Department of the Treasury
Departmental Offices

FY 2021 Capital Investment Plan

Table of Contents

Note to Reviewers

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 2019: Actual obligations of budgetary resources, which may include annual funding, prior year balances, user fees, and other sources;
- FY 2020: Estimated obligations based on the enacted funding level for FY 2020 as reflected in the FY 2021 President's Budget. Figures may include annual funding, prior year balances, user fees, and other sources; and
- FY 2021: Estimated obligations based on the funding requested in the FY 2021 President's Budget. Figures may 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 accompanying "Summary of Capital Investments" table (see "FY 2021 Budget Authority Request" column).

Additional information about Treasury's IT capital investments is available at the link below:

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

Major IT Investments

Committee on Foreign Investment in the United States (CFIUS) Case Management System

Description:

The 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.

Investment Obligations: (In Millions of $):

Type	FY 2019 Actual	FY2020 Enacted	FY2021 President's Budget	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	0.00	9.11	7.30	-1.82	-19.92%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	0.00	0.00	0.00	0.00	0.00%
Total Obligations	0.00	9.11	7.30	-1.82	-19.92%

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 and launch of the system, with ongoing development funded in FY 2021. In the future CFIUS member agencies will be able to customize modules for their unique needs, allowing for streamlined investigations and conduct of Committee business.

Cybersecurity Enhancement Account

Description:

The Cybersecurity Enhancement Account (CEA) was created in FY 2017 to fund investments in critical cybersecurity capabilities with a Department-wide impact.

Investment Obligations: (In Millions of $):

Type	FY 2019	FY2020	FY2021	Change in $	% Change
Identify (Including Internal labor (Govt. FTE))	8.24	8.54	4.84	-3.70	-43.33%
Protect (Including Internal labor (Govt. FTE))	7.46	7.49	7.58	0.09	1.20%
Detect (Including Internal labor (Govt. FTE))	8.54	6.96	2.94	-4.02	-57.76%
Respond (Including Internal labor (Govt. FTE))	5.60	1.43	0.88	-0.55	-38.46%
Recover (Including Internal labor (Govt. FTE))	2.76	0.95	1.13	0.18	18.95%
Total Obligations	32.60	25.37	17.37	-8.00	-31.53%

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 2019 and 2020 Treasury:

- Instituted Department-wide Treasury Risk and Vulnerability (RVA)/ Suspicious Activity Report (SAR) reporting requirements and processes for High Value Assets (HVA) in line with OMB M-19-03 and DHS BOD 18-02.
- Created a Department-wide HVA RVA/SAR Risk Remediation Plan to track cyber risk mitigation for HVAs across the Department. Completed a final RVA Readiness Plan and distributed it to select bureaus and completed a draft SAR Readiness Plan.
- Conducted 6 RVA and 5 SAR assessments for HVAs. As a result, 10 high findings and 2 critical findings were closed in FY 19.
- Established a Request For Service (RFS) to stand up Discretionary HVA Assessments through Third-Party partner.
- Established requirements for the Enclave Inventory Management (EIM) and the System Detection, Analysis, and Risk Reporting (S-DARR).
- Closed out the Cybersecurity Analysis and Reporting Dashboard (CARD) system improvement development project on September 4, 2019, and the application transitioned to O&M.
- Closed out the Internal Revenue Service (IRS) Data-At-Rest-Encryption (DARE) project. The DARE project has continued under IRS funding as a part of the IRS Business Modernization plan.
- Closed out the Fiscal Service (IRS) Data-At-Rest-Encryption (DARE) as test equipment is now operational in Memphis with it being powered, networked, and configured in preparation for the testing phase.
- Implemented key SailPoint use cases into the IRS POC environment to validate design decisions and evaluate limited use-cases while awaiting stand up of development environment in Treasury GovCloud.
- Provisioned the CDM Development environment with High and Moderate (GovCloud) Team from EBS's WC2-H Amazon Web Services (AWS) Government Federal Risk and Authorization Management Program (FedRAMP).
- Deployed 27 functional requirements into production to drive proactive cyber risk and threat identification.
- Completed the initial data loss protection analytic capabilities projects supporting the Security Information and Event Management (SIEM)/Splunk ES implementation which are now in operation.
- Deployed packet capture technology to the Trusted Internet Connection (TIC) and is capturing production traffic.
- Deployed PhishMe Simulator and Triage enabling Treasury employees and contractors across the enterprise to recognize and report phishing emails.
- Deployed malware content filtering to analyze production traffic at the Treasury TIC on a limited basis. Validated that web and email traffic is being handled correctly and that there is no impact to business processes.

In the FY 2021 President's Budget, CEA initiatives are organized around the National Institute of Standards and Technology's (NIST) Cybersecurity Framework. Future objectives for the FY 2021 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.)*
    - Cybersecurity Risk Model: This initiative will identify, quantify, access, prioritize, and report on Enterprise Cyber Risks found across the Treasury Department**.** This project aligns with the Improving HVA Cybersecurity initiative from the FY 2020 Budget.

- Risk Management Dashboard: The dashboard will deliver an enterprise risk analysis and scoring capability allowing personnel to manage risks through clear, centralized rankings. This project aligns with the Proactive Cyber Risk and Threat Identification initiative from the FY 2020 Budget.
- Risk Management Framework (RMF) Automation Tool: The tool would include controls scorecard measurement, dashboard reporting, and the generation of Risk Management Framework (RMF) System Assessment and Accreditation (SA&A) artifacts. This project aligns with the Proactive Cyber Risk and Threat Identification initiative from the FY 2020 Budget.

- Protect the Delivery of Critical Infrastructure Services *(Goal: Develop and implement appropriate safeguards to ensure delivery of critical services.)*
  - HVA Security Enhancements: Treasury has elected to perform discretionary RVAs and Security Architecture Reviews (SAR) where DHS HVA RVAs are not feasible. This initiative provides support for these additional assessments. This project aligns with the Improving HVA Cybersecurity initiative from the FY 2020 Budget.
  - Data Centric Security and Encryption: This initiative would provide resources to address emerging threats that are not imminent today (e.g., artificial intelligence, social engineering, and quantum computing) in order to push protections closer to the data, consistent with the concept of Zero Trust that was recommended by the House Committee on Oversight and Reform following the Office of Personnel Management breach. This project aligns with the Enhancements to Cybersecurity Infrastructure initiative from the FY 2020 Budget.
  - Treasury Identity Enterprise Services (TIES): The tools and services provided by Continuous Diagnostics and Mitigation (CDM) identity and access management capability provide Treasury with an opportunity to implement TIES, an identity management system that provides enterprise-class services for centrally managing employee and contractor identities/user accounts, credentials, and access to systems at the Department level. This further aligns Treasury identity management with OMB M-19-17. This project aligns with the Enhancements to Cybersecurity Infrastructure initiative from the FY 2020 Budget.
  - Centralized Key Management Services (CKMS): This initiative will design, procure, and implement a centralized Treasury-wide key management service. Utilizing a centralized key management service will allow Treasury to bring all facets of crypto key management, including hardware, software, and processes, into one location. This project aligns with the Enhancements to Cybersecurity Infrastructure initiative from the FY 2020 Budget.
  - Cloud Access Security Broker (CASB): Cloud environments create an aperture through which a bad actor can enter and disrupt Treasury's mission. A Cloud Access Security Broker (CASB) will sit between Treasury Bureaus and cloud service providers to enforce security, compliance, and governance policies for and between the dozens of cloud applications used by Treasury. This project aligns with the Enhancements to Cybersecurity Infrastructure initiative from the FY 2020 Budget.
- Detect Cybersecurity Events (*Goal: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.)*
  - Cybersecurity Threat Hunting Analysis: This investment provides access to data via intelligence feeds to supply the indicators and toolsets Treasury needs to identify malicious behavior within its datasets, providing the Government Security Operations Center (GSOC) analysts with enhanced insight and understanding of cyber threat actors' command and control, infrastructure, and capabilities. This project aligns with the Enhanced Incident Response and Recovery Capabilities initiative from the FY 2020 Budget.
- Respond to Detected Cybersecurity Incidents (*Goal: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.)*

- Enhanced Treasury Cyber/Fraud Management Capabilities: A cross-functional incident response team will provide Treasury with the ability to support analysis and triage of cybersecurity and fraud incidents with the goals of increasing detection, reducing potential dwell time between the detection and containment, and reducing the overall impact of an incident to the Treasury. This project aligns with the Enhanced Incident Response and Recovery Capabilities initiative from the FY 2020 Budget.

- 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.)*
  - HVA Security Enhancements: This initiative includes the mitigation of enterprise level cyber risks discovered through the RVA/SAR assessments and/or other Enterprise Risk Management Activities to provide better visibility of Treasury's current cyber posture. This project aligns with the Improving HVA Cybersecurity initiative from the FY 2020 Budget.

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. 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.

Investment Obligations: (In Millions of $):

Type	FY 2019	FY2020	FY2021	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	0.50	0.40	0.25	-0.15	-36.92%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	36.91	34.15	34.60	0.45	1.32%
Total Obligations	37.41	34.55	34.86	0.30	0.88%

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 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

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 2019	FY2020	FY2021	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	46.25	37.83	27.98	-9.84	-26.03%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	27.94	28.54	27.88	-0.66	-2.31%
Total Obligations	74.19	66.36	55.86	-10.50	-15.83%

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

Description:

Treasury IT Infrastructure Telecommunications (TNet) 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 2019	FY2020	FY2021	Change in $	% 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))	78.00	78.08	80.39	2.31	2.96%
Total Obligations	78.00	78.08	80.39	2.31	2.96%

Purpose, Accomplishments, Future Objectives:

The 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

Type	FY 2019	FY2020	FY2021	Change in $	% Change
Sub-Total O&M Obligations (Including Internal labor (Govt. FTE))	8.03	10.33	8.73	-1.60	-15.49%
Total Obligations	8.03	10.33	8.73	-1.60	-15.49%

Purpose, Accomplishments, Future Objectives:

Data analytics remain a priority investment area, with new capabilities in machine learning and artificial intelligence, enhancing TFI's ability to identify threat finance networks. Additional investments in IT consolidated systems and secure networks will make TFI's workforce more efficient and effective in

managing workload across multiple classification systems while also enhancing the security surrounding the information, intelligence, and analysis used. These investments ensure sufficient IT infrastructure for existing programs and enhanced capacity to address increasing or emerging threat areas. Investments include:

- Operational enterprise tool capable of fusing TFI's disparate data streams for Treasury Foreign Intelligence Network (TFIN) desktop analysis by TFI staff that builds upon the TFI Data Discovery initiative.
- Increased bandwidth within existing infrastructure to support and build a more robust capability for collaborative data discovery initiative.
- OFAC IT Infrastructure upgrades to include secure online communications tools, enhancements to the consolidated IT systems, 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 2019	FY2020	FY2021	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	4.00	10.72	11.97	1.25	11.66%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	0.00	0.00	0.00	0.00	0.00%
Total Obligations	4.00	10.72	11.97	1.25	11.66%

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.

The FY 2019 funding was used for Main Treasury roof replacement, and exterior repairs and restoration to the Freedman's Bank Building (FBB). FY 2020 funding is being used to make investments that will

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. Treasury's FY 2021 request will fund further repairs and renovations to Treasury's buildings such as the replacement and maintenance of masonry, windows, and interior spaces.