Department of the Treasury
Departmental Offices

FY 2022

Capital Investment Plan

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.

Investment Obligations: (In Millions of $):

Type	FY 2020 Actual Obligations	FY 2021 Estimated Obligations	FY 2022 President's Budget*	$ Change	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	29.19	38.71	77.79	39.08	100.98%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	0.00	0.00	0.00	0.00	0.00%
Total Obligations	29.19	38.71	77.79	39.08	100.98%

**Amounts in the table represent past, current and anticipated CEA obligations; the FY 2022 President's Budget provided CEA with $132M in multi-year budget authority through FY 2024.*

Purpose, Accomplishments, Future Objectives:

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; and,
- Provide platform to enhance communication, collaboration, and transparency. Through CEA investments in FYs 2020 and 2021 Treasury:
- 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 the FY 2022 President's Budget, CEA initiatives are organized around the NIST Cybersecurity Framework. Future objectives for the FY 2022 CEA funding include:
- 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.
- Detected 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.
- NIST Cross-Functional Investments: There are several investments within the CEA that are allocated across multiple NIST framework categories for improving critical infrastructure cybersecurity. The investments are Post-Incident Response, Treasury Shared Services Secure Operations Center (TSSSOC) and Threat Hunting, Treasury-wide Log Collection, Management and Certificate Security for Identification Management.

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 2020 Actual Obligations	FY 2021 Estimated Obligations	FY 2022 President's Budget	$ Change	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	1.85	1.00	0.01	-0.99	-99.00%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	33.48	34.05	31.00	-3.05	-8.95%
Total Obligations	35.33	35.05	31.01	-4.04	-11.53%

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.

The Treasury Shared Service Center (TSSC) will continue to scale and expand HRConnect products and services to new federal agencies. In FY 2019, the Treasury Shared Service Center improved its day-to-day functionality and completed the following projects: (a) Single Sign On for HRConnect In FY 2020 and beyond TSSC will deploy new customers as they emerge and will continue to provide capabilities to enable its customers' missions. This includes migrating the HRConnect system from data centers to the Treasury Secured Cloud environment.

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 2020 Actual Obligations	FY 2021 Estimated Obligations	FY 2022 President's Budget	$ Change	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	37.37	31.37	31.37	0.00	0.00%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	28.31	27.90	27.93	0.04	0.13%
Total Obligations	65.68	59.27	59.30	0.04	0.06%

Purpose, Accomplishments, Future Objectives:

The Treasury Enterprise Identity, Credential and Access Management (TEICAM) Business Case consolidates funding that supports Treasury's implementation of Homeland Security Presidential Directive (HSPD)-12, Federal Enterprise Identity Credential and Access Management (FICAM) and Public Key Infrastructure (PKI) requirements. This investment supports the target vision of, "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 internally and within the federal space; -increased security (by decreasing data breaches and trust violations); -compliance with laws, regulations and standards; -improved interoperability; -elimination of redundancy. Treasury/TEICAM has achieved many of the defined goals for PIV card issuance, physical access, logical access, data synchronization, enterprise single sign-on, federation, and PIV required for both privileged and unprivileged users. These goals have helped the Department align with the required OMB and FICAM goals. Additionally, TEICAM has updated the Department strategic roadmap & planned for the following investment goals:

1) Coordinate & extend the use of the physical access Visitor Management System (VMS) in FY18-FY19.
2) Plan, design, & implement a Treasury-wide PIV credentialing station replacement in FY18-FY19.
3) Plan, design and implement an Enterprise Derived Credential issuance capability to support authentication to Treasury services/infrastructure from mobile devices across Treasury in FY18-FY19.
4) Plan and design an Enterprise Identity Management System approach to support provisioning and de-provisioning needs across Treasury.

In an effort to improve cost-savings, the Department utilizes interagency resources to authenticate users, synchronize data, and to procure and maintain enterprise-wide compliant PIV credentials (USAccess). As a mixed life-cycle investment, the TEICAM Operations and Maintenance tasks includes OMB, FISMA, and Cyber reporting specific to identity, credential, and access management.

Planned objectives and accomplishments include:

- Maintaining above 95% card issuance rate and providing replacements (local printing and Temporary card) for the PIV in time sensitive activities.
- PACS progress to meet PACS rollout goals;
- Treasury has maintained 100% PIV required privileged account access and 92% PIV required unprivileged access.
- The Treasury Enterprise SSO infrastructure was completed with six Treasury Enterprise applications integrated by the end of FY17.
- Implemented a Treasury-wide PKI encryption Key Recovery and Migration approach.
- Integrated Federation with external partners DOL, USAID, and CFPB to allow use of Treasury applications and SSO.
- Deploying a derived credential solution and visitor management system.

Treasury IT Infrastructure Telecommunications (TNET)

Description:

Treasury TSS supports Treasury's mission and its programs by maintaining a cohesive enterprise network architecture that fosters secure, reliable, trusted, and cost-effective data, internet, voice and video communications, supporting all Treasury Bureaus.

Investment Obligations: (In Millions of $):

Type	FY 2020 Actual Obligations	FY 2021 Estimated Obligations	FY 2022 President's Budget	$ Change	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	0.00	0.00	0.00	0.00	0.00%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	140.66	148.74	138.02	-10.72	-7.21%
Total Obligations	140.66	148.74	138.02	-10.72	-7.21%

Purpose, Accomplishments, Future Objectives:

The Treasury Network (TNet) provides a secure enterprise voice, video, and data wide area network that connects authorized domestic and international government facilities across the US, the US territories, and at select US Embassies via the State Department's network. The TNet Wide Area Network (WAN) service is a cost effective enterprise network supporting Bureau business needs and enabling Agency technological initiatives, such as Data Center Consolidation and Mobile Treasury.

- A common architecture and security baseline for enterprise services and IT security controls;
- A shared interchange point through DHS Trusted Internet Connection Access Point (TICAP) between Bureaus and the public Internet;
- An agency wide multiple protocol labeling standard (MPLS) virtual private network (VPN) with Dynamic Multipoint Virtual private network(DMVPN) overlay
- A variety of private line, managed internet, managed trusted internet and other non MPLS telecommunication related services obtained under the TNET task order of the GSA Networks contract
- A 24x7 Help Desk support and a common set of Service Level Agreements (SLA);
- Oversight and governance of Treasury telecommunications program management and engineering services; and,
- Ensure telecommunications policy and compliance in accordance with Treasury, DHS and OMB mandates. The TNet PMO also provides Telecommunications policy, oversight and leads compliance for telecommunications related issues overall, for the Department.

Examples of this include policy, implementation, oversight, and compliance for OMB M-08-05 "Implementation of Trusted Internet Connections", OMB M-08-23 "Securing the Federal Government's Domain Name System Infrastructure", OMB M-11-24 "Implementing Executive Order 13571 on Streamlining Service Delivery and Improving Customer Service", and similar Executive Office, OMB and Federal CIO guidance and oversight. Starting with FY2018, the previous Treasury Enterprise Voice (TEV) program is being consolidated into the existing TNet program. TEV is responsible for providing converged and traditional telephony for participating Agencies and Treasury bureaus. By converging voice, video, and data onto the same network platform, Treasury realizes efficiencies in both capital investment and operating expense. With the two previous programs combined into a single program, additional scale and efficiencies can be achieved.

Consolidated infrastructure and network traffic within data center facilities to optimize performance of all devices for Treasury bureaus.