Department of the Treasury
Departmental Offices (DO)

FY 2023

Capital Investment Plan

Note to Reviewers: Consistent with the corresponding Summary of Capital Investments table, the columns included in the investment tables below are defined as:

- **FY 2021 Actuals** -Total actual obligations
- **FY 2022 Estimated Obligations -** Anticipated obligation from all budgetary resources (i.e., balances from prior years, user fees, and FY 2022 CR levels).
- **FY 2023 President's Budget** – Requested level reflecting the President's FY 2023 budget submission

OR

- **FY 2023 Estimated Obligations**- Anticipated obligation from all budgetary resources (i.e., balances from prior years, user fees, and FY 2023 President's Budget

Major IT Investments

Cybersecurity Enhancement Account (CEA)

Description:

The Cybersecurity Enhancement Account was created in FY 2017 to fund investments in critical cybersecurity capabilities with a Department-wide impact. The CEA is positioned as a centralized account to support enterprise-wide cyber services and to further enhance cyber capabilities, providing a platform to enhance efficiency, communication, transparency, and accountability around the Treasury's mission.

Investment Obligations: (In Millions of $):

Type	FY 2021 Actual	FY 2022 Estimated Obligations	FY 2023 President's Budget	Change $	Change %
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	28.04	20.52	215.00	194.48	947.76%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	0.00	0.00	0.00	0.00	0.00%
Total Obligations	28.04	20.52	215.00	194.48	947.76%

Purpose, Accomplishments, Future Objectives:

The CEA account focuses on an enterprise-wide investment approach to build stronger protections and further benefit the bureaus in their cybersecurity goals. This approach also unifies cyber spending across the Department. The FY 2023 President's Budget includes $215 million for the CEA to protect and defend sensitive agency systems and information and strengthen the role of the Treasury Chief Information Officer (CIO) in identifying, responding, and protecting against cyber threats. The CEA initiatives are organized around the NIST Cybersecurity Framework as follows:

- Identify the Business Context, Resources & Cybersecurity Risk Goal: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- Protect the Delivery of Critical Infrastructure Services Goal: Develop and implement appropriate safeguards to ensure delivery of critical services.
- Detect Cybersecurity Events Goal: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

- Respond to Detected Cybersecurity Incidents Goal: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- Recover by Maintaining Resilience and Restoration Plans Goal: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

In FY 2021, CEA investments have bolstered the Department's cyber posture in the following ways:

- Conducted enterprise-wide assessments and threat analysis to support the post-incident response efforts to address and mitigate impacts of the SolarWinds cybersecurity incident.
- Conducted 11 HVA SARs/RVA assessments outside of the DHS process.
- Increased system security monitoring capabilities.
- Developed operating capabilities to centrally manage encryption keys.
- Furthered efforts implementing the Risk Management Framework (RMF) automation tool.

In FY 2022 and FY 2023, CEA investments will focus on accomplishing the following goals:

- Enhance Department-wide coordination of cybersecurity efforts and improve responsiveness to threats.
- Provide leadership with greater visibility into cybersecurity efforts and encourage information sharing.
- Improve identification of cyber threats and better protect information systems from attack.
- Provide platform to enhance communication, collaboration, and transparency.

Investments made from CEA will help to accomplish several goals, including:

- Enhance Department-wide coordination of cybersecurity efforts and improve responsiveness to threats.
- Provide leadership with greater visibility into cybersecurity efforts and encourage information sharing.
- Improve identification of cyber threats and better protect information systems from attack.
- Provide platform to enhance communication, collaboration, and transparency.

HR LoB - HRConnect

Description:

HR Connect is a Human Resources enterprise system. It is a web-based solution built on PeopleSoft software. HR Connect transforms core back-office HR functions, moving them from a processing-centric capability to a strategic-centric capability.

Investment Obligations: (In Millions of $):

Type	FY 2021 Actual	FY 2022 Estimated Obligations	FY 2023 President's Budget	Change $	Change %
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	1.21	0.81	0.81	0.00	0.00%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	34.43	35.85	34.77	-1.09	-3.03%
Total Obligations	35.64	36.67	35.58	-1.09	-2.96%

Purpose, Accomplishments, Future Objectives:

HRConnect is Treasury's enterprise human resources system. It is one of four federal OPM HR Lines of Business providing HR services to the federal government. HRConnect is based on a combination of (a) web-based solution built on PeopleSoft commercial-off-the-shelf (COTS) software, (b) Software as a Service (Saas) platforms (e.g. Talent Management and Career Connector) and (c) internally developed applications (e.g. Entrance on Duty System). HRConnect transforms core back-office HR functions, moving them from a processing-centric capability to a strategic-centric capability enabled through its commercial software underpinning. Additionally, self-service components of the software fundamentally transform the standard government HR service delivery model, putting additional information, services and processes (i.e., personal data, position management, requests for personnel action, recruitment, reporting, etc.) directly in the hands of managers and employees.

HRConnect supports the common HR Line of Business processes and provides core HR functionality that is interoperable, portable and scalable. This shared solution provides automated systems that are configurable to the individual organizations' needs while providing a single solution across the Department and federal landscape. HRConnect's core functions include: Personnel Action Processing, Managing Payroll, Administering Benefits, Time and Attendance and Labor Distribution. By enabling the retirement of legacy systems and automating and streamlining many aspects of human resources, HRConnect facilitates increased efficiency and overall productivity for its customers. HRConnect is the system used by all Treasury bureaus and several other government agencies (over 22 entities) with over 200,000 employees and contractors in total.

In FY 2021, the Treasury Shared Service Center implemented 42 change requests focusing on usability and customer experience to include additional functionality that support the HR Specialists as well as improving the look and feel of the application In Q1, the team upgraded the application to bring it current with the PeopleSoft Update Manager images and Tools. The latest functionality allows to incrementally make changes to the application: new tiles on the home page, new classic plus look on the employee self-service, tracking outside employment for IRS, redesign of the Team views, updates to the worklists, implementing Position Budget Management for Census. The team has also completed the USA Staffing integration and DOC web services integration. In addition, quickly responded to the emerging vaccination tracking requirements utilizing the delivered PeopleSoft tables to implement the functionality; over 90% of Treasury personnel logged in and entered their information. A few of technical improvements, included: Nessus implementation, CAST implementation, piloted the transition of 3 environments to Oracle Managed Services compartment in Q3, improved the fire wall configurations and finalized the closure of the Memphis and Martinsburg HRC footprints.

Treasury Enterprise Identity, Credential and Access Management (TEICAM)

Description:

The Treasury Enterprise Identity, Credential and Access Management (TEICAM), formerly submitted as EIdM, consolidates funding of Treasury implementing the Homeland Security Presidential Directive- (HSPD) 12, E-Auth, and Federal PKI initiatives.

Investment Obligations: (In Millions of $):

Type	FY 2021 Actual	FY 2022 Estimated Obligations	FY 2023 President's Budget	Change $	Change %
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	31.37	70.59	70.51	-0.08	-0.11%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	27.90	16.89	17.02	0.13	0.75%
Total Obligations	59.27	87.48	87.53	0.05	0.05%

Purpose, Accomplishments, Future Objectives:

The TEICAM Business Case consolidates funding that supports Treasury's implementation of HSPD-12, FICAM and PKI requirements. Supporting the target vision: "One Treasury One Card" to provide universal access. Availability and use of a PIV/identity management standard within Treasury provides a mechanism for Physical and Logical access to Treasury-wide assets. The TEICAM phased implementation provides all of Treasury:

- Trusted identity processes for both Federal and public users of Treasury applications
- Enhanced security (by decreasing data breaches and trust violations)
- Compliance with laws, regulations, standards
- Improved interoperability
- Expanded use of PIV encryption and digital signature certificates (ensuring adoption of multi-factor authentication)

Treasury/TEICAM has achieved many of the defined goals for PIV card issuance, physical and logical access, data synchronization, enterprise single sign-on, federation, and PIV required for privileged and unprivileged users. These goals have helped the Department align with the required OMB and FICAM goals. TEICAM has updated the Department strategic roadmap & planned for the following investment goals:

1. CDM II Management: Implementation of Credential (CRED) and Privileged Access Management (PAM); On-board new bureaus (IRS, DO Orbit programs, etc) to the CDM Managed Service Offering (MSO); Continue working with DHS CISA on integration activities for the Federal Dashboard for Treasury's CDM Data reporting
2. Expand usage of Enterprise Derived Credential capability to support authentication to Treasury infrastructure from mobile devices across Treasury through FY 2023
3. PIV-I solution: Implement an application programming interface (API) connection between a Fiscal Service application used to capture applicant data and HRConnect through FY 2023
4. Implement an enterprise Hardware Security Module (HSM) as a service through FY 2023

5. Enterprise solution to track and monitor Only Locally Trusted (OLT) PKI certificates generated and in use at each bureau
6. Plan, design, and implement a modernized Treasury Enterprise Federation Service (TEFS) solution that enforces multifactor authentication and aligns with the Treasury Zero Trust Architecture (ZTA) Treasury utilizes interagency resources to authenticate users, synchronize data, and to procure enterprise-wide compliant PIV credentials (USAccess).
7. Plan, test, & implement version 8.1 PIV cards across the enterprise through FY 2024

Planned objectives and accomplishments include:

- Maintaining above 95% PIV card issuance rate and providing replacements for the PIV in time sensitive activities;
- Maintained 100% PIV required privileged account access and 97% PIV required unprivileged access;
- CDM II privileged access management is operating with a cloud infrastructure and production at four bureaus performing O&M functions; we have commenced technical work on bringing the IRS on as the fifth and largest managed service customer;
- Treasury Enterprise Federation Service (TEFS) onboarded 12 new customers and integrated with third-party identity providers to expand citizen services and access;
- Executed a Treasury-wide BPA for citizen authentication services access to the entire enterprise, allowing for secure and fast public access to Treasury systems;
- Developed an alternative authentication solution and deployed it within 6 weeks to ensure continuity of government during the pandemic;
- Implemented a hardware security module (HSM) as a service for the Derived PIV solution and DO.
- Implementation of the department-wide PKI Only Locally Trusted (OLT) monitoring solution.

Treasury Government Security Operations Center (GSOC)

Description:

Government Security Operations Center. GSOC is the agency’s top-level Security Operations Center (SOC) whose mission is to serve as the focal point for management of Department wide cyber incidents and is responsible for security detection, analysis, and incident management lifecycle practices to improve the Department’s overall security posture. GSOC ensures adherence to Departmental and federal security standards; and improves cyber threat awareness and responsiveness across Treasury Bureau customers. GSOC is federally mandated to run and report on cyber threats 24x7x365.

Investment Obligations: (In Millions of $):

Type	FY 2021 Actual	FY 2022 Estimated Obligation	FY 2023 President's Budget	Change $	Change %
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	0.00	5.39	2.46	-2.93	-54.28%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	16.41	17.08	17.68	0.60	3.54%
Total Obligations	16.41	22.47	20.15	-2.32	-10.33%

Purpose, Accomplishments, Future Objectives:

Investments have contributed to Treasury's success in defending against cyber adversaries and provides leadership and direction in mitigating threats to Treasury systems and services. Future objectives include: collecting and storing data from all bureaus to meet M-21-31 objectives, expanding TSSSOC to offer additional security operations and incident response services to bureaus, and improving communication and collaboration throughout the Department through automation.

Major Non-IT Investments

DO Electric Vehicle Fleet

Description:

In the FY 2022 Budget request, Treasury requested funding for EVs in individual bureau accounts. However, Treasury requested $5 million in FY 2023 in the Department-wide Systems and Capital Investments Program (DSCIP) account for leasing of EVs and purchasing associated charging and supply equipment. Funding will be used for the replacement of traditional internal combustion vehicle leases with zero-emission vehicles across the Department. Where possible, electric vehicles will replace traditionally powered leased vehicles as well. Additional charging station infrastructure will be installed to support fleet electrification. Some existing charging stations will require updates or replacement.

Investment Obligations: (In Millions of $):

Type	FY 2021 Actual	FY 2022 Estimated Obligations*	FY 2023 President's Budget	Change $	Change %
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	0.00	0.00	5.00	5.00	0.00%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	0.00	0.00	0.00	0.00	0.00%
Total Obligations	0.00	0.00	5.00	5.00	0.00%

*Note, FY 2022 Estimated Obligations shown only covers the Departmental Salaries and Expenses obligations for electric vehicles. Other bureaus may dedicate funding for electric vehicles in FY2022.

Purpose, Accomplishments, Future Objectives:

Treasury is committed to supporting the Administration's goals of combatting the impacts of climate change and achieving 100 percent zero emission vehicle acquisition by 2035. The Department of the Treasury is accelerating the conversion of its vehicle fleet to electric vehicles (EVs) as a part of strategic objective 4.4 (Sustainable Treasury Operations). Electrifying the Treasury fleet will support environmental and energy sustainability and will make Treasury more adaptive and resilient to the impacts of climate change.

For FY 2023, Treasury is treating EV investments as a corporate asset through the DSCIP account. Should any funding be provided in FY 2023 appropriations, the Department will develop an allocation plan and transfer funds to bureaus. For FY 2022, no funding was approved for EV infrastructure. In support of the Agency Priority Goals (APG) effort, Treasury is working to make sure that reviews are conducted for every lease renewal. Should there be an opportunity to convert the lease to an EV, Treasury will determine the associated infrastructure costs. Overall targets were reassessed to determine what is possible for the APG but the goal of making progress (e.g., converting to EV leases, providing infrastructure) in support of the Administration's priority here is still the plan.

Main Treasury Building and Freedman's Bank Building

Description:

Correct life safety and code issues, reduce building systems risk, and maintain the buildings. Absent full funding to perform a complete repair and renovation, Treasury is utilizing available funding to correct the most severe issues.

Investment Obligations: (In Millions of $):

Type	FY 2021 Actual	FY 2022 Estimated Obligations	FY 2023 President's Budget	Change $	Change %
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	8.88	9.65	6.12	-3.53	-36.60%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	0.00	0.00	0.00	0.00	0.00%
Total Obligations	8.88	9.65	6.12	-3.53	-36.60%

Purpose, Accomplishments, Future Objectives:

This investment is to address life safety and code compliance issues, reduce building systems risk by upgrading a number of outdated systems, and bring both facilities into alignment with current building standards. Absent full funding to perform a complete repair and renovation of these historical buildings, available funding will be used to correct the most urgent issues. These investments are being executed with the expectation that were Treasury to pursue a full renovation and modernization, recent investments could be largely retained, achieving cost savings over the long term. These investments support a safe and healthy work environment that meets Treasury operational requirements. Project needs are mission focused and prioritized based on life-safety, security, code discrepancies, and needs that pose significant financial risk if not addressed in a timely manner.

Treasury Operations has continued to strategically focus on restoring the health of the building envelope (shell) to correct the deteriorating building structure and infrastructure. Components of the Main Treasury (MT)F building that have been repaired, replaced, or funded include new roofs (FY 2019/2021) and repairs to 40 percent of the windows (FY 2015/2017). The Freedman's Bank Building (FBB) components that have been repaired, replaced, or funded/planned include new roofs (FY 2017/2019), domestic water line (FY 2020/2022), and replacement of all windows (FY 2009/2011). Funding and completion of these exterior items represent significant progress towards the preservation of the two buildings, maintaining a safe and healthy workplace, and reducing damage to the interior plaster and paint. The contract for the first phase of the Main Treasury exterior restoration was awarded late in FY 2021. Completion of the first phase is expected (restoration of the west façade) during FY 2022. A water line leak led to a partial failure of an interior basement wall in the FBB. In January 2022 a Victaulic coupling failed on a water pipe in the MT and flooded the fifth floor and all the floors below it, compromising workstations, walls, ceilings, and carpeting. Situations like these make it difficult for Treasury to support its staff within Treasury DO. The Facility Condition Assessment (FCA) will provide estimates on the remaining life and dependability of operating systems allowing for the development of more robust preventive maintenance plans. driving better, safer, and more inclusive experiences for Treasury staff.