Department of the Treasury
Departmental Offices

FY 2020

Capital Investment Plan

Table of Contents

The Office of Management and Budget (OMB) Capital Planning Guidance changed how certain IT Investments are categorized. The Agency IT portfolio summary consists of Part 1: IT Investments for Mission Delivery; Part 2: IT investment for Administrative Services and Support Systems, and Part 3: IT Investments for IT infrastructure, IT Security, and IT Management (so called "standard investments"). The guidance no longer requires Part 3 investments to be reported as major or non-major investments. However, the Department of the Treasury's Capital Investment Plan will continue to report these investments.

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

- *FY 2018: Actual obligations of budgetary resources including annual funding, prior year balances, user fees, and other sources;*
- *FY 2019: Estimated obligations based on the Annualized Continuing Resolution funding level assumed for the FY 2020 President's Budget. Figures include annual funding, prior year balances, user fees, and other sources; and*
- *FY 2020: Estimated obligations based on the funding requested in the FY 2020 President's Budget. Figures include annual funding, prior year balances, user fees, and other sources. The amount of new budget authority requested for a given investment can be found in the Summary of Capital Investments table (see "FY 2020 Budget Authority Request" column).*

Treasury is committed to working with partners to further improve capital investment reporting and performance management. As a result, plan formatting may continue to evolve. Additional information about Treasury's capital investments is available at the link below.

https://itdashboard.gov/drupal/summary/015

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 2018	FY 2019	FY 2020	Change in $	% Change
Cyber Enhancements (Including Internal labor (Govt. FTE))	0.70	0.76	1.54	0.78	-102.63%
Data Loss Prevention (DLP) Analytics (Including Internal Labor (Govt. FTE))	3.60	4.09	1.79	-2.3	-56.24%
Encrypted Traffic Inspections and DLP at Fiscal Service TICs (Including Internal Labor (Govt. FTE))	0.38	0.13	0.31	0.18	138.46%
Enhanced Incident Response and Recovery Capabilities (Including Internal Labor (Govt. FTE))	1.58	2.87	5.99	3.12	108.71%
Enhancements to Cybersecurity Infrastructure (Including Internal Labor (Govt. FTE))	0.60	6.21	4.60	-1.61	-25.93%
High Impact Initiatives (Including Internal Labor (Govt. FTE))	4.90	7.99	0.47	-7.52	-94.12%

Type	FY 2018	FY 2019	FY 2020	Change in $	% Change
Improving High Value Asset (HVA) Cybersecurity (Including Internal Labor (Govt. FTE))	3.10	3.91	2.42	-1.49	-38.11%
Malware Content Filter (Including Internal Labor (Govt. FTE))	0.29	0.49	1.24	0.75	153.06%
Mitigation of Cyber Threats to US Financial Sector (Including Internal Labor (Govt. FTE))	1.58	0.32	0.79	0.47	146.88%
Proactive Cyber Risk and Threat Identification (Including Internal Labor (Govt. FTE))	1.37	1.62	2.63	1.01	62.35%
TSDN System Upgrades and Security Enhancements (Including Internal Labor (Govt. FTE))	6.40	2.89	1.59	-1.3	-44.98%
Administrative Fee	1.91	1.98	0.92	-1.06	-53.54%
Total Obligations	26.41	33.26	24.29	-8.97	-26.97%

Purpose, Accomplishments, Future Objectives:

Investments made from the Department of the Treasury's Cybersecurity Enhancement Account (CEA) will help to accomplish several goals, including:

- Enhance Department-wide coordination of cybersecurity efforts and improve the Department's responsiveness to cybersecurity threats;
- Provide bureau and agency leadership with greater visibility into cybersecurity efforts and further encourage information sharing across bureaus;
- Improve the identification of cyber threats and better protect information systems from attack; and,
- Provide a platform to enhance efficient communication, collaboration, and transparency around the common goal of improving the cybersecurity of Treasury systems.

Through CEA investments in FYs 2018 and 2019 Treasury:

- Identified initial solution candidate list for the IRS Strong Authentication project and performed scoring, utilizing previously-developed suitability criteria.
- Developed the Solutions and Architecture Concepts for the IRS Malware Sandboxing project.
- Conducted 3 HVA SARs and 1 HVA RVA, receiving the EFTPS SAR report with 4 standard findings and NO critical findings to report.
- Increased system security monitoring capabilities via implementation of system monitoring, logging and event management.
- Completed initialization and standard configuration of the new infrastructure with reduced vulnerabilities.
- Began development of risk dashboard for risk and/or threat identification, finalizing the requirement traceability matrix (RTM) for the Enclave Inventory Management (EIM) and System Detection, Analysis, and Risk Reporting (S- DARR).
- Completed mail inspection – email detonation with malware detection deployment and testing.
- Developed and established process and procedures for use of technology for Cyber Security Operations.

Future objectives for the FY 2020 CEA funding include:

- *Improving the High Value Asset (HVA) Cybersecurity:* The HVA Cybersecurity initiative builds on the prior investments to secure Treasury's top tier HVAs and data at rest encryption solutions for payment platforms, tax processing systems, and collection processing systems, as well as enhanced user authentication for these systems. It will deliver enhanced data assurance capabilities, minimizing accessibility of highly sensitive data in the event of compromises to multi-layered defenses and storage solutions.

- *Proactive Cyber Risk & Threat Identification:* This initiative significantly improves network visibility, threat identification, incident response time, data aggregation, and data management by Treasury's enterprise cybersecurity operations center (SOC). It provides high definition monitoring of IT assets and activities, and detailed visibility across the enterprise and into bureau networks and will result in faster detection, response, and recovery time in the event of an advanced persistent threat attack, other malicious activities, or negligent acts.
- *Cybersecurity Enhancements:* This request improves cyber security situational awareness through the implementation of processes and automated tools that support cyber information sharing department-wide and eliminates organizational stovepipes that negatively impact the Department's cyber security posture. Enhanced situational awareness will provide Department-wide awareness of breaches and attack information. It will increase the effectiveness of cyber security functions and achieve efficiencies through the elimination of redundant efforts.
- *Enhanced Incident Response & Recovery Capability:* This initiative improves the Department's ability to identify, respond to, and recover from cyber threats through the implementation of solutions that support early detection and avoidance of currently unknown threats. Activities include retroactive examination of network traffic; assessment of adversarial movement; determination of information compromise; implementation of mitigations and countermeasures; and reconstitution. The initiative will reduce the risk of incident occurrence, minimize their impact, and decrease recovery time.
- *Enhancements to Cybersecurity Infrastructure:* This initiative will enhance encryption, enterprise-wide identity management, and network monitoring and scanning. It is critical to the Department's cyber posture due to the increases in volume, sophistication, frequency, impact, and brazenness of global Cyber threats and recent privacy breaches (including financial institutions). It results in higher level of assurance for data integrity and access management.

Department-wide Cybersecurity Program

Description:

Provides leadership of Treasury-wide Cyber-security initiatives. Provides shared network defense and incident response capabilities.

Investment Obligations: (In Millions of $):

Type	FY 2018	FY 2019	FY 2020	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	0.56	0.86	1.31	0.45	52.95%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	9.97	21.64	31.17	9.53	44.06%
Total Obligations	10.53	22.49	32.48	9.99	44.40%

Purpose, Accomplishments, Future Objectives:

The Department-wide Cybersecurity Program provides leadership and oversight for the offices and bureaus across Treasury in all aspects of cybersecurity. The program is responsible for ensuring implementation of the Federal Information Security Modernization Act (FISMA) of 2014 as well as other federal laws and guidance related to cybersecurity. The program also provides central coordination and reporting on cybersecurity metrics and programs to external agencies, and set Treasury cybersecurity policy. The Department-wide Cybersecurity program also provide departmental situational awareness of cybersecurity incidents and coordinates response to intrusion activity. The program also serves as the lead in implementing the Treasury Cybersecurity Strategy.

In FY 2018 this investment successfully led to achieving the highest possible overall rating, “Managing Risk,” on the Office of Management and Budget’s Cybersecurity Risk Management Assessment scorecard. The investment has contributed to Treasury's success in defending against cyber adversaries, and provides leadership and direction in closing high-impact vulnerabilities such as the Heartbleed vulnerability. In the future the program seeks to bolster shared network defenses and response capabilities, and validate the protections surrounding High Value Assets across the Department.

CFIUS Case Management System

Description:

The Committee on Foreign Investment in the United States (CFIUS) Case Management System is an end-to-end IT infrastructure comprised of a public-facing portal and a case management system for use by member agencies in conducting investigations.

Investment Obligations: (In Millions of $):

Type	FY 2018	FY 2019	FY 2020	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	0.00	0.00	13.00	13.00	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	13.00	13.00	0.00%

Purpose, Accomplishments, Future Objectives:

This investment will fund development of an end-to-end IT infrastructure comprised of a public-facing portal and a case management system to modernize processes and to handle anticipated increasing caseloads for CFIUS member agencies that will promote efficiencies in the Committee's processes. This will include the ability to work in both classified and unclassified environments, meeting FedRAMP high certification requirements. The FY 2020 investment will be the initial set up of the system. In the future CFIUS member agencies will link to the system, allowing for streamlined investigations and conduct of Committee business.

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 2018	FY 2019	FY 2020	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	1.31	1.10	1.15	0.06	5.05%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	41.80	35.69	37.49	1.80	5.05%
Total Obligations	43.12	36.79	38.65	1.86	5.05%

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 2018, the Treasury Shared Service Center improved its day-to-day functionality and completed the following projects: (a) EODS Enhancements, (b) EODS Forms for OCC, (c) Unified Ticketing System. In FY 2019 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 2018	FY 2019	FY 2020	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	38.78	25.61	22.43	-3.18	-12.41%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	26.44	26.39	27.66	1.27	4.81%
Total Obligations	65.22	52.00	50.09	-1.91	-3.67%

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; and,
- 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 2018	FY 2019	FY 2020	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	3.27	0.25	0.25	0.00	0.58%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	77.91	77.90	78.35	0.45	0.58%
Total Obligations	81.18	78.15	78.60	0.45	0.58%

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.

Office of Terrorism and Financial Intelligence IT Investments

Description:

The Office of Terrorism and Financial Intelligence (TFI) relies on a number of information technology systems that help Treasury enhance national security. Treasury Financial Intelligence Network (TFIN) Treasury’s Top Secret/SCI platform. TFIN enables mission-critical work, such as Anti-Money Laundering/Counter Financing of Terrorism and counter intelligence. The Office of Foreign Asset Control’s (OFAC) Administrative System for Investigations and Sanctions (OASIS) is used to prepare the Terrorist Assets Report and enforce sanctions.

Investment Obligations: (In Millions of $):

Type	FY 2018	FY 2019	FY 2020	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	0.00	0.00	3.12	3.12	0.00%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	7.05	6.89	13.89	7.00	101.6%
Total Obligations	7.05	6.89	17.01	10.12	146.88%

Purpose, Accomplishments, Future Objectives:

Investments in IT will improve TFI's ability to keep sensitive information safe while increasing defenses against unauthorized users, improving office efficiency, reducing friction between financial institutions and the office while improving TFI's overall analytic capacity. These upgrades are needed to accomplish Treasury's Strategic goals and objectives. Without upgrades to secure networks and multi-layered defenses, Treasury would be vulnerable to attacks. Investments include:

- TFIN Network Defense upgrades that will enhance TFI's ability to monitor the classified networks against cyber threats by incorporating more comprehensive and integrated risk and threat management;
- Increased bandwidth within existing infrastructure to support and build a more robust capability for collaborative data discovery initiative;
- Multi-factor authentication to create a layered defense and make it more difficult for unauthorized individuals to access a target such as a physical location, computing device, network, or database;
- Cross Domain - One Way Transfer provides secure transfer of data between the unclassified domain and that of a high security level;
- Expand User Activity Monitoring (UAM) to the unclassified Treasury networks as exfiltration of sensitive information is most likely to occur on an unclassified network; and,
- OFAC IT Infrastructure upgrades to OASIS and TAR reporting, to include secure online communications tools for secure bi-directional transfers with financial institutions, enhancements to the OASIS case management system, and increased data analytics functionality to the wider TFI investigative datasets.

Major Non-IT Investments

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 2018	FY 2019	FY 2020	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	4.26	4.00	4.00	0.00	0.00%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	0.00	0.00	0.00	0.00	0.00%
Total Obligations	4.26	4.00	4.00	0.00	0.00%

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.

With FY 2018 funding, Treasury is initiating the first phase of replacing the failing Main Treasury roof, correcting code issues with an egress stair in the Freedman's Bank Building (FBB), advancing the new electrical service in the FBB, and finalizing the correction of code deficiencies in the FBB restrooms. The FY 2019 funding will be utilized to continue the Main Treasury roof replacement and initiative the exterior repairs and restoration to the FBB. If all requested funding is received for FY 2020, investments will be made to complete the FBB exterior repairs and restoration, replace a failing water main to the FBB, continue the Main Treasury roof replacement, and initiate modernizing the heating/ventilation/air-conditioning (HVAC) system controls. When completed, these noted investments will obtain the following objectives:

- Correct code violations with the egress stairs and restrooms in the FBB;
- Provide a weather tight roof for Main Treasury that will stop ongoing interior water damage and permit interior plaster and paint repairs to occur;
- Eliminate the current risk of the FBB losing its only domestic water supply by providing a new main feed. The current feed is failing and believed to be original to the circa 1918 structure;
- Initiate the exterior repair and restoration of the FBB. This will be the first comprehensive repair and restoration in the building's 100-year history and will repair open masonry joints that allow water infiltration and energy loss;
- Extend the distribution of the new electrical service within the FBB that will permit full use of the new power service which is more efficient and cost effective; and,
- Initiate the modernization of the HVAC system controls which will result in less energy consumption and reduced utility costs.