

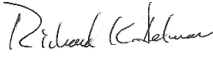


OFFICE OF
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

October 10, 2023

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-24-001)

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 six challenges, one of which is new and reports on the challenges faced with operating in an uncertain environment. As shown below, five 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. The new challenge considers factors beyond Treasury’s control and their impact on Treasury’s operations.

- 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 (Repeat)
- Operating in an Uncertain Environment (New)

We identified challenges 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. While the national emergency declaration for the COVID-19 pandemic ended in May 2023, Treasury programs established to support the pandemic are in various stages of maturity and continue to pose challenges for Treasury. 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
Assistant Secretary for Management

Contents

Challenge 1: COVID-19 Pandemic Relief (Repeat)	1
Pandemic Programs- End of Period of Performance	1
Payroll Support Programs	1
Coronavirus Economic Relief for Transportation Services	2
Coronavirus Relief Fund.....	2
First Emergency Rental Assistance Program (ERA1)	3
Pandemic Programs- Ongoing Period of Performance	3
Second Emergency Rental Assistance (ERA2) and Homeowner Assistance Funds	4
Coronavirus State and Local Fiscal Recovery Funds.....	4
State Small Business Credit Initiative	6
Emergency Capital Investment Program	7
CDFI Equitable Recovery Program.....	8
Accountability and Transparency.....	9
Challenge 2: Cyber Threats (Repeat)	10
Challenge 3: Anti-Money Laundering/Terrorist Financing and Bank Secrecy Act Enforcement (Repeat)	13
Challenge 4: Information Technology Acquisition and Project Management (Repeat)	14
Challenge 5: Climate Initiatives Risk (Repeat)	17
Challenge 6: Operating in an Uncertain Environment (New)	18
Debt Limit and the Budget	19
Rising Interest Rates and Inflation	20
Appendix: Acronyms and Abbreviations	22

Challenge 1: COVID-19 Pandemic Relief (Repeat)

The COVID-19 pandemic continues to affect the health and economic stability of communities worldwide and thus the Department of the Treasury's (hereinafter Treasury or the Department) responsibilities and workloads are still enormously expanded. Specifically, Treasury has been instrumental to the implementation of economic relief provisions of the *Coronavirus Aid, Relief, and Economic Security Act*¹ (CARES Act), the *Consolidated Appropriations Act, 2021*² (CAA, 2021), the *American Rescue Plan Act of 2021*³ (ARP), and the *Consolidated Appropriations Act, 2023*⁴ (CAA, 2023). Treasury is tasked with disbursing over \$655 billion⁵ in aid to more than 30,000 recipients, including state, local, territorial, and tribal government entities, in a relatively short period of time and with limited staffing. As such, the Department established the Office of Recovery Programs (ORP) to implement Treasury's COVID-19 pandemic programs. A Chief Recovery Officer, who is the lead administrator and the principal advisor to the Treasury Secretary and Deputy Secretary on pandemic programs, leads the office. With ORP leading, the Department implemented multiple pandemic programs and is now challenged with managing those programs in different stages of maturity. In addition, Treasury must carry the administrative and monitoring responsibilities in its role resolving Single Audit Act findings and potentially serving as cognizant agency for a significant number of entities⁶ in compliance with the Office of Management and Budget's (OMB) *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*.⁷

Pandemic Programs- End of Period of Performance

For pandemic programs near the end of the period of performance, Treasury faces challenges (1) closing out awards, (2) resolving Single Audit Act findings, (3) maintaining internal control, guidance, and methodologies for oversight of funds disbursed, (4) collecting high quality, reliable data, and (5) sustaining operations with limited funding. The pandemic programs near maturity or in the close out phase include the Payroll Support Programs (PSP), Coronavirus Economic Relief for Transportation Services (CERTS), the Coronavirus Relief Fund (CRF), and the first Emergency Rental Assistance Program (ERA1).

Payroll Support Programs

To maintain pay and benefits of airline industry workers, Treasury implemented PSP1 authorized under the CARES Act for up to \$32 billion of direct financial assistance for passenger air carriers, cargo air carriers, and contractors. 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 (PSP2) and \$15 billion (PSP3), respectively. Using existing resources and contractor support, Treasury disbursed a total of approximately \$58.9 billion, as of June 30, 2023,

¹ Public Law 116-136 (March 27, 2020)

² Public Law 116-260 (December 27, 2020)

³ Public Law 117-2 (March 11, 2021)

⁴ Public Law 117-328 (December 29, 2022)

⁵ 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.

⁶ 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)

⁷ <https://www.ecfr.gov/current/title-2/part-200>

to air carriers and contractors under all three payroll support programs. My office has completed 10 audits of recipients' certified financial data provided to Treasury in applications for a PSP1 award. Our audits identified approximately \$1.37 million in questioned costs/improper payments. It is important for Treasury to recoup these payments and to obtain support documentation to confirm awarded amounts for the hundreds of other recipients that have not yet been audited. My office will continue audits of PSP1 recipients' certifications and initiate audits of certifications submitted by PSP2 recipients in fiscal year 2024. It is incumbent upon the Department to maintain strong internal controls over recipients' compliance with signed terms and conditions for receiving financial assistance.

Coronavirus Economic Relief for Transportation Services

Congress expanded financial support to non-air carrier transportation service providers under the 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. Treasury disbursed approximately \$1.97 billion to 1,464 recipients as of February 3, 2023. The CERTS period of performance ended on October 22, 2022. During the close out phase of this program, Treasury should maintain strong internal controls to ensure compliance with grant agreements. Although there is no mandate directing my office to audit CERTS recipients, we are currently auditing Treasury's administration of the program.

Coronavirus Relief Fund

The \$150 billion 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. 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), "Use of Funds," of the *Social Security Act*, as amended.⁸

The Department also has a fundamental role to clarify its policy⁹ over the uses of funds when interpretation matters arise. As of September 30, 2023, recipients are still in the process of

⁸ Section 601 (d), Use of Funds, recipients shall use the 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. The period of performance end date of the CRF was extended through December 31, 2021 by the Consolidated Appropriations Act, 2021. The period of performance end date for Tribal entities was further extended to December 31, 2022 by the State, Local, Tribal, and Territorial Fiscal Recovery, Infrastructure, and Disaster Relief Flexibility Act, Division LL of the Consolidated Appropriations Act, 2023, P.L. 117-328, December 29, 2022, 136 Stat. 4459.

⁹ *Coronavirus Relief Fund Guidance for State, Territorial, Local, and Tribal Governments* Federal Register, Vol. 86, No. 10; January 15, 2021

reporting on and closing out their awards, and questions may arise that require interpretation.

My office has completed desk reviews¹⁰ of CRF recipients and has identified approximately \$2 billion in questioned costs, which will require interpretation of Treasury's policy to determine eligibility of those expenditures and whether funds should be returned or recouped. The quarterly reporting for the CRF will end with the third quarter of calendar year 2023, making it critical that Treasury provide as much clarity as possible for ensuring recipients understand the compliance requirements and are accountable and transparent in how they report uses of funds. My office has received over 400 complaints regarding recipient, and in some instances sub-recipient, uses of CRF proceeds and approximately 300 of these complaints require continued collaboration between the Department and my office. In addition, Treasury's responsibilities to provide management responses to Single Audit Act findings for the CRF within required timeframes is a challenge given limited resources and funding.

First Emergency Rental Assistance Program (ERA1)

To assist vulnerable households at risk of housing instability, Congress established the first of two ERA programs, ERA1, in CAA, 2021 availing about \$25 billion to households in need. Division N, Title V, Subtitle A, of CAA, 2021, created ERA1 and requires that my office conduct monitoring and oversight of the receipt, disbursement, and use of ERA1 funds. As of June 22, 2023, Treasury disbursed \$24.98 billion of the \$25 billion appropriated by CAA, 2021 for ERA1. Treasury disbursed ERA1 funds 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. With ERA1 disbursements complete and the end of the period of performance for these awards, Treasury faces challenges administering the closeout process and resolving Single Audit Act findings associated with hundreds of eligible grantees and related sub-recipients. To date, my office has received more than 3,500 complaints from the public concerning ERA usage, expediency of payments to beneficiaries, and potential improper payments. Treasury will need to work with my office to recoup ERA funds not used for allowable purposes.

Pandemic Programs- Ongoing Period of Performance

For programs where the period of performance and administration is ongoing, Treasury faces challenges (1) ensuring proper allocation and distribution of funds, (2) developing and maintaining internal control, guidance, and methodologies and procedures for monitoring and reporting, (3) finding and/or maintaining qualified staff needed to administer and monitor programs, (4) collecting high-quality, reliable data, (5) resolving Single Audit Act findings, (6) remediating and recouping funds, and (7) sustaining operations with limited funding. These programs include the second Emergency Rental Assistance Program (ERA2), the Homeowner Assistance Fund

¹⁰ The CARES Act assigned the Department of the Treasury Office of Inspector General with responsibility for compliance monitoring and oversight of the receipt, disbursement, and use of CRF payments. The purpose of a desk review is to perform monitoring procedures of the prime recipient's receipt, disbursement, and use of CRF proceeds as reported in the grants portal on a quarterly basis.

(HAF), the Coronavirus State and Local Fiscal Recovery Funds (SLFRF), the State Small Business Credit Initiative (SSBCI), the Emergency Capital Investment Program (ECIP), and the Community Development Financial Institutions (CDFI) Fund's Equitable Recovery Program (ERP).

Second Emergency Rental Assistance (ERA2) and Homeowner Assistance Funds

With ARP, Congress established a second ERA program, ERA2, to provide additional assistance to vulnerable households at risk of housing instability, availing over \$21.55 billion to households in need. For ERA2, as of June 22, 2023, Treasury disbursed \$20.94 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 ERA2 does not include tribal governments as eligible grantees. ERA2 funds are to remain available until September 30, 2027. While CAA, 2021 requires that my office conduct monitoring and oversight of the receipt, disbursement, and use of ERA1 funds, ARP does not require my office to monitor ERA2. ERA2 disbursements are ongoing and Treasury faces challenges in maintaining internal control and establishing guidance and methodologies for monitoring, reporting, and oversight of funds disbursed. In addition, the lack of consistent quality, reliable grantee disbursement data and an adequate workforce impedes Treasury's ability to perform proper monitoring and recoupment functions. Further, Treasury faces challenges resolving Single Audit Act findings associated with hundreds of eligible grantees and related sub-recipients. To date, my office has received more than 3,500 complaints from the public concerning ERA usage, expediency of payments to beneficiaries, and potential improper payments. Treasury will need to work with my office to recoup ERA funds not used for allowable purposes.

In addition to ERA2, ARP 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. Treasury has implemented the HAF program and as of July 2023, disbursed more than \$9.8 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.

The ERA and HAF programs are fully implemented and, while Treasury has issued relevant guidance for each of the programs, it is essential its program offices continue to respond to recipients to clarify guidance and to provide insight into the eligible uses of the funds Treasury distributed. Clear and timely responses to recipient questions is critical in enabling program recipients to administer their programs and disburse funds to households effectively.

Coronavirus State and Local Fiscal Recovery Funds

The SLRF 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). Administering SLFRF requires recipients to obligate funds by December 31, 2024 and expend all obligations by December 31, 2026, except as noted below for the Surface Transportation projects and Title I. This 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 approximately 26,000 Non-Entitlement Units (NEU) of

Local Governments that received funding through a state or U.S. territory. 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 required to have a Single Audit or alternate compliance examination engagement over which Treasury may have agency cognizance or oversight. As a result, Treasury will face challenges with ongoing compliance monitoring of SLFRF recipients and related administrative issues.

While Treasury has built the Treasury Recovery Award Management System for recipient communication and reporting, there are still challenges obtaining sufficient quality data from SLFRF, CPF, and LATCF recipients. For SLFRF recipients, Treasury allows for lengthy narrative responses as part of the data collection that may be more cumbersome to review and lack critical details. Confirming data quality and providing timely data to the public and oversight community has been challenging for Treasury. To effectively administer and monitor recipients' compliance, Treasury must have access to sufficient data that accurately reflects how recipients have expended pandemic awards. While progress has been made, it is critical that Treasury continue to refine mechanisms to ensure the data is complete, accurate, reliable, and transparent in reflecting how recipients have expended pandemic awards. Treasury will need to continue to collect sufficient and timely data for monitoring recipients' compliance with pandemic programs, and to ensure remediation and recoupment actions occur, as appropriate. Additionally, while much of Treasury's pandemic funding has been distributed, Treasury must deliver the remaining CPF and LATCF funds through fiscal year 2024, ensuring accurate allocations and award distributions, and timely obligations.

Treasury ORP initially had difficulty finding specialized staff to administer and monitor the SLFRF program and faces ongoing challenges to recruit and retain staff as the program matures. Treasury has also been challenged with compliance report review backlogs and vast testing workloads. As discussed in more detail under the Accountability and Transparency section below, Treasury faces future funding challenges to support ORP operations, to include ongoing administration of the SLFRF program and recipient monitoring. An additional challenge for Treasury has been coordinating with other Federal Agencies, such as Federal Emergency Management Agency, the Department of Transportation, and the Department of Housing and Urban Development to develop regulations and update reporting guidance for SLFRF recipients. In August 2023, Treasury published an interim rule for guidance to ensure that recipients are aware of the additional SLFRF allowable uses of funds for emergency disaster relief and infrastructure projects, in accordance with program flexibilities provided under Division LL of the CAA, 2023 legislation. While provisions in the interim rule became effective September 20, 2023, Treasury will need to consider additional feedback through fiscal year 2024. Consistent with the existing SLFRF eligible uses, recipients must obligate funds for the new SLFRF eligible uses by December 31, 2024. Recipients must expend SLFRF funds obligated to provide emergency relief from natural disasters by December 31, 2026. Recipients must expend SLFRF funds obligated for Surface Transportation projects and Title I projects by September 30, 2026.

With the overlap of CRF, SLFRF, CPF, and LATCF recipients, we expect that there may be continued confusion between the uses of funds requirements and reporting mechanisms that may be a challenge for recipients. 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 Single Audits. 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 2023, Treasury provides the option of an alternate compliance examination engagement for SLFRF recipients meeting certain eligibility requirements. Treasury worked with OMB and the audit community to find a solution for receiving these non-audit reports. The Federal Audit Clearinghouse, which operates on behalf of OMB to support oversight and assessment of federal award audit requirements and maintain a public database of completed audits, is now receiving these alternate compliance examination reports for fiscal year 2022, and will continue to do so going forward. Single Audit and alternative compliance examination procedures are relatively new to 25,000 SLFRF recipients, so there will continue to be more guidance and oversight required of Treasury.

State Small Business Credit Initiative

The SSBCI, which was originally created in the *Small Business Jobs Act of 2010*¹¹ 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 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. As a result of the debt ceiling crisis, the *Fiscal Responsibility Act of 2023*¹² rescinds \$150 million from the SSBCI program. As of July 2023, out of \$8 billion in approved applications in the capital program, Treasury has distributed \$2.45 billion to 64 states, U.S. territories, and Tribal governments.

Treasury faces challenges as it continues to administer the program through the approval of applications, distribution, and monitoring of the funds. 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

¹¹ Public Law 111-240 (September 27, 2010)

¹² Public Law 118-5 (June 3, 2023)

approved for SSBCI funding comply with program requirements. In November 2022, Treasury issued its *SSBCI Capital Program National Compliance Standards* to set forth recommended practices to support participating jurisdictions in implementing their SSBCI capital programs.¹³ These standards compliment the SSBCI Capital Program Policy Guidelines, which require certifications from lenders, investors, borrowers, and investees for each SSBCI-supported transaction.¹⁴ Certifications include information on conflicts of interest and use of proceeds among other things. The guidelines also state that participating jurisdictions should, as part of their compliance monitoring procedures and as appropriate to the requirements of a specific certification, establish a process to determine whether the required certifications have been properly documented. However, Treasury does not require participating jurisdictions to independently verify the representations made by the authorized representative of the small business borrower or investee. Relying on the participating jurisdictions to ensure that required certifications are collected could lead to Treasury not (1) identifying non-compliant recipients, (2) holding recipients accountable for SSBCI-supported transactions, and/or (3) properly remediating and recouping funds.

Additionally, under the SSBCI program, an Allocation Agreement establishes the terms and conditions for participating jurisdictions to receive capital funds. The Allocation Agreement, in part, requires a participating jurisdiction to promptly notify Treasury in writing if there has been any material adverse change in the condition, financial or otherwise, or operations of the participating jurisdiction that may affect its approved programs. As noted in our previous Management Challenges Letter, Treasury still needs to define what constitutes a material adverse change that may affect the participating jurisdictions' approved programs. Treasury may have difficulty collecting high quality, reliable data and monitoring the recipients' use of funds. Further, Treasury must ensure proper allocation and distribution of funds in compliance with the multiple set-asides of the program. Therefore, Treasury must continue to develop and maintain internal controls, program guidance, and methodologies and procedures for monitoring and reporting the use of SSBCI funding. Treasury must also be cognizant of possible additional reductions in the funding of the program, which could impact their ability to maintain qualified staff needed to administer and monitor programs and sustain operations.

Emergency Capital Investment Program

As authorized under CAA, 2021, Treasury has invested \$8.57 billion in 175 CDFIs¹⁵ and Minority Deposit Institutions, which is all of the capital available for investment under ECIP, providing capital to low-to-moderate income community financial institutions that support small businesses and consumers. Originally, Treasury 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

¹³ *SSBCI Capital Program National Compliance Standards*. U.S. Department of the Treasury. November 17, 2022.

¹⁴ *SSBCI Capital Program Policy Guidelines*, U.S. Department of the Treasury, November 10, 2021, and as amended August 16, 2023.

¹⁵ 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.

fully implement and administer investments.¹⁶ With all allowable investments made, *The Fiscal Responsibility Act of 2023*, enacted on June 3, 2023, rescinded the funding that was available for a second investment round. After the implementation audit, Treasury provided policies and procedures related to the ECIP. It is imperative that Treasury implement and uphold policies and procedures to govern its post-investment activities.

Participants in the ECIP are required to calculate and provide their baseline amount of qualified lending through an Initial Supplemental Report. This baseline will be used to calculate the dividend or interest rates applicable to each participant in accordance with the Rate Reduction Incentive Guidelines and the ECIP legal agreements. In June 2023, Treasury provided waivers for certain ECIP recipients, removing the requirement in the ECIP Securities Purchase Agreement for attestation from their independent auditor that the processes and controls used to generate the Supplemental Reports are satisfactory for 2022. This change potentially lowers the reliability of self-reported data. Also in June 2023, Supplemental Reporting deadlines were extended for progress reports from certain ECIP recipients because Treasury had not yet received final approval on the forms and instructions. Treasury also extended 2022 quarterly reporting to August 17, 2023 and first and second 2023 quarterly reporting to September 1, 2023. Treasury needs to implement planned controls to ensure that investments provide the intended benefits. Accountability and transparency are crucial for the integrity of the program.

CDFI Equitable Recovery Program

On April 10, 2023, the CDFI Fund announced the awarding of \$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.

The CDFI Fund is in the process of adapting existing policies and procedures, compliance monitoring tools, and data collection forms that have been successfully used to monitor the CDFI Fund's other programs to effectively monitor the CDFI ERP Awards.

In addition, the CDFI Fund plans to implement designation of minority lending institutions (MLI) as defined under the CAA, 2021 separately from the award of ERP funds. The CDFI Fund requested public comment on the criteria that will be used to designate a certified CDFI as a MLI from July 28, 2022, to November 25, 2022. As noted within the CDFI ERP Notice of Funds Availability, this criterion was not used as part of the CDFI ERP award process. Going forward, Treasury has a lengthy period of performance for award recipients, so there is much work to be done overseeing the CDFI ERP awards and determining next steps regarding the new MLI certification.

¹⁶ OIG, *Audit of Treasury's Implementation of the Emergency Capital Investment Program* (OIG-22-028; March 8, 2022)

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 of the pandemic relief funding. 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 Single Audit findings to ensure that recipients take appropriate and timely corrective action and issue management decision letters.¹⁷ 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 compliance examination findings specific to each of its pandemic relief programs. Given the anticipated budget shortfalls 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 (SIGPR),¹⁸ Treasury Inspector General for Tax Administration, 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, 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 Treasury has leveraged its existing workforce, hired contractors, and obtained detailees from other Federal agencies to address the demands of the pandemic programs, it continues to face future funding challenges to carry out its expansive administrative and compliance monitoring role. For fiscal year 2023, Treasury ORP supported nine pandemic programs valued at over \$648 billion for awards across 30,000 recipients. Total administrative budget for the year was \$96.6 million.¹⁹

¹⁷ 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-ECFR4424206aeacf751/section-200.521>)

¹⁸ 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 SIGPR's activities and Treasury's loan programs. SIGPR terminates five years after enactment of the CARES Act (March 27, 2025).

¹⁹ <https://home.treasury.gov/system/files/266/07A.-COVID-FY-2023-CJ.pdf>

At the same time Treasury worked to modify its operating model to rely on data-centric, risk-based monitoring and to minimize staffing to oversee the programs, 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. However, this may not be enough to carry out the large-scale compliance monitoring responsibilities of SLFRF, CPF, ERA, HAF, and LATCF.

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 the COVID-19 pandemic national emergency declaration ended in May 2023, I remain 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 and reported by GAO as a government-wide issue in its 2023 high-risk list published biennially.²⁰ 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 on-going conflict in Ukraine,²¹ or when serious flaws are discovered in software or systems that allow for remote administrative-level access.

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 increasing sophistication. Such attacks include distributed denial of service, phishing, fraudulent wire payments, business email compromise, malicious spam (malspam), ransomware, and

²⁰ GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas* (GAO-23-106203: April 20, 2023)

²¹ 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)

compromise of supply chains (both hardware and software). Additionally, Treasury must remain cognizant of the increased risk profile a remote workforce presents, as it 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, and denial of service attacks upon a network or service can disrupt operations and prevent remote workers from performing their duties.

There is continuing concern over foreign adversaries creating and exploiting vulnerabilities in the Nation's supply chain for information and communication technology and services. 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.²² On May 10, 2023, this EO was extended again for 1 year.²³ 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,²⁴ 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*²⁵ to provide the strategy for achieving a zero-trust architecture, and require 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*²⁶ 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 fiscal year 2022 memorandum, Treasury reported the Enterprise Cyber Risk Management program enhanced the risk assessment process to identify 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,

²² EO 13873, *Securing the Information and Communications Technology and Services Supply Chain* (May 15, 2019)

²³ *Message to the Congress on the Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain* (May 10, 2023)

²⁴ 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.

²⁵ 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>)

²⁶ 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>)

management must be cognizant of, and mitigate, the risks posed by attacks made against other federal and non-federal agencies and Treasury contractors and subcontractors. Threats and risks to third parties' networks and systems also pose risks to Treasury's networks and systems, due to interconnections 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* (FISMA) audits (fiscal years 2015, 2016, 2017, and 2018),²⁷ with one repeat recommendation, related to third-party cloud service providers demonstrating FISMA compliance, remaining unimplemented as of fiscal year 2022. As of this letter, work is being performed to verify closure of the recommendation.

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 Cybersecurity and Critical Infrastructure Protection 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. 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.²⁸ 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.²⁹ 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 2020, GAO recommended that Treasury track the content and progress of sector wide cyber risk mitigation efforts, and prioritize their completion according to sector goals and priorities in the sector-specific plan. Additionally, Treasury should update the financial services sector-specific plan to include specific metrics for measuring the progress of risk mitigation effects and information on the sector's ongoing and planned risk mitigation efforts.³⁰ However, as of January 2023, GAO reported Treasury had yet to develop methods to determine the level and type of framework adoption, stating that the voluntary nature of private sector participation in sector risk management agency activities affects the agency's ability to implement certain recommendations related to critical infrastructure protection. Treasury was planning implementation of a tool to track sector risks and mitigation efforts, but it was still in development. Lastly, Treasury reported to GAO that it did not believe it would be beneficial to update the sector-specific plan until the Department of

²⁷ Public Law 113-283 (December 18, 2014)

²⁸ NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0, February 12, 2014; superseded by Version 1.1; April 16, 2018)

²⁹ GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption* (GAO-18-211; February 18, 2018)

³⁰ GAO, *Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts* (GAO-20-631; September 17, 2020)

Homeland Security completes its updates to the national plan and provides guidance on sector-specific plans.³¹

The Department reported in its response to last year's letter that it made strategic investments to evolve their cybersecurity infrastructure and bring it into alignment with zero-trust architecture requirements, and mitigate risks associated with the modern threat landscape. Treasury also reported a continued focus on network defense efforts for its High Value Assets.³² 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. Additionally, criminals and other bad actors evolve and continue to develop 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 a variety of targeted financial measures to include designations and economic sanctions. TFI has significantly increased sanctions against Russia related to its actions against Ukraine and its other malign activities. TFI's counter-terrorism designations disrupt the financial networks that support terrorist organizations. Other TFI tools, such as diplomatic and private sector engagement, regulatory oversight, and intelligence analysis, also play an important role. Disrupting terrorist financing depends on a whole-of-government approach and requires collaboration and coordination within Treasury, other federal agencies, the private sector, and international partners.

Collaboration and coordination are key to successfully identifying and disrupting illicit financial networks and meeting TFI's mission. This effort requires effective and efficient working relationships among components within TFI and the Intelligence Community. 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 Treasury's critical 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.

³¹GAO, *Priority Open Recommendations: Department of the Treasury* (GAO-23-106469; July 7, 2023)

³² 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.

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.³³ FinCEN is required to maintain a highly secure database for financial institutions to report BSA information. FinCEN has previously identified that the success of that system depends on the financial sector's confidence that those reports are adequately protected, but unauthorized disclosures threaten to undermine that confidence. The challenge for FinCEN is to ensure the BSA information remains secure in order to maintain the confidence of the financial sector, while meeting the access needs of law enforcement, regulatory, and intelligence partners. FinCEN also faces an additional challenge, to develop and implement a new secure database for certain businesses to report their beneficial ownership information, as required by the *Corporate Transparency Act*.³⁴ FinCEN expects to implement the database in January 2024.

Challenge 4: Information Technology Acquisition and Project Management (Repeat)

The *Federal Information Technology Acquisition Reform Act*³⁵ (FITARA), enacted in December 2014, was the first major overhaul of federal IT management since the passage of the *Clinger-Cohen Act of 1996*,³⁶ 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. 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.³⁷ In its April 2023 high-risk report, GAO acknowledged that the Federal Government has undertaken numerous initiatives to better manage the more than \$100 billion that is invested annually in IT. However, GAO reported that federal IT investments too frequently fail to deliver capabilities in a timely manner. They also incur cost overruns or schedule slippages while contributing little to mission-related outcomes. These investments often lack disciplined and effective management in areas such as project planning, requirements definition, and program oversight and governance. GAO noted that

³³ Public Law 91-508 (October 26, 1970)

³⁴ Public Law 116-283 (January 1, 2021)

³⁵ Public Law 113-291 (December 19, 2014)

³⁶ Public Law 104-106 (February 10, 1996)

³⁷ GAO, *High-Risk Series, An Update* (GAO-15-290; February 11, 2015)

Congress and OMB continue to demonstrate leadership commitment to ensuring agencies implement IT reform initiatives. Additionally, OMB and agencies made progress in implementing GAO's recommendations—73 percent of recommendations have been fully implemented, an increase from 65 percent reported in GAO's 2021 High-Risk List.³⁸ In general, GAO recommends that agencies should implement its 294 open recommendations related to improving the management of IT acquisitions and operations. For example, federal agencies should improve the effectiveness of agency CIOs, enhance IT workforce planning practices, and develop plans for modernizing or replacing legacy systems. GAO also calls on Congress to consider formalizing the federal CIO position and establishing responsibilities and authorities for government-wide IT management, which is an open recommendation for this high-risk area that GAO suggested in September 2022.³⁹

The House Oversight and Accountability 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 December 2022, Treasury received a B for its FITARA implementation efforts. Areas needing most improvement were transparency and risk management (i.e. IT investment risk) and agency CIO authority enhancements. The latest scorecard currently features seven grading categories – down from eight categories on the December 2021 scorecard due to the sunset of the data center optimization category.

As of March 2023, Treasury reported that approximately \$2.5 billion was spent on major IT investments, which is expected to increase. Additionally, approximately 38 percent of Treasury's total IT spending is on 62 major investments. Overall, approximately 87 percent of Treasury's total IT projects were on schedule and approximately 76 percent were within budget. 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. As of August 2023, Treasury's CIO assessed 44 IT investments as having moderately low or low risk to accomplishing their goals. Treasury's CIO also reported 17 IT projects as having medium risk to accomplishing their goals. 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.⁴⁰

Treasury's CIO noted one project, Wholesale Securities Services, as having a high-risk CIO summary investment rating. Treasury's Wholesale Securities Services includes the Financing

³⁸ GAO, *High-Risk Series, Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas* (GAO-21-119SP: March 2021)

³⁹ GAO, *Chief Information Officers: Private Sector Practices Can Inform Government Roles* (GAO-22-104603: September 2022)

⁴⁰ 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.

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. The Bureau of the Fiscal Service (Fiscal Service) has implemented a Program Management Improvement Accountability Act Framework to improve transparency and accountability of project performance, including a monthly dashboard of key metrics on cost, schedule, scope, efficiency, and quality. In addition, Fiscal Service's Chief Information Security Officer is actively monitoring compliance with all Cyber Executive Orders and National Security Council accelerated timelines. Enterprise Architecture and Investment Sub-councils discuss the investment risks regularly and the ratings are also shared with Fiscal Service senior leadership to ensure transparency of the risk. If negative trends surface or persist, the Fiscal Service CIO and CFO have the ability to request an internal Fiscal Service "ChatStat"⁴¹ to take swift action and address risks. ChatStats and related open action items are tracked on the Fiscal Service's Program Management Improvement Accountability Act Project Performance Dashboard.

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.

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*⁴² 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 is currently estimated to cost \$1.78 billion. However, this cost estimate will be updated to better reflect supply chain and industry labor limitations as well as additional costs incurred as the project progresses. In fiscal year 2023, estimates were \$25.96 million for the next phase of the replacement facility project including the completion of the design, and architecture and engineering work for the new facility. The U.S. Army Corps of Engineers will award a construction contract for the replacement facility during fiscal year 2024 with construction expected to begin by fiscal year 2025. Until the estimated completion of the facility in 2027, BEP will need to ensure effective project oversight for 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.

⁴¹ A ChatStat process is where investments or projects are formally reviewed to address negative performance trends or concerns, and to identify course-correction actions that are formally tracked. ChatStats are monitored monthly by Fiscal Service senior leadership until resolved.

⁴² Public Law 114-264 (December 14, 2016)

Challenge 5: Climate Initiatives Risk (Repeat)

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: (1) advance consistent, clear, intelligible, comparable, and accurate disclosure of climate-related financial risk, including both physical and transition risks;⁴³ (2) 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 (3) 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 continues to play a significant role working with other federal agencies, foreign governments, and international financial institutions to stimulate global action on addressing climate change, promoting environmental justice, and addressing climate-related risks. In 2021, Treasury created a new Climate Hub and appointed a Climate Counselor to help set the strategic direction of its efforts to address climate change and coordinate across those efforts. The Treasury Climate Hub will coordinate and enhance existing climate-related activities by engaging 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 work to ensure that Treasury is prioritizing climate action. On July 27, 2023, Treasury announced the appointment of a new Climate Counselor.

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 (DO) 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

⁴³ Physical risk refers to the harm to people and property arising from acute, climate-related disaster events such as hurricanes, wildfires, and floods as well as longer-term chronic phenomena such as higher average temperatures. Transition risk refers to stresses to certain institutions or sectors arising from the shifts in policy, consumer and business sentiment, or technologies associated with the changes necessary to limit climate change.

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 work to address climate-related risks to the financial system 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. OCC and the Federal Insurance Office are members of the international organization, the Network of Central Banks and Supervisors for Greening the Financial System (NGFS). In October 2021, FSOC issued its Report on Climate-Related Financial Risk, as mandated by EO 14030. 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 the incorporation of 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, through either the Office of Financial Research (OFR), the Federal Insurance Office, or OCC. It will be important that each recommendation be addressed not only timely, but also collectively with the other FSOC members to ensure a cohesive response.

To meet the challenges relating to the types and quality of available data and measurement tools, the OFR is developing an interagency data and analytics platform – the Joint Analysis Data Environment (JADE). Based on a pilot program, JADE will provide FSOC member agencies with access to data, analytical software, and high-performance computing tools to allow users to jointly analyze financial stability risks and vulnerabilities. With an initial version now operational, the OFR will need to continue to expand JADE to evolve and include new data and allow access to other FSOC member agencies. Furthermore, OCC has implemented multiple initiatives to address climate-related financial risk. They have partnered with other federal banking regulators to work collaboratively in understanding the risks and continue to consider the comments received on the draft Principles for Climate-Related Financial Risk Management for Large Banks. OCC also engages with international groups such as the Network of Central Banks and Supervisors for Greening the Financial System, to share best practices and understand the development of climate-related financial risk management in the financial sector. Internally, OCC's Office of Climate Risk led by a Chief Climate Risk Officer assesses climate-related financial risks and advises management on OCC policy, banking supervision, and research. These collaborations will continue to be important for 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.

Challenge 6: Operating in an Uncertain Environment (New)

In assessing the Department's most serious challenges, we remain mindful of external factors and future uncertainties that affect its operations. These factors include, but are not limited to, the repeated cycle of budget and debt ceiling stopgaps, rising interest rates, and inflation. Congress has yet to resolve unfinished business when it comes to the Nation's debt, and the long-term

sustainability of programs. Although legislation was passed to temporarily suspend the debt limit until January 1, 2025,⁴⁴ no long-term solution has been found. The impact of these challenges and their 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 programs and reforms be managed and communicated effectively to achieve performance and accountability.

Debt Limit and the Budget

The debt limit—commonly called the debt ceiling—is the total amount of money that the U.S. government is authorized to borrow to meet its existing legal obligations. The amount is set by law and has been increased or suspended over the years to allow for the additional borrowing needed to finance the government’s operations. Failing to increase or suspend the debt limit would have catastrophic economic consequences, as it would cause the government to default on its legal obligations. As experienced, even threats that the U.S. government may fail to meet its obligations have led credit agencies to downgrade the Federal Government’s credit rating in 2011 and 2023, which increases borrowing costs and hurts the long-run budget. Until lawmakers enact legislation to raise or suspend the debt limit, Treasury must use its cash balance and the available extraordinary measures—special temporary strategies to handle cash and debt management—to fund ongoing government activities. The challenges Treasury generally faces with a debt limit impasse include the disruption of its prudent cash management policy implementation, uncertainty in the Treasury debt market, communicating and managing the economic impact, and diversion of resources.

Treasury’s prudent cash balance policy is to maintain sufficient funds to cover at least the one-week-ahead cash need, including net fiscal outflows and the gross volume of maturing marketable debt. This policy is a risk-management tool to protect against potential interruptions to market access. However, because the debt limit constrains Treasury’s borrowing, it can become impossible to comply with this policy during debt limit impasses. A cash balance below the policy level creates substantial risks in the event of unexpected adverse circumstances. These risks typically worsen as a debt limit impasse goes on and the cash balance declines towards zero. For example, on June 1, 2023, Treasury had an end-of-day cash balance of just \$23 billion compared to a policy level that called for approximately \$300 billion on that day (and an average balance in 2022 of more than \$600 billion). Furthermore, once a debt limit impasse is resolved, Treasury must rapidly replenish its cash balance back towards the policy level, which can result in elevated volatility in the primary and secondary markets for bills. Also, actions to manage the amount of outstanding Treasury securities when outstanding debt is at or near the statutory limit can add uncertainty to the Treasury market. For example, during past debt limit impasses, Treasury has postponed auctions and dramatically reduced the amount of bills outstanding, which compromised the regularity of auctions and the certainty of supply, on which Treasury relies to achieve the lowest borrowing cost over time.

As debt nears the limit, managing both debt and cash require more time and Treasury resources. Treasury's operational focus on the debt limit begins as early as 6 to 9 months before the debt limit is expected to be reached and increases as debt nears the limit. In 2023, while Congress deliberated on increasing the debt limit, Fiscal Service and the Office of Fiscal Projections implemented extraordinary measures to prevent the United States from defaulting on its obligations.

⁴⁴ Public Law 118-5, (June 3, 2023)

Extraordinary measures included (1) suspending investments in the Government Securities Investments Fund of the federal employees' Thrift Savings Plan and Civil Service Retirement and Disability Fund (CSRDF), (2) redeeming certain investments held by CSRDF and Postal Service Retiree Health Benefits Fund earlier than normal, (3) suspending new issuances of State and Local Government Series securities, and (4) exchanging \$1.9 billion of Treasury securities held by the CSRDF for securities issued by the Federal Financing Bank. These activities diverted time and Treasury resources from other cash and debt management issues and impacted people ranging from senior leaders to operational staff. This diversion of staff resources increases the risk in performing daily operational activity as normal processes are delayed and fewer staff resources are available for normal operational tasks. Estimates provided by Fiscal Service and the Office of Fiscal Projections, the entities primarily affected by the delays, indicated that these entities' personnel devoted approximately 7,730 hours to managing debt near the limit when delays in raising the debt limit occurred in 2023.

The Fiscal Responsibility Act of 2023, enacted on June 3, 2023, suspends the debt limit through January 1, 2025; increases the limit on January 2, 2025, to accommodate the obligations issued during the suspension period; and sets statutory caps on defense and non-defense discretionary spending for fiscal years 2024 and 2025. Specifically, discretionary budget authority will be capped at \$1.59 trillion in 2024—a reduction of \$12 billion compared to fiscal year 2023, which provides the first cut to base discretionary spending authority in more than a decade—and \$1.61 trillion in 2025—an overall increase of 1% compared with fiscal year 2024. The legislation also includes a penalty for failure to enact regular appropriations by January 2024 in the form of one percent reductions to defense and nondefense spending levels (to take effect by April 30, 2024), which is intended to aid the budget process and deter excessive reliance on continuing resolutions; a similar penalty and timeline also apply for fiscal year 2025. Continued delays in enacting annual appropriations timely could have a negative impact on Treasury's operations. According to the DO fiscal year 2024 Congressional Budget Justification, the lack of adequate funding for inflationary increases and gradual reduction of full-time employee levels across Treasury policy offices, erodes DO's capacity to maintain support of fundamental DO mission areas. DO mission areas include maintaining the public debt, setting Treasury's strategy, and performing legal analysis on issues related to Treasury equities. Inflationary pressures lead to increased funding needs for programs and modernization efforts budgeted in prior years. Funding is needed to ensure that DO can sustain critical policy work necessary to maintain a strong economy and create economic growth and financial stability.

Rising Interest Rates and Inflation

Rising interest rates and lower bond ratings impact Treasury's costs to manage the Federal Government's finances and resources effectively. The increasing cost to service the federal debt makes these critical markets vulnerable to stresses, which could have significant consequences for economic growth and financial stability. With federal, state, and local government debt now exceeding \$30 trillion, ensuring that these markets remain resilient is a critical component of sound fiscal policy.

The rapid increase in interest rates were a contributing factor to multiple bank failures in early 2023, resulting in a period of increased market volatility that threatened U.S. financial stability. When the Federal Reserve increased interest rates throughout 2022 and into 2023, some banks did not have sufficient liquidity to satisfy their obligations. Banks often invest the money received from demand deposits and checking and savings accounts in long-term assets with the intention

that the interest rates on their long-term investments will exceed the interest rates paid to their customers resulting in a gain for the bank. However, the rapid pace of interest rate hikes resulted in many banks having to pay customers a higher interest rate while their funds were tied up in long-term investments that were paying lower interest rates. The result was some banks experienced a liquidity crisis. Because these banks did not have sufficient liquidity and access to capital, they failed. Sound banks were also adversely impacted, because the interest rate increases depreciated the value of their investment portfolios. As a result of the liquidity crisis, many banks have taken steps to strengthen their financial positions; however, they remain under pressure. Uncertainty regarding future interest rates continue to pose risk to banks. Treasury as a leading banking regulator, through OCC, must be mindful of these liquidity risks on the institutions they supervise and the broader U.S. financial system.

Appendix: Acronyms and Abbreviations

ARP	American Rescue Plan Act of 2021
BSA	Bank Secrecy Act
CAA, 2021	Consolidated Appropriations Act, 2021
CAA, 2023	Consolidated Appropriations Act, 2023
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CDFI	Community Development Financial Institutions
CIO	Chief Information Officer
COVID-19	Coronavirus Disease 2019
CPF	Coronavirus Capital Projects Fund
CRF	Coronavirus Relief Fund
CRE	Commercial Real Estate
Department	Department of the Treasury
DO	Departmental Offices
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
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 Assistance Fund
IT	Information Technology
JADE	Joint Analysis Data Environment
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
OFR	Office of Financial Research
OIG	Office of Inspector General
OMB	Office of Management and Budget
ORP	Office of Recovery Programs
PRAC	Pandemic Response Accountability Committee
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