OFFICE OF
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

October 14, 2022

INFORMATION MEMORANDUM FOR SECRETARY YELLEN

FROM: Richard K. Delmar
Deputy Inspector General

SUBJECT: Management and Performance Challenges Facing the Department of the Treasury (OIG-CA-23-002)

In accordance with the Reports Consolidation Act of 2000, we are providing you with our perspective on the most serious management and performance challenges facing the Department of the Treasury (herein "Treasury" or "the Department"). In this year's memorandum, my office is reporting five challenges, one of which is new and reports on the challenges faced with implementing climate initiatives. As shown below, four challenges are repeated and updated from last year to include Treasury's continued role in combatting the economic fallout of the Coronavirus Disease 2019 (COVID-19) global pandemic, as well as its impacts on related workforce and workstreams.

- COVID-19 Pandemic Relief (Repeat)
- Cyber Threats (Repeat)
- Anti-Money Laundering/ Terrorist Financing and Bank Secrecy Act Enforcement (Repeat)
- Information Technology Acquisition and Project Management (Repeat)
- Climate Initiatives Risk (New)

In addition to the above challenges, we are reporting a concern about regulating digital assets.

We identified challenges and a concern 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 caused a global health emergency and economic crisis that Treasury continues to tackle. Furthermore, Treasury will continue to provide financial assistance to the transportation industry and to all 50 states, units of local government, U.S. territories, and tribal governments for the foreseeable future. As noted throughout this memorandum, Treasury will need to continue to act swiftly and draw on its existing resources to meet economic needs.

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: Anna Canfield Roth
Acting Assistant Secretary for Management

Contents

Challenge 1: COVID-19 Pandemic Relief (Repeat)

The Coronavirus Disease 2019 (COVID-19) pandemic continues to affect the health and economic stability of communities worldwide. In the early stages of the COVID-19 outbreak, Congress passed legislation in succession to address the public health crisis and the economic fallout affecting individuals, businesses, and many industry sectors. The *Coronavirus Preparedness and Response Supplemental Appropriation Act of 2020*, signed into law on March 6, 2020, authorized $8.3 billion in emergency funding to address health and medical care. [1] Shortly thereafter, the *Families First Coronavirus Response Act* was enacted on March 18, 2020, which provided approximately $104 billion to address the financial stress of individuals and households.[2] The *Coronavirus Aid, Relief, and Economic Security Act* (CARES Act)[3] passed on March 27, 2020 and 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 others. As the public health crisis continued into late 2020 and 2021, Congress legislated additional relief in passing the *Consolidated Appropriations Act, 2021*[4] (CAA, 2021) on December 27, 2020, and the *American Rescue Plan Act of 2021*[5] (ARP) on March 11, 2021. These laws provided another $900 billion and $1.9 trillion of economic stimulus, respectively.

The Department of the Treasury (hereinafter Treasury or the Department) has been instrumental to the implementation of economic relief provisions of the CARES Act, CAA, 2021, and ARP. As a result, Treasury's responsibilities and workloads expanded enormously. Treasury is tasked with disbursing over $655 billion[6] in aid to more than 35,000 recipients, including state, local, territorial, and tribal government entities, in a relatively short period of time and with limited staffing. The Department is challenged with (1) filling and transitioning key leadership positions for pandemic programs not fully established, (2) quickly establishing internal controls, guidance, and methodologies for monitoring, reporting, and oversight of funds disbursed, (3) data collection, quality, and reliability, and (4) lack of funding to sustain operations. In addition, Treasury must carry the administrative and monitoring responsibilities in its new role resolving Single Audit findings and potentially serving as cognizant agency for a significant number of entities [7] under the Office of Management and Budget's (OMB) *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*. [8]

Because of Treasury's expanded responsibilities and workloads, pandemic recovery programs and provisions of the CARES Act, CAA, 2021, and ARP within the oversight purview of my office, are extensive and include programs that support transportation industry workers; renters and homeowners; and state, local, territorial, and tribal government entities through direct financial

[1] Public Law 116-123 (March 6, 2020).
[2] Public Law 116-127 (March 18, 2020).
[3] Public Law 116-136 (March 27, 2020).
[4] Public Law 116-260 (December 27, 2020).
[5] Public Law 117-2 (March 11, 2021).
[6] Amount excludes Economic Impact Payments distributed by the Internal Revenue Service and support to small businesses under the Paycheck Protection Program administered by the Small Business Administration.
[7] Single Audit Act of 1984 (P.L 98-502; October 19, 1984), as amended by the Single Audit Act Amendments of 1996 (P.L 104-156; July 5, 1996).
[8] https://www.ecfr.gov/current/title-2/part-200

assistance. The pandemic programs Treasury is responsible for and their challenges are discussed below.

Financial Assistance Programs - Air Carrier Worker Support and Other Transportation Services

Payroll Support Programs

To maintain pay and benefits of airline industry workers, Treasury implemented the Air Carrier Worker Support Program provisions of the CARES Act that authorized up to $63 billion of direct financial assistance for passenger air carriers, cargo air carriers, and contractors. Using existing resources and contractor support, Treasury quickly stood up the Payroll Support Program (PSP1) and made direct payments of approximately $28.6 billion to 611 applicants as of April 7, 2022. Financial support for air carrier workers was extended twice by CAA, 2021 and ARP which provided additional assistance to passenger air carriers and contractors up to $16 billion and $15 billion, respectively. Using the mechanisms that established PSP1, Treasury implemented the Payroll Support Program Extension (PSP2) and the Payroll Support Program 3 (PSP3) to make corresponding payments. As of July 27, 2022, Treasury disbursed approximately $15.6 billion to 489 applicants under PSP2 and $14.6 billion to 484 applicants under PSP3.

My office will continue audits of PSP1 recipients' certifications and initiate audits of certifications submitted by PSP2 recipients in fiscal year 2023. My office is not mandated to audit the applicants' certifications to receive PSP3 payments authorized under ARP. However, Treasury disbursed financial assistance to passenger air carriers and contractors based on information submitted by recipients on their PSP2 certifications, which we will audit. That said, my office plans to assess Treasury's calculation of award amounts under PSP3 and Treasury's post-award monitoring of recipients under PSP1, PSP2, and PSP3. It is incumbent upon the Department to implement and maintain strong internal controls 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.

Coronavirus Economic Relief for Transportation Services

Congress expanded financial support to non-air carrier transportation service providers under the Coronavirus Economic Relief for Transportation Services (CERTS) provisions of CAA, 2021. Treasury established the CERTS Program that provides $2 billion in non-competitive grants to eligible companies that certify revenue loss of 25 percent or more due to the COVID-19 pandemic. In consultation with the Department of Transportation, Treasury provided initial guidelines on May 6, 2021, that included among other things, the priority use of funds must be for payroll, although operating expenses and debt accrued to maintain payroll are eligible uses. Treasury disbursed approximately $1.97 billion to 1,464 recipients as of May 20, 2022. It is incumbent upon the Department to establish and maintain strong internal controls over recipients' compliance with grant agreements. Although there is no mandate directing my office to audit CERT recipients, we plan to monitor and audit Treasury's administration of the program.

Financial Assistance Programs - State, Local, U.S. Territorial, and Tribal Governments

Coronavirus Relief Fund

The $150 billion Coronavirus Relief Fund (CRF), established under Title VI of the *Social Security Act*, as amended by Title V of the CARES Act, continues to be a large endeavor for both the Department and my office. The Department disbursed the entire $150 billion in 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. As you are aware, the CARES Act created a unique challenge in distinguishing between the programmatic administrative responsibility for payments made from the CRF and the Treasury Office of Inspector General's (OIG) independent oversight. Although Treasury is 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 has authority to recoup funds if it is determined that recipients fail to comply with uses of funds for COVID-19 related costs under Section 601 (d), "Uses of Funds," of the *Social Security Act*, as amended.[9]

The Department also has a fundamental role to clarify its policy[10] over the uses of funds when interpretation matters arise. As recipients are still in the process of reporting on and closing out their awards, we anticipate that questions will continue to arise that will require interpretation. Providing as much clarity as possible is essential for ensuring recipients understand the compliance requirements and are accountable and transparent in how they report uses of funds. My office has received over 300 complaints regarding recipient, and in some instances sub-recipient, uses of CRF proceeds that require continued collaboration between the Department and my office.

Coronavirus State and Local Fiscal Recovery Funds

The *Coronavirus State and Local Fiscal Recovery Funds* provisions of ARP provide state, local, U.S. territorial, and tribal governments another $350 billion under the Coronavirus State Fiscal Recovery Fund and the Coronavirus Local Fiscal Recovery Fund (together referred to as SLFRF); $10 billion under the Coronavirus Capital Projects Fund (CPF); and $2 billion under the Local Assistance and Tribal Consistency Fund (LATCF).

SLFRF

As of August 2022, Treasury has disbursed approximately $349.9 billion of the $350 billion SLFRF through non-competitive direct assistance to over 35,000 direct recipients, including approximately 26,000 Non-Entitlement Units (NEU) of Local Governments that received funding through a state or U.S. territory. Administering SLFRF poses challenges given the volume of recipients that Treasury must oversee that include all 50 states, U.S. territories, tribal governments, local government recipients with population sizes of 250,000 or more, and

[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 31, 2021, as extended by the CAA, 2021.

[10] *Coronavirus Relief Fund Guidance for State, Territorial, Local, and Tribal Governments* Federal Register, Vol. 86, No. 10; January 15, 2021.

approximately 26,000 NEUs. States and U.S. territories were required to establish a process for NEUs to provide pre-pandemic budget and other critical information and documentation before distributing funds. In addition to the volume of NEUs for Treasury to oversee, reconciliation between states' and U.S. territories' disbursements to NEUs and recipient performance reporting may be challenging. That is, performance reporting for NEU funding is the responsibility of the NEUs and not the states and U.S. territories where accountability for the disbursement of funds resides. Furthermore, due to increased pandemic funding many NEUs are now required to have a Single Audit or alternate compliance examination engagement over which Treasury may have agency cognizance as detailed below related to challenges with Treasury's ongoing compliance monitoring of SLFRF recipients and related administrative issues.

While Treasury has built a portal within Salesforce[11] for recipient communication and reporting, there are still challenges obtaining sufficient quality data from SLFRF recipients. Treasury allows for lengthy narrative responses as part of the data collection that may be more cumbersome to review and lack critical data details. Confirming data quality and timely providing data to the public and oversight community has been challenging for Treasury. To effectively administer and monitor SLFRF recipients' compliance, Treasury must have access to sufficient data that accurately reflects how recipients have expended SLFRF awards. As Treasury continues to receive quarterly and annual reports on SLFRF recipients' uses of funds, it is critical that Treasury continues to refine mechanisms to ensure the data is complete, accurate, reliable, and transparent in reflecting how recipients have expended SLFRF awards.

Treasury management has expressed difficulty finding the staff needed to administer and monitor the SLFRF program. The Office of Recovery Programs had a number of key leadership positions that were either vacant or temporarily staffed throughout fiscal year 2022. As discussed in more detail under the accountability and transparency section below, Treasury faces future funding challenges to support the Office of Recovery operations, to include ongoing administration of the SLFRF program and recipient monitoring.

CPF

As of September 2022, Treasury awarded $1.4 billion to 13 states[12] from the $10 billion of CPF available to address infrastructure challenges, such as reliable internet, that low to moderate income and rural communities have experienced during the COVID-19 pandemic. Although Treasury issued recipient reporting guidance for states, U.S. territories, and Freely Associated States in August 2022, Treasury still needs to inform eligible tribal government recipients of their reporting obligations to provide full accountability and transparency as to how CPF awards are used. To do this, Treasury needs to begin collecting sufficient and accurate CPF data.

[11] Salesforce is a cloud-based customer- relationship management software platform.

[12] Treasury announced awards for Louisiana, New Hampshire, Virginia, West Virginia, Kansas, Maine, Maryland, Minnesota, Arkansas, Connecticut, Indiana, Nebraska, and North Dakota.

LATCF

Treasury has been delayed in standing up the LATCF program, which was appropriated $2 billion for fiscal years 2022 and 2023 to make COVID-19 assistance payments to eligible revenue sharing counties and Tribes. Treasury issued LATCF guidance, including general reporting requirements to eligible recipients, and as of September 30, 2022, both tribal governments and revenue counties are able to apply for funds. Now, Treasury will need to prepare for the collection of sufficient and accurate LATCF data for monitoring recipients' compliance with the program.

With the overlap of recipients of CRF, SLFRF, CPF, and LATCF, we expect that there will be confusion between the uses of funds requirements, and reporting mechanisms that may be a challenge for recipients going forward. Given the volume of recipients and varying requirements under these programs, Treasury will need to ensure that there are sufficient resources for the remaining distribution of funds and ongoing monitoring of recipient reporting and compliance with terms and conditions for funds received. Furthermore, with the level of funding under both CRF and SLFRF, Treasury may have agency cognizance over many smaller local governments (particularly NEUs) and tribal governments now required to have a Single Audit for the first time. To minimize recipient burden, Treasury developed alternate reporting requirements for smaller SLFRF recipients, which would otherwise be subject to Single Audit. In the Compliance Supplement for 2022, Treasury provides the option of an alternate compliance examination engagement for SLFRF recipients meeting certain eligibility requirements. Treasury has been working with OMB and the audit community to find a solution for receiving these reports as the Federal Audit Clearinghouse (FAC) was not designed to collect non-audit products. Treasury plans to collect these reports directly for fiscal year 2021 compliance examinations, and is continuing to work with the FAC to receive these reports for fiscal year 2022, which is expected to begin as soon as October 2022. While the alternative compliance examination engagement addresses the burden to these smaller government entities and auditors, Single Audit and alternative compliance examination procedures may be new to thousands of SLFRF recipients, so there will be much more guidance and oversight required of Treasury in its cognizance role and related to the Compliance Supplement. Treasury must be prepared to use results of Single Audits and alternate compliance examinations as part of its compliance monitoring of recipients and will need the appropriate level of staffing to address these issues on such a large scale. As discussed in more detail under the accountability and transparency section below, Treasury is evaluating whether it will have cognizance over thousands of non-federal recipients of SLFRF and its impact as it faces budget shortfalls in fiscal year 2023 to carry out its ongoing administration and monitoring of SLFRF recipients.

Emergency Rental Assistance and Homeowner Assistance Programs

To provide assistance to vulnerable households at risk of housing instability, Congress established two Emergency Rental Assistance (ERA) Programs and a Homeowner's Assistance Fund (HAF) availing over $56 billion to households in need. Division N, Title V, Subtitle A, of CAA, 2021, created the initial ERA Program (ERA1) and ARP created a supplemental ERA Program (ERA2) and HAF.

ERA1
Treasury established ERA1 and as of September 30, 2022, disbursed $24.93 billion of the $25 billion appropriated by CAA, 2021. The $24.93 billion was disbursed to states (including Washington, DC), U.S. territories, tribal governments (with a provision for the Department of Hawaiian Home Lands), and units of local government with populations of 200,000 or greater to pay for rent, utilities, and other housing-related expenses and arrears through September 30, 2022. In addition to disbursing the funds, Treasury provided guidance on ERA1 fund usage and set up a Portal where government recipients are to report on their spending.

CAA, 2021 requires that my office conduct monitoring and oversight of the receipt, disbursement, and use of ERA1 funds. We will conduct our oversight with audits of Treasury's (1) establishment and implementation of the program, (2) payments of funds, and (3) guidance and management over the program. We will use the data reported in Treasury's ERA Portal to inform our monitoring function; thus, it is imperative that Treasury ensures recipients' compliance to Treasury ERA guidance when reporting to Treasury's ERA Portal. My office is also authorized to require repayment of funds to Treasury when we determine a recipient failed to comply with ERA1 requirements.

ERA2
For ERA2, as of June 30, 2022, Treasury disbursed $21.51 billion of the $21.55 billion appropriated in ARP. Similar to ERA1, ERA2 provides funding for eligible renter households' rent, utilities, and other housing-related expenses and arrears, but does not include tribal governments as eligible grantees. ERA2 funds are to remain available until September 30, 2027. Treasury has also provided ERA2 guidance for the state, territory, and local, government recipients. My office is tasked with oversight of the program and will conduct our ERA2 oversight with a similar methodology to our ERA1 oversight.

HAF
ARP also created HAF to prevent mortgage delinquencies, defaults, foreclosures, loss of utility services, and displacement by covering mortgage-related expenses, utility expenses, and arrears for homeowners experiencing financial hardship after January 21, 2020. As of August 2022, Treasury has disbursed more than $9.5 billion of the $9.9 billion authorized to states (including the District of Columbia and Puerto Rico), tribal governments (including the Department of Hawaiian Home Lands), Guam, American Samoa, the U.S. Virgin Islands, and the Commonwealth of the Northern Mariana Islands. The funds are available until September 30, 2025 and Treasury provided guidance on HAF. ARP mandates that my office provide oversight of the funds, which will include audits of Treasury's (1) establishment and implementation of the fund, (2) payments of funds, and (3) guidance and management over the program.

While Treasury has issued relevant guidance for each of the programs, it is essential its program offices continue to be responsive to recipients to clarify guidance and to provide insight into the eligible uses of the funds Treasury distributed. Clear and timely guidance and responsiveness to recipient questions are also critical in enabling program recipients to administer their programs and disburse funds to households in need without delay.

State Small Business Credit Initiative

The State Small Business Credit Initiative (SSBCI), which was originally created in the *Small Business Jobs Act of 2010* to increase availability of credit for small businesses, ended in 2017. However, Section 3301 of ARP reauthorized SSBCI and provided $10 billion in funding for the program. Under SSBCI, participating states, U.S. territories, and tribal governments may obtain funding for programs that partner with private lenders to extend credit to small businesses. Additionally, ARP modified SSBCI in a number of ways including the following set-asides: (1) $500 million in allocations to tribal governments in proportions determined appropriate by the Secretary of the Treasury; (2) $1.5 billion in allocation to states, U.S. territories, and tribal governments for business enterprises owned and controlled by socially and economically-disadvantaged individuals (SEDI); (3) $1 billion to be allocated as an incentive for states, U.S. territories, and tribal governments that demonstrate robust support for SEDI businesses; (4) $500 million to be allocated to very small businesses with fewer than 10 employees; and (5) $500 million to provide technical assistance to certain businesses applying for SSBCI or other state or federal programs that support small businesses.

Primary oversight of the use of SSBCI funds is the responsibility of the participating state, U.S. territory or tribal government. The participants are responsible for providing Treasury with quarterly assurances that their programs approved for SSBCI funding comply with program requirements. However, Treasury will face challenges in holding participants accountable for the proper use of funds, as it has not clearly defined the oversight obligations of the states, U.S. territories, and tribal governments or specified minimum standards for determining whether participants have fulfilled their oversight responsibilities. In the past, Treasury has also not required participating states to collect and review compliance assurances made by lenders and borrowers or defined what constitutes a material adverse change in a state's financial or operational condition that must be reported to Treasury. As a result, Treasury may have difficulty finding recipients to be in default of program requirements and holding recipients accountable.

Community Development Investment Programs[13]

Emergency Capital Investment Program

As authorized under CAA, 2021, Treasury has invested $8.26 billion in 161 Community Development Financial Institutions (CDFI) and Minority Deposit Institutions of the $9 million available under the Emergency Capital Investment Program (ECIP), providing capital to low-to-moderate income community financial institutions that support small businesses and consumers. Treasury has experienced challenges in fully implementing ECIP. As reported in our audit of ECIP's implementation, Treasury had not completed key documentation, such as policies and procedures to include a post-investment compliance and monitoring plan to fully implement and administer investments. [14] With investments now underway, it is more imperative that Treasury develop and implement policies and procedures to govern its post–investment activities. Because

[13] Treasury OIG is required to submit to the Committee on Financial Services of the House of Representatives and the Committee on Banking, Housing, and Urban Affairs of the Senate, and the Secretary of the Treasury, not less frequently than 2 times per year, a report relating to the oversight provided including any recommendations for improvements to the Community Development Investment programs.
[14] OIG, *Audit of Treasury's Implementation of the Emergency Capital Investment Program* (OIG-22-028; March 8, 2022)

of the demands for resources within the Office of Recovery Programs, Treasury may continue to experience further delays and challenges administering the ECIP.

CDFI Rapid Response Program

Treasury has disbursed $1.19 billion of the $3 billion, authorized under the CAA, 2021, under the CDFI Fund Rapid Response Program (CDFI RRP), to deliver immediate assistance to low-income communities through competitive grants to CDFIs. However, as we reported in our audit of the CDFI RRP implementation,[15] the CDFI Fund did not include the award term and condition for integrity and performance matters in its assistance agreement template. CDFI Fund stated this was rectified before the agreements were signed. We will confirm that CDFI Fund included the required language in the executed assistance agreements with CDFI RRP grant recipients as part of our ongoing mandated audits of the CDFI RRP.

CDFI Equitable Recovery Program

The CDFI Fund is delayed in awarding the remaining $1.75 billion of the $3 billion authorized under CAA, 2021 for the CDFI Fund Equitable Recovery Program (CDFI ERP). Awards granted under ERP are intended for low- or moderate-income minority communities that have significant unmet capital or financial services needs, and were disproportionately impacted by the COVID-19 pandemic. This program will be more challenging for the CDFI Fund to administer in fiscal year 2023 because of unique and complex program materials for the application process and award administration needed to address program policy priorities in order to meet the statutory intent. In addition, CDFI Fund plans to implement designation of minority lending institutions as defined under the CAA, 2021 separately from the award of ERP funds and will begin in fiscal year 2023.

Accountability and Transparency

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. Along with administering and delivering economic relief, Treasury must manage the unprecedented oversight that pandemic relief funding is subject to. As noted above, Treasury is evaluating whether it will have cognizance over thousands of non-federal recipients of SLFRF and be required to carry out a larger administrative and monitoring role to ensure compliance under OMB's *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*. Among its responsibilities as a Federal awarding agency, Treasury must follow-up on audit findings to ensure that recipients take appropriate and timely corrective action and issue management decision letters.[16] Many recipients are smaller governments, which for the first time are subject to Single Audit or the alternative compliance examination available to eligible recipients meeting eligibility requirements. Regardless of cognizance, Treasury will have to work with recipients to resolve Single Audit and alternative

[15] OIG, *Audit of the Community Development Financial Institutions Fund's Implementation of the CDFI Rapid Response Program* (OIG-22-023; December 21, 2021).
[16] 2 CFR § 200.521, "The management decision must clearly state whether or not the audit finding is sustained, the reasons for the decision, and the expected auditee action to repay disallowed costs, make financial adjustments, or take other action. If the auditee has not completed corrective action, a timetable for follow-up should be given..." (https://www.ecfr.gov/current/title-2/subtitle-A/chapter-II/part-200/subpart-F/subject-group-ECFR4424206eaecf751/section-200.521)

compliance examination findings specific to each of its pandemic relief programs. Given the anticipated budget short-falls as noted below, carrying out this level of oversight of thousands of recipients will be very challenging for Treasury.

In addition to my office's ongoing work on pandemic programs, Treasury is subject to additional Congressional oversight bodies, the Special Inspector General for Pandemic Recovery[17] (SIGPR), the Government Accountability Office (GAO), and the Pandemic Response Accountability Committee (PRAC). Treasury is also accountable for providing transparency over the expenditure of pandemic relief funds. Many reporting requirements of sections 15010 and 15011 of the CARES Act were extended under the CAA, 2021, PRAC amendments. Most notably, Treasury is responsible for reporting obligations and expenditures of large covered funds (over $150,000) to the PRAC. While my office continues to collect and report CRF data to the PRAC under an agreement with the Department as noted above, Treasury is responsible for reporting expenditures of its other pandemic relief programs. As noted above, data collection and quality are still challenges for Treasury under the various pandemic programs. The Department must balance its ongoing response to the financial impacts of the public health emergency with its responsibility to stakeholders for reporting and transparency.

While the economic fallout of COVID-19 pandemic continues, Treasury must persevere in navigating this challenging time. While Treasury has leveraged its existing workforce, hired contractors, and obtained detailees from other Federal agencies to address the demands of the pandemic programs, it faces future funding challenges to carry out its expansive administrative and compliance monitoring role. Treasury projected an administrative funding shortfall of $35 million to continue compliance activities over SLFRF and ERA recipients in its *Congressional Budget Justification and Annual Performance Plan and Report for FY 2023*.[18] Treasury requested "Administrative Funding Transfer Authority" to move appropriated administrative funding amounts from one pandemic program to another to cover the anticipated shortfall. Without this flexibility, Treasury estimated that funds to administer the SLFRF program will run out by mid-fiscal year 2023 and early fiscal 2024 for ERA, causing further shortages in resources. Treasury is pro-actively working to reduce spending across the board on SLFRF and other impacted programs, as well as in central service areas to extend essential operations, but this may not be enough to carry out the large-scale compliance monitoring responsibilities in the event Congress does not approve the "Administrative Funding Transfer Authority" timely. On September 23, 2022 Treasury notified recipients of funding constraints impacting Treasury's ability to provide ongoing administrative support and monitoring of funds distributed under SLFRF, CPF, ERA, HAF, and LATCF. Treasury advised that a number of functions will be halted or reduced, such as recipient monitoring and reporting, if its request for administrative funding flexibility is not provided. Given the adverse impacts of Treasury's planned measures, my office expressed concerns to Congress, most notably to the reduction of recipient monitoring and reporting, in a letter dated October 3, 2022. We stressed that Treasury's funding constraints jeopardize accountability and transparency of more than $400 billion distributed to thousands of recipients of SLFRF, CPF, ERA, HAF, and LATCF. In addition, we highlighted the cascading effect of Treasury's reduced recipient monitoring and reporting on oversight functions performed

[17] SIGPR was authorized under the CARES Act to oversee loans, loan guarantees, and other investments provided by Treasury and must report to congress quarterly on the SIGPR's activities and Treasury's loan programs. SIGPR terminates five years after enactment of the CARES Act (March 27, 2025).
[18] https://home.treasury.gov/system/files/266/07A.-COVID-FY-2023-CJ.pdf

by my office and the PRAC as we depend on Treasury obtaining quality data from recipients on uses of pandemic funds.

Going forward, Treasury may experience difficulties in balancing its ongoing pandemic oversight responsibilities and workloads while managing several ongoing challenges as described throughout this memorandum. While I am hopeful that fiscal year 2023 will see an end to the horrific fallout that the COVID-19 pandemic has had on our nation, I am also mindful that both short-term and long-term challenges lay ahead for both Treasury and my office.

Challenge 2: Cyber Threats (Repeat)

Cybersecurity remains a long-standing and serious challenge facing the Nation as reported by GAO as a government-wide issue in its 2021 high- risk list published biennially.[19] A reliable critical infrastructure, including information systems and networks, is vital to our national security and economic stability. Cyber threats remain a persistent concern as Treasury's information systems are critical to the core functions of government and the Nation's financial infrastructure, along with the financial sector it oversees. As cyber threats continue to evolve and become more sophisticated, subtle, and easier to perform, Treasury must fortify and safeguard its internal systems and operations while modernizing and maintaining them. Although managing known risks is an ongoing challenge, Treasury must also be ready to reinforce and/or redirect cybersecurity efforts when unforeseen events occur, such as the COVID-19 pandemic, the recent conflict in the Ukraine, [20] the 2020 SolarWinds attack,[21] or when serious flaws are discovered in software or systems, such as Log4J[22] and VMWare,[23] that allow for remote administrative-level access.[24]

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

The tools used to perpetrate cyber-attacks continue to become easier to use and more widespread, lowering the technological knowledge and resources needed to launch successful attacks of

[19] GAO, *High-Risk Series, Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas* (GAO-21-119SP: March 2021).
[20] A joint Cybersecurity Advisory was issued by the Cybersecurity and Infrastructure Security Agency to "warn organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. This activity may occur as a response to the unprecedented economic costs imposed on Russia as well as materiel support provided by the United States and U.S. allies and partners." (*Alert (AA22-110A) Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*; April 20, 2022)
[21] The SolarWinds attack, reported in December 2020, was a supply chain attack that used the update mechanism for legitimate software to distribute malicious software.
[22] Log4j is software used by other software to enable logging of selected events upon a system.
[23] VMWare, Inc. provides a variety of software tools to manage virtual or cloud environments.
[24] Cybersecurity and Infrastructure Security Agency, *Emergency Directive 22-02 Mitigate Apache Log4J Vulnerability* (April 8, 2022), *Emergency Directive 22-03 Mitigate VMWare Vulnerabilities* (May 18, 2022).

increasing sophistication. Such attacks include distributed denial of service, phishing, fraudulent wire payments, business email compromise, malicious spam (malspam), ransomware, and compromise of supply chains (both hardware and software). While the federal workforce shifts from a primarily telework status to a hybrid work environment, Treasury must remain cognizant of the increased risk profile a remote workforce, which provides threat actors with a broader attack surface. Increased network traffic from remote sources provides cover for attackers to blend in with the federal workforce and launch cyber assaults. These opportunities may allow threat actors to launch a denial of service attack upon a network that can prevent remote workers from performing their duties and disrupt operations.

There is continuing concern over foreign adversaries creating and exploiting vulnerabilities in the Nation's supply chain for information and communication technology and services as evidenced by the 2020 SolarWinds attack that affected many federal agencies and private sector companies. Executive Order (EO) 13873, *Securing the Information and Communications Technology and Services Supply Chain*, was issued on May 15, 2019, to secure the supply technology and services chain by banning the import, use, or sale of technology or services designed, developed, manufactured, or supplied from persons or companies that are owned or controlled by governments defined as hostile to the United States.[25] On May 12, 2022, this EO was extended again for 1 year.[26] There are risks that Treasury's systems and resources already in use, including critical infrastructure, contain components from sources that have yet to be designated as threats. Once a source is designated as such, repairs and/or upgrades of key system components may no longer be available. Therefore, there is risk of disruption of critical operations. The Department will need to continue to monitor developments in this area closely and plan for the possibility that its current supply chain may no longer be available.

Furthermore, EO 14028, *Improving the Nation's Cybersecurity*, issued on May 12, 2021, calls for federal agencies to update existing plans to prioritize resources for adoption and use of cloud technology and to adopt a zero-trust architecture,[27] among other things. To achieve the goals outlined in EO 14028, OMB issued M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*[28] to provide the strategy for achieving a zero-trust architecture, and requires agencies to meet specific cybersecurity standards and objectives by the end of fiscal year 2024. OMB also issued M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*[29] to use only software that complies with secure software development standards. As mentioned above, Treasury management must be mindful that the efforts to secure Treasury's supply chain may hamper cloud adoption and the implementation of zero-trust architecture. In response to our prior year memorandum, Treasury reported the Enterprise Cyber Risk Management program enhanced the risk assessment process to identify

[25] EO 13873, *Securing the Information and Communications Technology and Services Supply Chain* (May 15, 2019).
[26] *Notice on the Continuation of the National Emergency with Respect to Securing the Information and Communications Technology and Services Supply Chain* (May 12, 2022).
[27] Zero-trust architecture is a method of designing a system in which all actions are presumed dangerous until reasonably proven otherwise, thereby reducing the chance of a successful attack causing further damage.
[28] OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (January 26, 2022), (https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf).
[29] OMB M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (September 14, 2022), (https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf).

compliance items separately from cybersecurity risk reporting, and continued to grow the Supply Chain Risk Management program.

We continue to remind the Department that, in addition to Treasury's own networks and systems, management must be cognizant of, and mitigate, the risks posed by attacks made against other federal and non-federal agencies and Treasury contractors and subcontractors. Increased threats and risks posed to third parties' networks and systems due to the opportunities that extended telework 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. 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 were reported in four consecutive *Federal Information Security Modernization Act of 2014* [30] audits (fiscal years 2015, 2016, 2017, and 2018), with one repeat recommendation, related to third-party cloud service providers demonstrating FISMA compliance, remaining unimplemented as of fiscal year 2022.

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 and the conflict in Ukraine place on financial institutions and the financial sector, it is important that the Department monitors 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.[31] 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.[32] 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 May 10, 2022 letter[33] regarding its top open recommendations, GAO acknowledged that Treasury had developed a cybersecurity profile for the sector that maps the NIST Cybersecurity Framework's (CSF) five core functions[34] to existing regulations and guidance for financial services entities, but had not developed methods to determine the level and type of framework adoption; the recommendation remained open.

[30] Public Law 113-283 (December 18, 2014).
[31] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0, February 12, 2014; superseded by Version 1.1; April 16, 2018).
[32] GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption* (GAO-18-211; February 18, 2018)
[33] GAO, *Priority Open Recommendations: Department of the Treasury* (GAO-22-105633; May 10, 2022)
[34] The NIST Cybersecurity Framework functions include: Identify, Protect, Detect, Respond and Recover.

The Department continues to report progress in managing risk as Treasury obtained an overall rating of "Managing Risk" across all NIST CSF categories (Identify, Protect, Detect, Respond and Recover) on the OMB Cybersecurity Risk Management Assessment for the first time in fiscal year 2021. Treasury also reported the creation of enhanced risk profiles to allow senior leadership greater visibility into the risks for all Departmental High Value Assets. [35] While addressing increases in cyber threats, Treasury will need to continue to balance cybersecurity demands while maintaining and modernizing Information Technology (IT) systems. To this end, Treasury must ensure that cybersecurity is fully integrated into its IT investment decisions as discussed in Challenge 4.

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

Over the past year, the Office of Terrorism and Financial Intelligence (TFI) has remained dedicated to countering the ability of financial networks that support terrorists, organized transnational crime, weapons of mass destruction proliferators, and other threats to international security through intelligence analysis, sanctions, and international private-sector cooperation. As previously reported, identifying, disrupting, and dismantling these networks continue to be challenging as TFI's 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, by using designations and economic sanctions. TFI has significantly increased sanctions against Russia related to its actions against Ukraine and other malign activities. 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. 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.

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

[35] 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.

faces an additional challenge, to develop and implement a new secure database for small businesses to report their beneficial ownership information, as required by the Corporate Transparency Act.[36] However, FinCEN does not expect to implement the database until January 2024.

Challenge 4: 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* [37] 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.[38] 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.[39] In its March 2021 high risk report, GAO acknowledged that the Federal Government 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. In general, federal agencies had not (1) modified their practices to fully address the role of the CIO, (2) documented modernization plans or included key best practice elements in the plans, (3) taken further action to reduce duplicative IT contracts, and (4) implemented the remaining 400 open recommendations related to management of IT acquisitions and operations. For example, 21 of the 24 major federal agencies, still have not implemented IT management policies that fully addressed the role of their CIOs consistent with federal laws and OMB's FITARA guidance. The guidance covers, among other things, enhancing the authority of federal CIOs and ensuring that program staff have the necessary knowledge and skills to effectively acquire IT. In addition, progress in establishing key IT workforce planning processes is also lacking. GAO also noted that the General Services Administration and OMB had fewer funds available than anticipated to award to new

[36] Public Law 116-283 (January 1, 2021).
[37] Public Law 104-106 (February 10, 1996).
[38] Public Law 113-291 (December 19, 2014).
[39] GAO, *High- Risk Series*, *An Update* (GAO-15-290; February 11, 2015).

projects for replacing aging IT systems.[40] Furthermore, GAO recommended that, in general, agencies needed to improve CIOs' authorities, enhance transparency and improve risk management of IT investments, and consolidate federal data centers.[41]

The House Oversight and Reform Committee worked with GAO to develop a 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 B. More recently, in 2021, Treasury received a B for its FITARA implementation efforts, and dropped to a C in July 2022. Areas needing most improvement were enhanced transparency and risk management (i.e. IT investment risk), improved cybersecurity, and agency CIO authority enhancements. The latest scorecard features seven grading categories – down from eight categories on the December 2021 scorecard due to the sunsetting of the data center optimization category.

As of March 16, 2022, Treasury reported that approximately $2.56 billion was spent on major IT investments, which is expected to increase in fiscal year 2023. Given this sizable investment, we are reporting the Department's IT acquisition and project management as an ongoing management and performance challenge distinct from challenge 2 that addresses cybersecurity concerns. Treasury's bureaus reported 48 major IT investments. Treasury's CIO assessed 46 IT investments as having moderately low or low risk to accomplishing their goals. Two IT investments, which reside at the Bureau of the Fiscal Service (Fiscal Service), were assessed as having medium risk[42] to accomplishing their goals:

- Post Payment Services, and
- Debt Collection Services (DCS).

Projects identified with medium overall risk in cost and scheduling require special attention from the highest level of agency management. During fiscal year 2022, some projects within DCS were behind schedule and over budget. Treasury also identified projects within DCS as having a high risk to accomplishing their goals. In June 2022, Treasury reported that Fiscal Service has conducted internal "chat stats" to address project schedule variances for both Post Payment Services and DCS. Treasury is also meeting about one project within the Post Payment Services investment to prepare an updated plan and integrated master schedule to address prior schedule and cost variances. Overall, approximately 91 percent of Treasury's total IT projects were on schedule and approximately 78 percent were within budget. As of March 16, 2022, approximately 43 percent of Treasury's total IT spending is on 48 major investments.

[40] GAO, *High-Risk Series, Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas* (GAO-21-119SP: March 2020).
[41] GAO, *High-Risk Series, Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas* (GAO-21-119SP: March 2021).
[42] 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 a five-point risk scale as follows: 5=low risk, 4= moderately low risk, 3= medium risk, 2= moderately high risk, and 1=high risk.

Another major investment of note, Treasury's Wholesale Securities Services (WSS), includes the Financing Modernization project, a multi-year program to modernize the debt financing system to align with Treasury's strategic priorities and long-term business requirements. This modernization will include development of a new system to support operations, meet customer expectations, become current with existing technologies, manage technical debt, and improve the delivery of secure, flexible, and resilient financing services. Fiscal Service expects to complete the project's network connectivity design by the first quarter of fiscal year 2023.

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 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. 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. Fiscal Service's financial community was trained on TBM and has eliminated all uncategorized IT spending, or spending that is not categorized into standard IT buckets but are continuing efforts on maturity of that data.

Non-IT related acquisitions also require attention to ensure timely delivery and minimization of cost overruns for achieving cost savings. The Program Management Improvement Accountability Act of 2016, P.L. 114-264, 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.

The Bureau of Engraving and Printing (BEP) project to replace its Washington, DC facility with a new facility was estimated to cost $1.25 billion. However, this cost estimate will be updated to better reflect supply chain and industry labor limitations as well as further analysis of project cost. The Board of Governors of the Federal Reserve System (Board) requested a project management assessment be conducted by MITRE Corporation with specific reporting around costs, schedule, and change management. [43] This report had several recommendations, and BEP has worked with the Board to address them. BEP has resumed the design and engineering work for the new facility. In fiscal year 2022, BEP continued site preparation for construction of the new building. Until the estimated completion of the facility in 2027, BEP will need to ensure it employs effective project oversight for preparation of the land, construction of the building, purchase of equipment and machinery, and employment of a workforce to produce the new family of secure notes and maintain confidence in U.S. currency.

[43] In 2016, BEP provided its Western Currency Facility expansion plans to the Board. According to Board officials, the Board's role is to reimburse expenses related to the Western Currency Facility expansion, which did not require a formal approval request or cost justifications from BEP for initiating the expansion.

Challenge 5: Climate Initiatives Risk (New)

In January 2021, EO 14008, *Tackling the Climate Crisis at Home and Abroad*, identified the immediate need for comprehensive action to address the catastrophic impacts of climate change. EO 14008 emphasizes that U.S. leadership, and that of federal departments and agencies, will be required to significantly enhance global action and achieve the necessary policy outcomes on climate change. Furthermore, in May 2021, the White House introduced EO 14030, *Climate-Related Financial Risk,* which aims to: (a) advance consistent, clear, intelligible, comparable, and accurate disclosure of climate-related financial risk, including both physical and transition risks; (b) mitigate that risk and its drivers, while accounting for and addressing disparate impacts on disadvantaged communities and communities of color and spurring the creation of well-paying jobs; and (c) achieve the Administration's target of a net-zero emissions economy by no later than 2050. The Secretary of the Treasury, as the Chair of the Financial Stability Oversight Council (FSOC), will lead several efforts related to EO 14030. Taken together, these two EOs place an emphasis on ensuring climate change is at the forefront of U.S. foreign policy and national security; establishing a government-wide approach to the climate crisis; and bolstering the resiliency of our communities, States, Tribes, territories, and financial institutions to position the United States to lead the global economy to a more prosperous and sustainable future. Treasury will play a significant role working with other federal agencies, foreign governments, and international financial institutions to stimulate global action on addressing climate change, environmental justice, and climate change-created economic and financial crises. In 2021, Treasury created a new Climate Hub and appointed a Climate Counselor to coordinate and lead many of its efforts to address climate change. The Treasury Climate Hub will coordinate and enhance existing climate-related activities by utilizing the tools, capabilities, and expertise from across the Department – including officials from Domestic Finance, Economic Policy, International Affairs, and Tax Policy. With a view of all Treasury climate initiatives, the Hub will enable Treasury to prioritize climate action.

As stated in its July 2021 Climate Action Plan, Treasury anticipates that climate change will continue to be a significant global challenge and that aspects of its mission and operations will be impacted by global warming, sea level rise, increased intensity and frequency of major weather events, and impacts on energy availability. To manage the process of climate change adaptation and resilience within Treasury's operations and its facilities, the Department has developed a comprehensive management framework, in accordance with the Interim Instructions for Preparing Draft Climate Action Plans under EO 14008. Treasury's Departmental Offices and operating bureaus will continually assess changing conditions and scientific understanding of climate change to adjust policies, programs, and activities to improve resilience and adaptation. Treasury's Climate Action Plan establishes the following five priority actions to strengthen and build upon Treasury's climate resilience and adaptive capabilities: (1) rebuilding programs and capabilities that may have atrophied or stagnated in recent years; (2) addressing climate change impacts and vulnerabilities across the range of Departmental operations, including administrative, manufacturing, and law enforcement activities; (3) ensuring a climate-focused approach to managing Treasury's real property portfolio footprint; (4) enabling procurement management to fully consider climate change realities; and (5) providing, measuring, and accounting for a financial investment approach appropriate to the Department's climate objectives.

Treasury is also engaged in the Administration's domestic efforts through its role as a leading banking regulator, with the Office of the Comptroller of the Currency (OCC), and its responsibilities within FSOC. Internationally, Treasury represents the United States at the G7 and G20, at the Financial Stability Board, and other institutions and forums such as the International Monetary Fund. In October 2021, FSOC issued its Report on Climate-Related Financial Risk, as mandated by EO 14030. In it, FSOC details the activities of each member to date to address climate-related financial risk, including Treasury, the Office of Financial Research, the Federal Insurance Office, and OCC. The report highlights challenges in efforts to comprehensively understand and address climate-related financial risk. Those challenges include the types and quality of available data and measurement tools, the ability to assess climate-related financial risks and vulnerabilities, and how best to incorporate these risks into management practices and supervisory expectations as appropriate. FSOC concluded the report with thirty-five recommendations. Many, if not most, apply to the Department, the Office of Financial Research, the Federal Insurance Office, and OCC. It will be important that each recommendation be addressed not only timely, but collectively with the other FSOC members to ensure a cohesive response.

Furthermore, OCC has implemented multiple initiatives to address climate change and climate-related financial risk. They have partnered with other Federal banking regulators to work collaboratively in understanding the risks and development of climate-related risk management. OCC has also engaged with international groups to share best practices. Internally, OCC established a Climate Risk Implementation Committee chaired by a Climate Change Risk Officer to assess climate risks and advise management on OCC policy, banking supervision, and research. These collaborations will continue to be important in developing a common understanding of climate-related financial risks and their impact to ensure the continued safety and soundness of the banking system. OCC also continues to work with FSOC and other member agencies to understand the broader implications of climate-related financial risks and their potential impact on financial stability.

Other Matter of Concern

Although we are not reporting digital assets as a management and performance challenge, we are highlighting it as an area of concern.

Use of digital assets, including cryptocurrencies, stablecoins, and in some countries, central bank digital currency (CBDC), has grown significantly over the past several years. As of September 15, 2022, digital assets reached a combined market capitalization of over $1 trillion, up from approximately $14 billion in late 2016 but down from $3 trillion during November of 2021.[44]

Treasury supports responsible innovation and seeks to maximize the gains from this new technology while protecting against possible risks to consumers, financial stability, and illicit finance. In the absence of sufficient oversight and regulatory safeguards, the increase in use of digital assets could pose risks to consumers, investors, and the broader financial system.

[44] Please click on the following link for current market capitalization information: Cryptocurrency Prices, Charts, and Crypto Market Cap | CoinGecko

In March 2022, President Biden convened experts from across the Administration to ensure a coordinated and comprehensive approach to digital assets policy and charged Treasury with a leadership role in this work. EO 14067, *Ensuring Responsible Development of Digital Assets*, establishes the following policy objectives with respect to digital assets: (1) protect consumers, investors, and businesses in the United States; (2) protect the United States and global financial stability and mitigate systemic risk; (3) mitigate the illicit finance and national security risks posed by misuse of digital assets; (4) reinforce United States leadership in the global financial system and in technological and economic competitiveness, including through the responsible development of payment innovations and digital assets; (5) promote access to safe and affordable financial services; and (6) support technological advances that promote responsible development and use of digital assets.

In September 2022, Treasury published a report on the future of the U.S. money and payments systems, in which Treasury encourages continued work on innovations to promote a system that is more competitive, efficient, and inclusive – and that also helps maintain and build on the United States' global financial leadership.[45] The report recommends advancing policy and technical work on a potential U.S. CBDC, so that the United States is prepared if a CBDC is determined to be in the national interest. Treasury also published a report on the implications of digital assets for consumers, investors and businesses, laid out a detailed Action Plan to prevent digital assets from being used for financial crimes, such as money laundering and terrorism financing, and sent a framework to the President for international engagement on digital asset issues. In October 2022, FSOC released a report on potential financial stability risks, and recommended steps to address gaps in the regulation of digital assets in the United States.[46]

Following the publication of these reports, Treasury has a number of responsibilities, including participating in an interagency working group regarding a potential central bank digital currency and working with other agencies to prepare resources for consumers. The Office of Domestic Finance, Office of Terrorism and Financial Intelligence, and Office of International Affairs will be primarily driving this work, in coordination with other parts of Treasury and the interagency, as appropriate.

[45] Treasury Report, *The Future of Money and Payments: Report Pursuant to Section 4(b) of Executive Order 14067* (September 2022).
[46] Financial Stability Oversight Council. *Report on Digital Asset Financial Stability Risks and Oversight* (October 2022).

Appendix: Acronyms and Abbreviations

ARP	American Rescue Plan Act of 2021
BEP	Bureau of Engraving and Printing
Board	Board of Governors of the Federal Reserve System
BSA	Bank Secrecy Act
CAA, 2021	Consolidated Appropriations Act, 2021
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CBDC	Central Bank Digital Currency
CDFI	Community Development Financial Institutions
CERTS	Coronavirus Economic Relief for Transportation Services
CIO	Chief Information Officer
COVID-19	Coronavirus Disease 2019
CPF	Coronavirus Capital Projects Fund
CRF	Coronavirus Relief Fund
CSF	Cybersecurity Framework
DCS	Debt Collection Services
Department	Department of the Treasury
ECIP	Emergency Capital Investment Program
EO	Executive Order
ERA	Emergency Rental Assistance
ERA1	Emergency Rental Assistance Program 1
ERA2	Emergency Rental Assistance Program 2
ERP	Equitable Recovery Program
FinCEN	Financial Crimes Enforcement Network
FAC	Federal Audit Clearinghouse
Fiscal Service	Bureau of the Fiscal Service
FITARA	Federal Information Technology Acquisition Reform Act
FSOC	Financial Stability Oversight Council
GAO	Government Accountability Office
HAF	Homeowner's Assistance Fund
IT	Information Technology
LATCF	Local Assistance and Tribal Consistency Fund
NEU	Non-Entitlement Units
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OIG	Office of Inspector General
OMB	Office of Management and Budget
PRAC	Pandemic Response Accountability Committee
PSP1	Payroll Support Program
PSP2	Payroll Support Program Extension
PSP3	Payroll Support Program 3
RRP	Rapid Response Program
SEDI	Socially and Economically-Disadvantaged Individuals
SIGPR	Special Inspector General for Pandemic Recovery
SLFRF	Coronavirus State and Local Fiscal Recovery Funds
SSBCI	State Small Business Credit Initiative

TBM	Technology Business Management
TFI	Office of Terrorism and Financial Intelligence
Treasury	Department of the Treasury
WSS	Wholesale Securities Services