formula-driven and based on the 2019 U.S. Census, while other payments were based on consultations with the Department of the Interior and Tribal Governments and other information obtained by the Department. The CARES Act created a unique challenge in distinguishing between the programmatic administrative responsibility for payments made from the Coronavirus Relief Fund and the Treasury Office of Inspector General's (OIG) independent oversight. Although Treasury was authorized to make payments, the CARES Act assigned Treasury OIG with responsibility for monitoring and oversight of the receipt, disbursement, and use of funds. Additionally, my office was given authority to recoup funds if it is determined that recipients fail to comply with uses of funds for COVID-19 related costs under

[8] 14 CFR Part 241, Uniform System of Accounts and Reporting for Large Certified Air Carriers.

Section 601 (d), "Uses of Funds," of the Social Security Act, as amended.[9] Given the direct oversight authorities of the Treasury OIG, the Department did not establish an administrative program to ensure recipient compliance. Recipients were not bound to any terms and conditions for the receipt of funds. We reported this in our first audit of the Coronavirus Relief Fund regarding the lack of terms and conditions and accountability and transparency of funds.[10] While this is unusual for a Federal agency that administers financial assistance programs, Treasury officials stated commitment to supporting our oversight role for ensuring transparency, accountability, and adherence to all statutory requirements and will continue to collaborate with us to ensure compliance by recipients. This continued collaboration is critical for overseeing such a large and widely dispersed recipient population given the challenges of defining and interpreting eligible uses of Coronavirus Relief Fund proceeds. That said, it is crucial that the Department maintain its fundamental role to establish and interpret policy over the uses of funds. As recipients are still in the process of using these funds, we anticipate that questions will continue to arise that will require interpretation and changes to Treasury's guidance and Frequently Asked Questions. Providing as much clarity as possible over allowable uses of Coronavirus Relief Fund proceeds is essential for ensuring recipients understand the compliance requirements and are accountable and transparent in how they report uses of funds. As part of my office's compliance monitoring and oversight function, we established a portal using GrantSolutions[11] for recipients to report their uses of funds on a quarterly basis starting September 2020 through the quarter ending September 2021. Recipient data will be reported to the newly created Pandemic Response Accountability Committee (PRAC) for display on its website (https://pandemicoversight.gov).

Along with administering and delivering economic relief, Treasury must manage the unprecedented oversight that CARES Act funding is subject to. In addition to my office's ongoing work on the Payroll Support Program and the Coronavirus Relief Fund, Treasury is subject to a number of additional CARES Act oversight provisions. As mentioned above, SIGPR was created to oversee $500 billion in "loans, loan guarantees, and other investments" provided by Treasury[12] and must report to congress 60 days after Senate confirmation, and quarterly thereafter, on SIGPR's activities and Treasury's loan programs. A Congressional Oversight Commission was established to report to Congress on Treasury's and the Federal Reserve Board's implementation activities under Title IV, Subtitle A, "Coronavirus Economic Stabilization Act of 2020." Moreover, the commission is required to report every 30 days on the use of contractors and administration of loan programs, the impact of programs on the nation's financial wellbeing, whether required disclosures of the CARES Act provide market transparency, and effectiveness of maximizing benefits and minimizing costs to taxpayers, among other things.[13] The PRAC, created within the Council of Inspectors General on Integrity and Efficiency, is comprised of Inspectors General of agencies involved in the COVID-19 response to include Treasury Inspector General for

---

[9] Section 601 (d), Use of Funds, " to cover only those costs of the State, Tribal government, or unit of local government that (1) are necessary expenditures incurred due to the public health emergency with respect to COVID–19; (2) were not accounted for in the budget most recently approved as of the date of enactment of this section for the State or government; and (3) were incurred during the period that begins on March 1, 2020, and ends on December 30, 2020."

[10] OIG, *Interim Audit Update–Coronavirus Relief Fund Recipient Reporting* (OIG-20-036; May 27, 2020).

[11] GrantSolutions is a grant program management Federal Shared service provider under the U.S. Department of Health and Human Services.

[12] SIGPR terminates five years after enactment of the CARES Act (March 27, 2025).

[13] The Congressional Oversight Commission issued its first report on May 18, 2020 (https://hill.house.gov/uploadedfiles/coc_1st_report_05.18.2020.pdf).

Tax Administration (TIGTA), SIGPR, and my office.[14] The CARES Act also provided additional funding to the Government Accountability Office (GAO) and Offices of Inspectors General to augment oversight of CARES Act programs and activities. Among several oversight reporting provisions, GAO is required to conduct a study of "loans and loan guarantees, and other investments" authorized under Section 4003.[15]

With no clear end to the COVID-19 pandemic in sight, Treasury must continue to navigate through this challenging time and be prepared to administer another fast-paced relief package in the near future, if legislated. To date, Treasury has been able to leverage its existing workforce and hired contractors to address the demands of the CARES Act workload. That said, there was reported strain associated with working remotely while managing normal responsibilities and additional work due to the COVID-19 pandemic. Going forward, Treasury may experience difficulties in balancing its new responsibilities and workloads while managing several ongoing challenges as described throughout this memorandum. While I am hopeful that fiscal year 2021 will see an end to the horrific fallout that the COVID-19 pandemic has had on our nation, I am also mindful that challenges lay ahead for both Treasury and my office in the short-term.

**Challenge 2: Operating in an Uncertain Environment (Repeat)**

The COVID-19 outbreak presented unique complexities for Treasury to include, among other things, implementing measures for the health and safety of its workforce, as well as, administering more than $2 trillion in financial assistance under the CARES Act. Despite these challenges, Treasury responded with limited onsite staff and details from within Treasury, other Federal agencies and outside contractors. Treasury acted quickly to work with its business partners[16] to prepare disbursements of more than 160 million of EIPs totaling over $267 billion within two months after the passage of the CARES Act; $28 billion in financial assistance under the Payroll Support Program to hundreds of companies in the aviation industry; up to $500 billion in loans to the aviation industries ($46 billion administered by Treasury, and the remainder through the Federal Reserve); $150 billion to state, local, territorial, and tribal governments; as well as working closely with the Small Business Administration to disburse up to $659 billion to over 5 million small businesses through the Payroll Protection Program and $190 billion through the Economic Injury Disaster Loan program.

In addition to its normal payment operations and the delivery of EIPs, Fiscal Service also facilitated the delivery of billions of dollars in other CARES Act funding and other urgent agency payments as a result of the pandemic in the most efficient and effective manner. Fiscal Service is also leveraging existing resources and processes in the disbursement of payments related to the Payroll Support Program and Coronavirus Relief Fund, as well as, disbursements under the "Coronavirus Economic Stabilization Act" under the oversight of SIGPR. Even with these

---

[14] PRAC is comprised of Inspectors General of the departments of Defense, Education, Health and Human Services, Justice, Labor, Treasury, and TIGTA, and any other Inspector General, as designated by the Chairperson of the PRAC from any agency that expends or obligates covered funds or is involved in the Coronavirus response. The PRAC is to promote accountability and transparency of CARES Act funds and has established a public-facing website to make use of funds publically available. PRAC also has authority to conduct and support audits and investigations of the COVID-19 responses to mitigate risks across Federal programs and agencies, as well as, provide management alerts to Congress and the President on issues requiring immediate attention.

[15] Coronavirus Economic Stabilization Act of 2020 (Section 4026(f)).

[16] Partners include the Federal Reserve Banks (Kansas City and St. Louis), financial agents, and vendors.

additional responsibilities, Fiscal Service continued to process payments on behalf of more than 250 Federal entities, including salaries, benefits, tax refunds, and vendor/miscellaneous payments. These payments were processed on time and in accordance with agency disbursement instructions. As noted in challenge 5, Fiscal Service plans to leverage its Do Not Pay (DNP) Initiative and DNP Business Center to assist programs making CARES Act payments in the identification and prevention of improper payments.

Departmental Offices re-allocated resources to implement and administer other responsibilities under the CARES Act. The Office of the Assistant Secretary for Management (OASM) provided resources to support implementation to ensure that approximately $180 billion of disbursements related to the Payroll Support Program and the Coronavirus Relief Fund were properly authorized and processed for delivery to Fiscal Service for payment. The Office of CARES Operations was established within OASM, to support the implementation of applicable provisions of the Coronavirus Economic Stabilization Act of 2020 (under SIGPR's oversight jurisdiction) and the Payroll Support Program. The Office of CARES Operations is broken into seven components to include Administrative and Budget, Performance Reporting and Data Analytics, IG and GAO Interface, Risk Management, Asset Management and Recipient Monitoring, Process Controls and Compliance, and Data Management. The Office of the Deputy Assistant Secretary for Human Resources and Chief Human Capital Officer (DASHR/CHCO), along with other Departmental Offices' detailed personnel, has allocated staff time to filling positions for the Office of CARES Operations and other project teams.

In other support efforts, the Office of the DSHR/CHCO and the Office of Strategic Planning and Performance Improvement (OSPPI) worked to incorporate Treasury's CARES Act responsibilities into the Treasury Strategic Plan and draft interim enterprise learning agendas. The Director of OSSPI helped to stand up the Office of CARES Operations, including planning, prioritization, project management, and establishing team norms and business practices. The Office of Privacy, Transparency and Records is managing higher volumes of Freedom of Information Act requests, while the Office of Risk Management has dedicated resources to develop a risk profile for the Office of CARES Operations that will be regularly updated over time. The Office of Budget and Travel (OBT) has shifted portfolios and workloads to accommodate additional work associated with working groups established within the OASM to process payments under the Payroll Support Program and the Coronavirus Relief Fund and to provide budget execution assistance with administrative funding Treasury received under the CARES Act.[17] The Office of the Deputy Chief Financial Officer worked to determine appropriate accounting treatment for complex CARES Act financial transactions, designed and implemented internal controls for CARES Act processes across Departmental Offices, and formulated credit models and related asset valuations for the various CARES Act investments and direct loans. Additionally, the Office of Chief Information Officer has worked on the site development of the CARES Act portal used by the Office of CARES Operations to monitor recipient compliance with the Payroll Support Program requirements.

[17] Under Division A of the CARES Act, Treasury was authorized $25 million under Title I to carry out Section 1109 related to establishing criteria for insured depositories and credit unions participating in the Paycheck Protection Program, among other things; and up to $100 million to carry out the Air Carrier Worker Support provisions under Title IV, Subtitle B.

While this additional level of effort was not anticipated at the beginning of fiscal year 2020, the Office of the DASHR/CHCO was able to address new work-streams. The Office of DASHR/CHCO recruited and on-boarded over 90 details from within Treasury and across the Federal government to work across all CARES Act functions. Nevertheless, some Treasury officials have raised concerns over the possibility of a lapse in appropriations during fiscal year 2021, and the disruption it would cause to implementation timelines and organizational performance processes. Additionally, concern was raised that with anticipated funding levels for fiscal year 2021, the cost associated with administering certain CARES Act programs may have an impact on Treasury's ability to fund other work.

While Treasury faces unforeseen challenges working through the COVID-19 pandemic going into fiscal year 2021, other previously reported uncertainties have yet to be resolved. As conveyed in prior years' memoranda, it is still unknown what the potential impacts of OMB's comprehensive "Government–wide Reform Plan and Reorganization Recommendations" (Government–wide Reform Plan) will be. OMB made agency-specific recommendations that would merge functions with similar missions across agencies. In response to OMB's proposed recommendation to transfer 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), Treasury has included a request for funding in the fiscal year 2021 budget to initiate the transfer and implementation of this enforcement program, which includes the transfer of enforcement authority for the Contraband Cigarette Trafficking Act and the Prevent All Cigarette Trafficking Act. Other potential impacts on Treasury include OMB's recommendations to increase coordination between agencies and avoid duplication of roles for 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 (USPS), which is estimated to be insolvent; however, USPS continues to hold a $15 billion unfunded liability to the Treasury's Federal Financing Bank. On July 29, 2020, the USPS Board of Governors unanimously approved an agreement with Treasury on the terms and conditions associated with a $10 billion lending authority provided in the CARES Act. The agreement has yet to be finalized due to the House Committee on Oversight and Reform's concerns related to the loan terms of the agreement, which would permit the funding to be used only on operational expenses with Treasury's approval. 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.

Another matter on the horizon is the proposed transfer of the United States Secret Service (USSS) to Treasury from the United States Department of Homeland Security (DHS) included in the President's fiscal year 2021 budget. The transfer is intended to improve the response to cyber-enabled financial crimes and benefit national security efforts. USSS has approximately 6,500 employees and is a global organization with locations in the United States and across the world. DHS' fiscal year 2021 budget for USSS is a $2.36 billion appropriations request including $20 million for 119 additional personnel and $20 million in costs for the proposed transition of the USSS to Treasury. If USSS is transferred, Treasury faces challenges with providing the necessary resources and implementing the infrastructure, as well as cultural challenges involved with integrating and overseeing the large and diverse missions of the USSS. These primarily include physical protection of the Nation's highest elected leaders, visiting foreign dignitaries, and facilities and major events; investigation and forensic services to combat counterfeiting with a focus on securing the Nation's critical infrastructures, specifically in the areas of cyber, banking,

and finance; and investigative expertise and innovative approaches to the detection, investigation, and prevention of financial crimes. The potential transfer of USSS to Treasury will be a critical and complex undertaking by itself and will be challenging during the ongoing COVID-19 pandemic if legislation is passed.

Dealing with additional workloads, staffing, and other critical matters during the COVID-19 pandemic may be more challenging than usual. Two offices significantly impacted are the Office of International Affairs, which requested an increase in its staffing level from 81 employees to 120 employees by the end of calendar year 2021, to meet expanding workloads as discussed below; and the Office of Terrorism and Financial Intelligence (TFI), which requested approximately 50 new positions for fiscal year 2021 to address priorities discussed in challenge 4 of this memorandum. These positions could be difficult to fill if approved because of the expertise required for these positions. Human capital management overall remains an area of concern as the lengthy security clearance process and backlog of background investigations has only recently improved since the responsibility for conducting background investigations was transferred from the Office of Personnel Management's (OPM) National Background Investigations Bureau to the Department of Defense's (DOD) Defense Counterintelligence and Security Agency, effective June 24, 2019. The intent of this transfer was to develop a unified approach for the security clearance process. As a result of this new process, the Department has seen a decrease in the number of pending background investigations. With that said, the security clearance process is still a culprit in the recruiting process and remained on GAO's 2019 high-risk list.[18] However, in their continuous effort to reduce the wait time for onboarding new personnel to fill special- sensitive and critical-sensitive positions within TFI, the Department still has an investigative waiver request in place for granting interim clearances while clearances are being adjudicated. If approved on a case-by-case basis, the Department may grant a secret level clearance with the condition that the employee has access to information at the secret level only. Employment is also conditioned on the favorable completion of an investigation and issuance of an approved clearance. While this may bring staff on faster, the clearance process still naturally creates some delays in the hiring process that impacts the mission critical need to fill positions dealing with programs and materials of the highest sensitivity.

As noted above, an increase in staffing levels in the Office of International Affairs was proposed to address the expanding demands on the Committee on Foreign Investments in the United States[19] (CFIUS), which is charged with reviewing transactions involving foreign investments in the United States to determine national security risks. 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 (FIRRMA)[20] modernized the review process, it also expanded CFIUS' jurisdiction to address growing concerns over certain investment structures that were not within CFIUS' 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 issued two final regulations

[18] GAO, *High-Risk Series, Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas* (GAO-19-157SP: March 2019).
[19] 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.
[20] Public Law 115-232 (August 13, 2018).

in February 2020 to implement changes to jurisdiction and process. The FY 2020 budget cited an expected increase in workload from approximately 200 to 1,000 cases annually. Because CFIUS' expanded jurisdiction under FIRRMA became effective recently on February 13, 2020, and the COVID-19 pandemic impact on case volume is tough to measure, it is difficult for Treasury to predict the effect of FIRRMA changes over the next year. CFIUS management stated that it does not plan to lower the 1,000 transactions yearly estimate for now. Treasury implemented a new Case Management System (CMS) in May 2020 that allows for submission of transaction-related information through a secure online portal. Treasury had no legacy case system so staff previously managed information on SharePoint and other Microsoft applications. Management intends to add legacy information from Treasury's secure data network into the CMS but for now must rely on older methods to work with that data. While the intent of CMS is to streamline CFIUS activities, there are further developments planned for functionality and analytics. In anticipation of increased transaction reviews, the Office of Investment Security and the Office of the Assistant General Counsel for International Affairs have been aggressively hiring for approximately 35 positions. Treasury plans to decrease reliance on contractors over time as new employees are hired. While management anticipates being close to filling 81 positions (including contractors) approved for fiscal year 2020, it requested another 39 positions as part of its fiscal year 2021 budget justification. Fiscal Service's Administrative Resource Center has had trouble dealing with increasing recruitment actions and recently began to assign more support staff to help. With increased telework during the COVID-19 pandemic, CFIUS activities that involve sensitive and classified materials have been more difficult to perform. In addition, coordination with other Federal partners has been tougher as they are experiencing their own COVID-19 challenges.

Over the past several years, we reported that the recruitment of cybersecurity personnel was a government-wide challenge due to the lengthy security clearance process. 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. In its April 23, 2020 letter[21] 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. In addition, GAO reported in 2019 that Treasury likely incorrectly categorized more than a thousand positions performing IT management functions. This means that Treasury may have unreliable information about its cybersecurity workforce that it will need to identify its workforce roles of critical need.

To further complicate matters, Treasury must also operate in the repeated cycle of budget and debt ceiling stopgaps. A long-term solution has yet to be found, and the U.S. debt limit was reinstated at $22 trillion on March 2, 2019. At that time, 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

[21] GAO, *Treasury Priority Recommendations* (GAO-20-549PR; April 23, 2020).

be exhausted before September 2019. Consequently, legislation was passed to suspend the statutory debt limit through July 31, 2021.[22] 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 2020 letter to the Department, GAO raised the same concerns to Congress in its July 2015 report[23] with the approach to managing the federal debt limit and its impact on Treasury's borrowing costs and the need for alternative approaches. Fiscal Service has increased its communication with the Department, particularly the Office of Fiscal Projections (OFP). OFP provides Treasury decision-makers with information on current and predicted cash balances. As the Federal Government's financial manager, Fiscal Service plays a unique role in ensuring that OFP has current and accurate federal financial data.

The impact of this challenge and the uncertainties require the Department to continue 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 3: 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, subtle, and easier to perform they pose ongoing challenges for Treasury to fortify and safeguard its internal systems and operations along with the financial sector it oversees. While managing known risks is an ongoing challenge, Treasury must also be ready to reinforce and/or redirect cybersecurity efforts when unforeseen events occur such as the COVID-19 global pandemic. As discussed throughout this challenge, the ongoing healthcare crisis has created more opportunities for malicious actors to disrupt and exploit information systems.

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 while 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 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. In its 2019 high risk list published biennially, GAO reported the nations' cybersecurity as a government-wide issue.

[22] Public Law 116-37 (August 2, 2019).
[23] GAO, *Debt Limit: Market Response to Recent Impasses Underscores Need to Consider Alternative Approaches* (GAO-15-476; July 9, 2015).

Long-standing cyber threats pose increased risks to networks and information systems during the ongoing COVID-19 global health pandemic as more opportunities are available for bad actors to stage cyber-attacks. As the tools used to perpetrate cyber-attacks become easier to use and more widespread, less technological knowledge and fewer resources are needed to launch successful attacks of increasing sophistication. Such attacks include distributed denial of service, phishing or whaling, fraudulent wire payments, malicious spam (malspam), ransomware, and compromise of supply chains (both hardware and software). The COVID -19 pandemic has shifted the Federal workforce to a primarily telework status which has provided attackers with more possibilities to disrupt services. Increased network traffic from remote sources provides cover for attackers to blend in with the Federal workforce and launch cyber assaults. Attackers may take advantage of the increased demand for information on COVID-19 by crafting highly attractive phishing, whaling, and malspam attacks that are more likely to succeed by luring workers in with promises of information related to COVID-19. These opportunities may allow hackers to launch a denial of service attack upon a network that can prevent remote workers from performing their duties and disrupt operations. Furthermore, information systems and its users are at heightened risk of COVID-19 related exploitation such as stimulus check scams, tax-fraud schemes, and fraudulent coronavirus testing kit scams, among other things.

There is continuing concern over foreign adversaries creating and exploiting vulnerabilities in the Nation's information and communication technology and services. Executive Order 13873 was issued on May 15, 2019, to secure the supply technology and services chain by banning the import, use, or sale of technology or services designed, developed, manufactured, or supplied from persons or companies that are owned or controlled by governments defined as hostile to the United States.[24] On May 13, 2020, this Executive Order was extended for one year.[25] 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. This is especially true during this global pandemic as companies continue to temporarily close manufacturing plants due to COVID-19 outbreaks or shipping is disrupted by travel restrictions.

We continue to remind the Department that, in addition to Treasury's own networks and systems, management must be cognizant of, and mitigate, the risks posed by attacks made against other agencies and Treasury contractors and subcontractors. Increased threats and risks posed to third-parties' networks and systems due to the opportunities that the COVID-19 pandemic provides to potential attackers also poses increased risks to Treasury's networks and systems. Treasury frequently enters into interconnection agreements with other Federal, State, and local agencies, and service providers, to conduct its business. Management must exercise due care when authorizing such 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 created by the COVID-19 pandemic. Management is also challenged with ensuring that

---

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

[25] *Text of a Notice on the Continuation of the National Emergency on Securing the Information and Communications Technology and Services Supply Chain* (May 13, 2020).

critical data and information maintained by third-party cloud service providers are properly protected. There have been ongoing issues related to management of cloud systems reported in four consecutive *Federal Information Security Modernization Act of 2014* [26] audits (fiscal years 2015, 2016, 2017, and 2018) with some recommendations yet to be implemented.

Treasury is looked upon to provide effective leadership to financial institutions in particular, and the financial sector in general, to strengthen awareness and preparedness against cyber threats to the Nation's critical infrastructure. As such, effective public-private coordination is essential to the Nation's financial and national security. In this regard, The Office of 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. Given the stress that the global COVID-19 pandemic has placed on financial institutions and the financial sector, as a whole, it is important that the Department reassess cyber risks in these areas. 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.[27] In 2018, GAO had reported that the extent of adoption of the NIST framework by critical infrastructure sectors was unknown since agencies were not measuring framework implementation. With respect to Treasury, GAO had recommended that steps be taken to consult with respective sector partners to develop methods for determining the level and type of adoption by entities across the financial services sector. In its April 23, 2020 letter[28] regarding its top open recommendations, GAO noted that Treasury had established ongoing initiatives such as developing common terminology for cyber terms, but had not developed methods to determine the level and type of framework adoption; the recommendation remained open. GAO also noted in its April 23, 2020 letter that Treasury has not provided actions related to a July 2019 report[29] to Treasury to develop a cybersecurity risk management strategy that includes key elements identified in federal guidance and establish a process for conducting an organization-wide cybersecurity risk assessment.

The Department continues to report progress in its risk-based approach to cybersecurity, focusing efforts on identifying High Value Assets (HVA) [30] that would be of interest to attackers seeking maximum impact, as well as, examining the security architectures of systems and performing risk and vulnerability assessments. Fiscal Service had reported that, as a result of new assessments, it has increased the number of systems designated as HVA from six to eight. The Department acknowledged that the presence of those systems results in an inherently concentrated risk of cyber-attacks for Treasury. Additionally, a Cybersecurity Strategy Center was established in October 2019 at Fiscal Service to maintain its cybersecurity strategy, drive execution of the cybersecurity programs, facilitate risk-based decision making for cybersecurity initiatives, and to monitor progress of its cybersecurity portfolio.

---

[26] Public Law 113-283 (December 18, 2014).
[27] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0, February 12, 2014; superseded by Version 1.1; April 16, 2018).
[28] GAO, *Treasury Priority Recommendations* (GAO-20-549PR; April 23, 2020)
[29] GAO*, Cybersecurity Risk Management* (GAO-19-384 , July 25, 2019)
[30] 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.

The Department also reported that it continues to leverage the Federal government-wide Continuous Diagnostics and Mitigation program to enable automated monitoring of vulnerabilities, and is leveraging new investments to better protect Treasury data and users of Treasury's IT services. In this regard, the Department noted that it continues to implement higher security settings for websites, web services, and e-mail.

While addressing potential increases in cyber threats during the COVID-19 global pandemic, Treasury will need to continue 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 6. This will also require a cadre of skilled IT resources that has been an ongoing issue to obtain as noted in challenge 2.

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

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

TFI's authorities are key tools in implementing U.S. policy to pressure foreign countries and regimes, such as Russia and Iran, through the use of designations and economic sanctions. TFI has significantly increased sanctions against Russia and Iran related to malign and 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. Concerns over TFI's ability to meet mission critical objectives are heightened by multiple vacant key positions. These vacancies include the Undersecretary for TFI, which has been vacant since October 2019, as well as the Assistant Secretary for Terrorist Financing, who left this year. As noted in challenge 2, TFI requested approximately 50 new positions for fiscal year 2021 to address this growing demand.

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 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, 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. In addition, the COVID-19 global pandemic outbreak created additional challenges for TFI senior management. For example, many TFI employees regularly work with classified information and with international organizations involving travel. Protocols for social distancing and expanded telework are challenges for TFI to accomplish its mission.

**Challenge 5: 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 note the renewed challenges facing the Department given the need to ensure transparency to the taxpayer and other stakeholders on the use of funds distributed under economic relief packages enacted to address individuals and industry sectors impacted by the COVID-19 global pandemic. As noted in challenge 1, Treasury was tasked with responsibilities to administer over $2 trillion of emergency funding. DATA Act reporting is now seen as one of the means to ensure transparency into the use of Federal funds related to COVID-19 expenditures. In it April 2020 memorandum, *Implementation Guidance for Supplemental Funding Provided in Response to the Coronavirus Disease 2019 (COVID-19)*[31] OMB requires that agencies leverage existing financial accountability and transparency mechanisms. In part, OMB requires (1) tracking of COVID-19 expenditures with usage of a Disaster Emergency Fund Code; (2) reporting financial assistance recipient information within two weeks of issuance, with the exception of loans; and (3) reporting outlay information at the financial award transaction level. To further enhance transparency, Treasury devoted significant resources and leveraged existing financial reporting systems to promote spending transparency and use of Federal financial data in order to strengthen Government-wide decision-making. Treasury has also shifted from quarterly to monthly reporting and certification beginning with the period ending June 2020, and plans to add a program activity attribute beginning with the first quarter of fiscal year 2021. The speed in which supplemental funding was distributed created new data management needs for Treasury along with labor intensive ingestion of data associated with the application for, and issuance of, economic relief. The rapidly delivery of funds within short timeframes may create opportunities and risks for illicit activity by anyone attempting to misuse or abuse funds that were intended for COVID-19 relief. Considering the challenges and risks associated with ensuring economic relief is deployed and used for intended purposes, Treasury

[31] OMB M-20-21, *Implementation Guidance for Supplemental Funding Provided in Response to the Coronavirus Disease 2019* (April 10, 2020).

must continue to address reporting and data quality issues noted in DATA Act audits and intensify efforts to reduce improper payments.

Given the data-centric aspects of the *Foundations for Evidence-Based Policymaking Act of 2018* [32] (Evidence Act), it is critical that data is of high quality to be useful. In accordance with the Evidence Act and OMB's M-19-23,[33] the Department is implementing Government-wide reforms for making data accessible and useful for decision-making. Under Title I of the Evidence Act, also known as Federal *Evidence Building Activities*, Federal agencies, among other things, must submit annually to Congress and OMB, an evidence-building plan for identifying and addressing policy questions relevant to programs, policies, and regulations. 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[34] (www.Data.gov) developed and maintained by the General Services Administration.

Since the law was enacted, Treasury leveraged the Department-wide Strategic Objective Annual Review (SOAR) that the Office of Strategic Planning and Performance Improvement (OSPPI) leads to collaboratively identify a preliminary set of research questions as a primary means of gathering relevant policy questions for each of the Department's strategic objectives. Treasury also began working with Treasury's Federally Funded Research Development Center to identify existing research efforts that align closely with the Department's research priorities. Under Phase 1 of its implementation efforts, Treasury's Assistant Secretary for Management established an Office of the Chief Data Officer and appointed an interim Chief Data Officer and interim Deputy Chief Data Officer. The Chief Data Officer's goals are to ensure data is used as a strategic asset, increase use of data in decision-making and evidence building, and increase coordination of data collection and use. Prior to the enactment of the Evidence Act, Treasury had already started developing a data governance framework in alignment with Evidence Act Title II requirements. At that time, Treasury's Deputy Chief Financial Officer (CFO) began a Data Governance and Analytics project designed to identify a data governance structure, develop standards, and increase the department's analytic capabilities through infrastructure and visualization improvements. Since that time, the Executive Steering Committee, which includes the Deputy CFO, Chief Information Officer, and OSPPI, was expanded to include Treasury's designated Statistical Official and the Deputy Assistant Secretary for Privacy, Transparency, and Records. Currently, this group is developing recommendations for the mission and goals of the Data Governance Body, along with recommendations for initial broader membership.

[32] Public Law 115-435; (January 14, 2019).
[33] OMB M-19-23, Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance.
[34] A single public interface on-line as a point of entry for sharing data assets with the public.

Detect Improper Payments

In light of the continuing government-wide problem with improper payments (estimated at $175 billion or 4 percent of all program outlays for fiscal year 2019),[35] the Federal agencies intensified efforts to reduce improper payments in major Federal programs. The DNP Initiative and 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.[36] Since our May 2016 report, that challenge continues to exist in obtaining better death information.[37] In October 2016, GAO reported that restrictions on the center's access to SSA's full death data remained in place.[38] Since the issuance of these three reports, the DNP Center's access to SSA's full death data has not changed. In June 2020, GAO issued its initial report examining key actions the Federal Government has taken to address the COVID-19 pandemic and evolving lessons learned relevant to the nation's response to the pandemic. In its report, GAO recommended that Congress take legislative action to provide Treasury with access to the SSA's full set of death records, and require that Treasury use it, to help reduce improper payments. [39]

In response to the *Federal Improper Payments Coordination Act of 2015*,[40] 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 payments beyond what can be detected through DNP Business Center's previously existing data sources.[41] 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

---

[35] GAO, *Payment Integrity: Federal Agencies' Estimates of FY 2019 Improper Payments* (GAO-20-344; March 2, 2020), percentage based on total Government outlays of 4.4 billion (https://www.fiscal.treasury.gov/files/reports-statements/mts/mts0919.pdf).
[36] OIG, *Fiscal Service Successfully Established the Do Not Pay Business Center But Challenges Remain* (OIG-15-006; November 6, 2014).
[37] 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).
[38] 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).
[39] GAO, *COVID-19: Opportunities to Improve Federal Response and Recovery Efforts* (GAO-20-625; June 25, 2020).
[40] Public Law 114-109 (December 18, 2015).
[41] 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' Exempt Organizations Select Check, (5) the IRS' e-Postcard database, and (6) the commercial database American InfoSource (AIS) Deceased Data.

Directory of New Hires.[42] Fiscal Service included legislative proposals in its fiscal year 2021 budget justification that included, among other things, that Treasury is granted access to SSA's full Death Master File for purposes of administering the DNP Business Center and preventing, identifying, and recovering improper payments for Federal agencies and federally funded state programs.

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 assessed the services provided to agencies by the DNP Data Analytics Service and found that performance metrics developed by Fiscal Service to measure the effectiveness of the DNP Data Analytics Service need to be strengthen.[43]

Altogether, the DNP Business Center works to identify and prevent improper payments in federally funded programs by providing access to relevant data and analytic services. Fiscal Service plans to leverage the DNP Initiative to assist programs making CARES Act payments in the identification and prevention of improper payments and will continue to seek additional ways to improve improper payment prevention and detection. In this regard, the DNP Business Center has worked with Federal Communications Commission, the IRS, the Small Business Administration (SBA), and SBA's Office of Inspector General to match CARES Act payments against DNP's data sets to help prevent and identify improper payments. As of July 10, 2020, the DNP Business Center has screened over 27 million payments made under the CARES Act, identifying over $600 million in improper payments as a result. Fiscal Service also meets regularly with the PRAC, GAO, and other stakeholders to obtain feedback about COVID-19 spending data to ensure that the data is available for oversight entities.

With its potential to reduce improper payments, the DNP Business Center is a major and important undertaking by Treasury and critical to ensuring that the more than $2 trillion in COVID-19 economic support funds are properly spent. 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 6: Information Technology Acquisition and Project Management (Repeat)**

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* [44] 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,

[42] 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.
[43] OIG, *Performance Metric Policy Needed for the Fiscal Service Do Not Pay Business Center's Data Analytics Services* (OIG-20-025; January 28, 2020).
[44] Public Law 104-106 (February 10, 1996).

management, governance, and oversight functions.[45] FITARA is 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 is 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.[46] In its March 2019 high risk report, GAO acknowledged that the executive branch has undertaken numerous initiatives to better 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 CIOs' authorities, establish action plans to modernize and replace obsolete IT investment, and address weaknesses in IT Dashboard[47] reporting of IT investment risk and incremental development implementation.[48] 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 a C. Areas needing most improvement were enhanced transparency and risk management (i.e. IT investment risk), improved cybersecurity, and data center optimization. The *FITARA Enhancement Act of 2017* [49] 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 calendar year 2019, Treasury met its savings, uptime, and utilization targets, but did not achieve its other targets in the data center optimization initiative.

In fiscal year 2020, Treasury reported $2 billion in non-IRS IT investment, which is expected to increase in fiscal year 2021. Given this sizable investment, we are reporting the Department's IT acquisition and project management as an ongoing management and performance challenge

---

[45] Public Law 113-291 (December 19, 2014).
[46] GAO, *High- Risk Series*, *An Update* (GAO-15-290; February 11, 2015).
[47] 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.
[48] GAO, *High-Risk Series, Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas* (GAO-19-157SP: March 2019).
[49] Public Law 115-88 (November 21, 2017).

distinct from challenge 3 that addresses cybersecurity concerns. Treasury's non-IRS bureaus reported 21 major IT investments. Treasury's CIO assessed 18 IT investments as having moderately low or low risk to accomplishing their goals. The remaining three IT investments, which reside at Fiscal Service, were assessed as having medium risk[50] to accomplishing their goals:

- Electronic Federal Tax Payment System (EFTPS),[51]
- Post Payment Services, and
- Wholesale Securities Services (WSS).

During fiscal year 2020, some projects within EFTPS and WSS were behind schedule and over budget, while Post Payment Services had select projects that were over budget. 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, 82 percent of Treasury's total IT projects were on schedule and 57 percent were within budget. During fiscal year 2020, Treasury spent 32 percent of its total IT spending on 40 major investments. A major WSS investment includes the Treasury Automated Auction Processing System (TAAPS), used by Fiscal Service for the announcement, auction, and issuance of marketable Treasury bills, notes, bonds, Treasury inflation-protected securities, and floating rate notes. In fiscal year 2017, Fiscal Service started a multi-year project to modernize the TAAPS application software and associated technology components to ensure that critical auction processes continue to work flawlessly, remain secure, and operate without service disruptions. However, in January 2020, Fiscal Service terminated its TAAPS application software project due to contractor delays and problems involving (1) the application code quality issues; (2) project leadership that did not include sufficient IT support; and (3) governance bodies relying on representations that the project was succeeding, despite some warning signs. It was not until third party reviews were conducted that the full extent of the project's challenges became clear.

An ongoing 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. The TBM framework consists of layers that represent different views into IT costs and performance, enabling greater transparency into the true cost of IT and its value to the business. Fiscal Service's financial community was trained on TBM and has reduced uncategorized IT spending by 60 percent. In early fiscal year 2021, Fiscal Service expects to see further reductions in IT portfolio spending.

---

[50] 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.

[51] Renamed Tax Collections Services in fiscal year 2021.

## Other Matters of Concern

Although we are not reporting these as management and performance challenges, we are highlighting three areas of concern: (1) coin redemption and (2) managerial cost accounting, and (3) internal control at BEP.

Coin Redemption

The Mint continues to address internal control issues to ensure the integrity of U.S. coinage in its coin redemption program. Over the past several years, it has suspended and recommenced the program in an effort to address weaknesses in its program. Since our audit in 2018, the Mint updated its standard operating procedures for the coin redemption program and in May 2020 has drafted a Notice of Proposed Rule Making in an effort to implement adequate internal controls over its program. Considering of the history of this program, we will monitor the implementation of these controls to ensure they are sufficient to properly safeguard U.S. coinage.

Managerial Cost Accounting

Managerial cost accounting continues to be 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. We have reported concerns that were identified in our audit of the Departmental Offices' OBT controls over its overhead[52] process and compliance with the *Economy Act.*[53] Specifically, we identified internal control weaknesses within OBT's overhead process and composite methodology used during fiscal years 2015 through 2018 to charge reimbursable customers. That is, OBT's methodology to accumulate, allocate, and charge overhead costs to reimbursable customers was not appropriate and consistently followed and the salaries and expenses directly charged to reimbursable customers through the composite methodology lacked adequate support. Therefore, we also concluded that OBT violated the Economy Act and potentially augmented its fiscal year 2015 appropriation by recovering indirect costs in excess of actual costs from reimbursable customers. These concerns, in turn, could also potentially be violations of the Anti-deficiency Act.

In response to our concerns, OBT management has implemented a new overhead process for fiscal years 2019 and 2020, and subsequently hired a consultant to review and improve the process. Based on the consultant's recent report, OBT management implemented a number of the consultant's recommendations to improve the process going forward, which we plan to review during our ongoing audit.

[52] Overhead, also known as indirect costs, include items that 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.
[53] Public Law 73-2 (March 20, 1933).

Internal Control Issues at BEP

Internal control is a process put in place by management to safeguard assets, promote accountability, and increase efficiency and effectiveness of operations. It helps an entity report reliable information about its operations and comply with applicable laws and regulations. The fiscal year 2019 BEP financial statement audit[54] identified 22 deficiencies in internal control with nine of them collectively reported as two significant deficiencies related to financial reporting and information technology controls. The remaining 13 deficiencies related to entity level controls; property, plant, and equipment; inventory; human resources; journal entries; financial reporting; and expenditures and were reported in a management letter.[55] BEP management noted that control issues were largely due to resource constraints caused by turnover in the workforce and increased workloads for key accounting personnel. BEP management has begun addressing concerns by hiring additional personnel and identifying parties responsible for the issues noted. A reliable system of internal control over financial reporting is vital for BEP's management to accurately and reliably report on its financial transactions and positions. Our office will continue to monitor BEP's progress in strengthening its financial management and reporting processes. As another matter, our office has an ongoing corrective action verification of recommendations related to a 2013 audit report that identified numerous deficiencies in BEP's contracting practices.[56] While this verification is nearing completion, we noted that contract file management continues to be a systemic issue at BEP. We expect to issue our verification audit in early fiscal year 2021. Given our concerns, we also plan to initiate an audit of BEP's transition from hard copy contract files to an electronic filing system beginning in fiscal year 2017.

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

[54] OIG, *Audit of the Bureau of Engraving and Printing's Financial Statements for Fiscal Years 2019 and 2018* (OIG-20-031; April 20, 2020).
[55] OIG, *Management Letter for the Audit of the Bureau of Engraving and Printing's Financial Statements for Fiscal Years 2019 and 2018* (OIG-20-032; April 20, 2020).
[56] OIG, *BEP's Administration of the Burson-Marsteller Public Education Awareness Contract Was Deficient* (OIG-13-046; August 13, 2013).