Department of the Treasury
Departmental Offices
FY 2027
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 2025 Actuals - Total actual obligations
- FY 2026 Estimated Obligations - Anticipated obligations from all budgetary resources (e.g., balances from prior years, user fees, and FY 2024 Operating levels).
- FY 2027 Estimated Obligations - Anticipated obligations from all budgetary resources (e.g., balances from prior years, user fees, and FY 2027 President's budget).

Major IT Investments

HRLOB – HRConnect

Description:

HRConnect (HRC) is the Department of the Treasury's enterprise system of record for Human Capital Management (HCM). It supports critical workforce functions, including personnel actions, payroll integration, time and attendance, and employee data across bureaus. As a federalized HCM platform and Shared Service Provider (SSP), HRC delivers secure, scalable, and standardized HR solutions to all Treasury bureaus and 38 other government agencies. The system currently supports approximately 236,000 employees and contractors and serves as the flagship product of Treasury's HR Line-of-Business (HRLOB).

HRC is built on Oracle PeopleSoft and hosted in Oracle Government Cloud, meeting FedRAMP High security requirements. The platform provides integrated core HR capabilities with both employee and manager self-service functionality. Key features include:

- Employee and Manager Self Service
- Position Budget Management
- Contractor Management
- Office of Government Ethics (OGE)
- Financial Disclosure Form 450 tracking
- Outside Employment tracking
- Separated Employee/Contractor Clearance
- Personnel Action Request (PAR) processing

HRC provides configurable capabilities that support both bureau-specific requirements and standardized implementation across Treasury and partner agencies. The system maintains bi-directional integration with the National Finance Center (NFC) for payroll processing and integrates with key federal systems including USA Staffing and USA Hire to support end-to-end human capital operations.

Investment Obligations: (In Millions of $):

Type	FY 2025 Actuals	FY 2026 Estimated Obligations	FY 2027 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including internal labor (Govt FTE))	26.149	7.847	7.239	-0.608	-7.75%
Sub-Total O&M Obligations (Including Internal Labor (Govt FTE))	48.035	46.343	46.466	0.123	0.27%
Total Obligations	74.184	54.19	53.705	-0.485	-0.89%

Purpose, Accomplishments, Future Objectives:

HRConnect serves as Treasury's enterprise HCM platform, enabling the delivery of standardized, technology-enabled HR services across all Treasury bureaus and partner federal agencies. As one of the Office of Personnel Management (OPM) HR Line of Business shared service providers, HRC supports the full lifecycle of human capital operations, including personnel action processing, payroll integration, benefits administration, time and attendance, and workforce data management.

In the absence of new investment-driven initiatives, HRC efforts are focused on sustaining and strengthening core operational capabilities to support Treasury and partner agencies. Key priorities include:

- Maintaining secure, reliable, and scalable HR service delivery across all supported agencies
- Supporting daily payroll processing and integration with NFC
- Ensuring continued interoperability with federal systems, including USA Staffing and USA Hire
- Meeting evolving federal policy, regulatory, and reporting requirements
- Supporting partner agency needs and ongoing service delivery

HRC provides a range of enterprise and operational benefits to Treasury and its partner agencies, including:

- Standardization: Delivers a single, consistent HR solution across bureaus and agencies, reducing fragmentation
- Efficiency: Streamlines HR processes through automation and self-service capabilities, reducing administrative burden
- Data Quality and Reporting: Improves data consistency and enables more reliable workforce reporting and decision-making
- Cost Avoidance: Reduces the need for duplicative systems and associated maintenance costs across agencies
- User Experience: Provides employees, managers, and HR professionals with direct, streamlined access to HR information and services

Continued investment in HRC sustains a secure, compliant, and enterprise-wide HR capability that supports mission operations across Treasury and partner agencies while avoiding duplication, reducing risk, and maintaining service continuity.

HRC has continued to deliver modernization, security, and operational improvements that enhance system performance, user experience, and compliance across Treasury and partner agencies. Key accomplishments include:

- Modernized HR Capabilities: Delivered enhancements to improve user experience and streamline HR processes, including updates to manager self-service and employee-facing functionality
- Automation and Process Improvement: Implemented automation for key HR functions such as Office of Government Ethics (OGE) Form 450 processing, reducing manual effort and improving data accuracy
- Integration with Federal Systems: Established and enhanced integrations with systems such as USA Staffing, reducing manual steps and improving efficiency in hiring workflows
- Security and Compliance Enhancements: Strengthened cybersecurity posture through implementation of multi-factor authentication, vulnerability remediation, and ongoing audit support
- System Modernization: Advanced HRConnect modernization efforts, including progress toward updated system versions and cloud-based infrastructure improvements
- Infrastructure and Cost Optimization: Retired legacy components and implemented more efficient architecture, including replacement of the legacy access gateway with a modern authentication approach, resulting in reduced operational costs
- Improved Identity and Access Capabilities: Enhanced authentication and access management through integration with enterprise identity services, supporting more secure and streamlined user access
- Interagency Collaboration: Partnered with federal stakeholders, including IRS and other agencies, to support system transitions, requirements alignment, and shared service delivery

These efforts have improved system reliability, strengthened security, and reduced operational

inefficiencies across HRConnect's enterprise user base. HRC will continue to focus on sustaining and advancing its role as Treasury's enterprise HR platform, with priorities centered on modernization, security, and service delivery:

- Sustain Core Operations: Maintain reliable, secure, and scalable HR service delivery for Treasury and partner agencies
- Advance Modernization Efforts: Continue system upgrades, cloud adoption, and platform enhancements to improve performance and user experience
- Strengthen Security Posture: Enhance cybersecurity controls, identity integration, and compliance with evolving federal requirements
- Enhance Integration and Interoperability: Expand and mature integrations with federal systems and identity platforms to support end-to-end HR processes
- Improve User Experience: Simplify and streamline HR processes through automation and improved self-service capabilities
- Support Workforce Modernization: Enable Treasury-wide initiatives to standardize HR services, improve workforce data management, and support strategic decision-making

Integrated Talent Management (ITM)

Description:

Integrated Talent Management (ITM) investment provides an enterprise Software as a Service (SaaS) solution to enable and automate learning management, performance management, succession planning, career development, and compensation planning processes throughout the Department of the Treasury.

Investment Obligations: (In Millions of $):

Type	FY 2025 Actuals	FY 2026 Estimated Obligations	FY 2027 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including internal labor (Govt FTE))	5.471	0	0.3	0.3	
Sub-Total O&M Obligations (Including Internal Labor (Govt FTE))	9.35	11.377	11.33	-.0047	-0.41%
Total Obligations	14.821	11.377	11.63	.253	2.22%

Purpose, Accomplishments, Future Objectives:

Integrated Talent Management (ITM), as Treasury's talent management application, automates, standardizes and ensures compliance of human resource business processes across the Department. ITM provides a shared user experience for employees and managers, with tools to enable professional development, manage employee performance, plan for workforce and succession planning needs, and formulate compensation worksheets for awards and pay increases.

ITM goals are linked to and directly support the Treasury Strategic Plan Goal 4.4, Deliver High-quality Common Services to the Treasury Enterprise, and further driven by emerging requirements from the Office of Personnel Management (OPM). Current priorities and objectives include:

- Deliver technology and training to enable the upskilling of professionals to support AI initiatives.
- Deliver and ensure compliance with annual mandatory training requirements.
- Enhance data integrations and automate business processes with Treasury Common Services Center applications (HRC, Mulesoft, Service Now, Data Insight Portal).
- Standardize delivery and reporting for security role-based training requirements.
- Standardize performance management for executives, senior leaders, and non-executive employees for all of Treasury.
- Deliver two annual upgrades to enhance the product tools and services.
- Implement technologies to enhance system audit logs and capabilities.

ITM meets the requirements of a Treasury-wide talent management application. ITM addresses a full range of talent management-related activities including learning management, competency management, performance management, compensation management, succession planning and workforce planning. Additional capabilities provided by ITM can include recruitment, analytics, low code application development leveraging microservices, and supplemental data and process automation through employee central.

ITM is dedicated to automating and streamlining non-core human resource business processes and procedures through continuous customer engagement and technology modernization. This includes learning management, performance management, career development, competency assessment, succession planning, mentoring, compensation, and reporting functions tailor configured to the business needs of the

bureau human capital offices. Notable projects include, but are not limited to:

- IRS ITM Optimization (I2O)
- Bi-annual System Upgrades
- Integration Modernization Initiative
- Standardized Performance Management
- Service NOW Integration
- Electronic Evaluation System
- Reporting Modernization
- Talent Intelligence Hub
- Single Sign On (SSO) Modernization
- Compensation and Awards
- Competency Assessments & Career Development
- Office of Executive Resources Performance and Compensation Management for SES
- RPA Services for Recording External Training
- Training Content Management Services

USA Staffing (USAS)/USA Hire (USAH)

Description:

USAS is the Office of Personnel Management (OPM) end-to-end talent acquisition solution. Through USAS, Treasury bureaus increase the efficiency of their staff acquisition lifecycle by recruiting, assessing, evaluating, certifying, selecting, and onboarding quality candidates for federal positions. The system supports a broad range of federal hiring flexibilities, authorities, and unique agency processes and is tightly integrated with OPM's USAJOBS and USAH.

OPM provides all hosting, data storage, maintenance, security, and disaster recovery for the system.

Treasury bureaus receive USAH standard assessments as part of their licensure inclusive of all federal job series from entry level to senior level. The standard assessment package includes Federal Supervisor Assessment and Early Career Talent Assessment. The assessments measure general competencies in reasoning skills, decision-making ability, math skills, reading comprehension, and soft skills including interpersonal skills, stress tolerance, and accountability. The assessments can be paired with other assessments to measure technical skills.

Investment Obligations: (In Millions of $):

Type	FY 2025 Actuals	FY 2026 Estimated Obligations	FY 2027 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including internal labor (Govt FTE))	8	0	0	0	0.00%
Sub-Total O&M Obligations (Including Internal Labor (Govt FTE))	11.449	10.289	10.295	.006	0.06%
Total Obligations	19.449	10.289	10.295	0.006	0.06%

Purpose, Accomplishments, Future Objectives:

USAS is the foundation for a successful hiring process, securely connecting HR, managers, applicants, and new hires to the data and tools they need.

Key benefits realized with the implementation of USAS and USAH solutions include:

- Deliver an exceptional hiring manager experience
- Create, authorize, and publish position descriptions
- Manage, monitor, and analyze staffing workload
- Streamline hiring processes for HR staff and applicants
- Enable paperless pre-employment and onboarding
- Increase the efficiency and reliability of the agency hiring process
- Provide robust applicant assessments
- Deliver personalized service and support, including account management, user support, and continuous improvement
- Generate robust reporting and analytics
- Ensure hosting, security, and privacy are fully managed and included

Goal 1 – Manage Operations & Maintenance (O&M) of Treasury's use of USAS and USAH

- Monitor bi-weekly product releases, ensuring timely communication of features and updates that are critical to Treasury operations or aligned with administrative priorities
- Oversee the intake and prioritization of system enhancement requests submitted by Treasury bureaus

- Lead customer communications by providing clear, consistent updates on system changes, issues, and improvements to stakeholders
- Ensure ongoing compliance with cybersecurity requirements, including reviewing security documentation, assisting with data calls, and supporting audits and assessments
- Monitor interconnections between USAS and other HR systems (e.g., HRConnect, ServiceNow)
- Serve as the Treasury Advisory Board member and participate in the quarterly USAS Advisory Board (AB) meetings to stay informed on evolving HR trends, review system updates and upcoming enhancements to USAS, USAH, and USAJOBS

Goal 2 – Support Treasury compliance with OPM's Merit Hiring Plan through solutions in USAS and USAH

- Technical Assessments – Support agency replacement of self-assessments with technical assessments
  - Strengthen candidate assessments by implementing structured, skills-based evaluation methods that are job-related, validated, and aligned with OPM's merit hiring principles
  - Expand the use of high-quality assessment tools (e.g., USAH, Structured Interview, Structured Resume Review) to better identify top talent early in the hiring process
- Time-to-Hire Improvements – Support agency plan to reduce time-to-hire metrics by identifying bottlenecks/opportunities for efficiency

The USAS accomplishments and planned objectives include the following:

Accomplishments

- Implementation of SMS/Text Capability
- Added an assessment decision tool to guide HR users towards high-quality assessments that align with Merit Hiring Plan rules, which aims to expand the use of technical or alternative assessments and discontinue self-assessments
- Expansion of the USAH Standard Assessment Package
- Inclusion of Federal Supervisor Assessment in the USAH Standard Assessment Package

Future Objectives

- Continued support of Treasury Merit Hiring Plan Initiatives
- Implementation of USAH Interview
- Use of USA Class (AI solution) to generate position descriptions
- Enablement of Talent Pools and sharing of certificates enterprise wide
- Enable Shared Candidate Inventory

Standard/Non-Standard IT Investments

Cybersecurity Enhancement Account (CEA) - Cloud Enterprise

Description:

Treasury aims to improve, entice, and further accelerate enterprise-wide cloud adoption through investment in the Treasury enterprise shared services cloud environments. The Department's focus on cloud security enhancement and upgraded capabilities to meet security and compliance risks will involve investment in security controls, monitoring, and increased threat protections by providing a common cloud operating platform for Departmental workloads, inclusive of all security elements required by Executive Order 14028 and subsidiary guidance.

Previously part of the Cybersecurity Enhancement Account (CEA) 015-000200319 Investment.

Investment Obligations: (In Millions of $):

Type	FY 2025 Actuals	FY 2026 Estimated Obligations	FY 2027 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including internal labor (Govt FTE))	17.28	29.66	2.03	-27.63	-93%
Sub-Total O&M Obligations (Including Internal Labor (Govt FTE))	2.19	0.73	0.29	-0.45	-61%
Total Obligations	19.47	30.39	2.32	-28.08	-92%

Purpose, Accomplishments, Future Objectives:

The CEA cloud investment focuses on an enterprise-wide investment approach to build stronger protections and further benefit the bureaus in their cybersecurity goals. With the creation of centralized appropriation, administration, and governance, Treasury has been able to develop and enhance Department-wide cloud services, support Bureau-level modernization goals, and drive a more robust coordination of efforts to improve the Department's ability to detect, identify, protect, recover, and respond to cybersecurity events. Through Cloud Enterprise investment, Treasury aims to improve, entice, and further accelerate enterprise-wide cloud adoption through investment in the Treasury enterprise shared services cloud environments.

In FY 2026, CEA – Cloud Enterprise investments are targeted to the Department's cloud focused modernization and the intrinsic enhancement of our cybersecurity posture. Our investments will build on prior year accomplishments, continue investment in enterprise shared services, enhance Department-wide coordination of cyber efforts, improve responsiveness to threats, deliver greater visibility and information shared, and improve threat detection, identification, and protection capabilities.

The FY 2027 estimated obligations include $2.32 million to support the consolidation efforts and transition of applications to the enterprise cloud helping to bolster cybersecurity operations through the shift in the control model. Adopting enforcement requirements such as FedRAMP authorization, and support of ZTA required to meet growing security risks, as Treasury continues to drive enhancements to web properties.

Cybersecurity Enhancement Account (CEA) - Multi-Factor Authentication

Description:

Treasury's investment in Multi-Factor Authentication (MFA) supports our development and implementation of compliant technologies for internal systems and applications. This investment is a critical component of the Department's solutions to prevent unauthorized access by adversaries, including nation state actors. MFA is a layered approach to security access to network or applications by certifying identity with a combination of two or more approved pieces of evidence (or factors) to an authentication mechanism. The Department's investment in, and sustainment of, MFA capabilities include strengthening MFA governance, ongoing investment in enterprise solutions to boost adoption, and strategic partnerships to streamline MFA related procurement effort for all Treasury Bureaus and Offices.

Previously part of the Cybersecurity Enhancement Account (CEA) 015-000200319 Investment.

Investment Obligations: (In Millions of $):

Type	FY 2025 Actuals	FY 2026 Estimated Obligations	FY 2027 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including internal labor (Govt FTE))	0.00	0.00	1.64	1.64	100%
Sub-Total O&M Obligations (Including Internal Labor (Govt FTE))	2.68	0.82	5.48	4.67	571%
Total Obligations	2.68	0.82	7.12	6.31	772%

Purpose, Accomplishments, Future Objectives:

The CEA multi-factor authentication (MFA) investment focuses on an enterprise-wide investment approach to build stronger protections and further benefit the bureaus in their cybersecurity goals. Treasury aims to develop and implement compliant technologies for internal systems and applications. This investment is a critical component of the Department's solutions to prevent unauthorized access by adversaries, including nation state actors.

In FY 2026, CEA investment is targeted to the Department's MFA-focused modernization and the intrinsic enhancement of our cybersecurity posture. Our investments will build on prior year accomplishments to enhance Department-wide coordination of cyber efforts and improve threat detection, identification, and protection capabilities. CEA will continue to support the cost of secure identity verification for taxpayers to use the government-wide electronic payment system.

The FY 2027 estimated obligations include $7.1 million for Treasury's Conversion to Active Directory (AD) Federation that provides for the authorization, authentication, and SSO functionality to applications and services virtually anywhere, including perimeter networks, partner organizations, and the cloud.

Cybersecurity Enhancement Account (CEA) - Other Cyber Priorities

Description:

Treasury maintains investment in Other Cybersecurity Priorities that address and respond to the changing threat landscape of the Department, given our interconnected technology environment, which has amplified the need for identifying and assessing the security posture of high value assets, national security systems infrastructure, Treasury's supply chain, cybersecurity governance, risk, and compliance (GRC), amongst other necessary priorities.

Previously part of the Cybersecurity Enhancement Account (CEA) 015-000200319 Investment.

Investment Obligations: (In Millions of $):

Type	FY 2025 Actuals	FY 2026 Estimated Obligations	FY 2027 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including internal labor (Govt FTE))	12.46	69.61	3.13	-66.48	-96%
Sub-Total O&M Obligations (Including Internal Labor (Govt FTE))	19.50	17.56	4.43	-13.13	-75%
Total Obligations	31.96	87.17	7.56	-79.61	-91%

Purpose, Accomplishments, Future Objectives:

Through the CEA Other Cybersecurity Priorities investment, Treasury maintains investment in initiatives that address and respond to the changing threat landscape of the Department, given our interconnected technology environment, which has amplified the need for identifying and assessing the security posture of high value assets, national security systems infrastructure, Treasury's supply chain, cybersecurity governance, risk, and compliance (GRC), amongst other necessary priorities. Additionally, Treasury is investing in a resilient future through the acquisition of federal labor cybersecurity subject matter expertise to support our complex technology portfolio, as well as the necessary resources to support the overall administration and governance of CEA appropriations and the ongoing performance of cybersecurity investments.

In FY 2026, CEA investments are targeted to the Department's cyber priorities focused on modernization and the intrinsic enhancement of our cybersecurity posture. Our investments will build on prior year accomplishments, continue investment in enterprise shared services, enhance Department-wide coordination of cyber efforts, improve responsiveness to threats, deliver greater visibility and information shared, and improve threat detection, identification, and protection capabilities.

The FY 2027 estimated obligations include $7.56 million. Treasury will continue development of Department-wide AI governance, train our workforce, implement AI tools and systems (e.g., generative code and chat tools), and ensure all AI implementations meet cybersecurity federal requirements. These AI capabilities, embedded into daily operations through automation, reduce the risk of data breaches and insider threats which result in costly remediation expenses. Looking forward, CEA investments' future objectives will continue to focus on Treasury's abilities to enhance Department-wide coordination of cybersecurity efforts and improve responsiveness to threats.

Cybersecurity Enhancement Account (CEA) - Security Logging

Description:

Treasury's investments in Security Logging ensure compliance with Office of Management and Budget (OMB) Memorandum 21-31 (M-21-31) to develop and implement security logging capabilities to receive, store, analyze, and process security event and system log data. Investment funding targets the creation and monitoring of data-stream disruptions, a shared log facility, storage and retention of log data, development of threat hunt and incident response playbooks, and the creation of user behavioral analytics capabilities to support detection of malicious behavior. The investment objective is for all logs to be accessible and visible for the highest level (enterprise) security operations center at the Department, the Treasury Shared Services Security Operation Center (TSSSOC).

Previously part of the Cybersecurity Enhancement Account (CEA) 015-000200319 Investment.

Investment Obligations: (In Millions of $):

Type	FY 2025 Actuals	FY 2026 Estimated Obligations	FY 2027 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including internal labor (Govt FTE))	0.00	14.22	1.43	-12.79	-90%
Sub-Total O&M Obligations (Including Internal Labor (Govt FTE))	24.46	16.19	5.42	-10.77	-67%
Total Obligations	24.46	30.42	6.85	-23.56	-77%

Purpose, Accomplishments, Future Objectives:

The CEA security logging investment focuses on an enterprise-wide investment approach to build stronger protections and further benefit the bureaus in their cybersecurity goals. Through the CEA Security Logging investment, Treasury ensures compliance with Office of Management and Budget (OMB) Memorandum 21-31 (M-21-31) to develop and implement security logging capabilities to receive, store, analyze, and process security event and system log data.

In FY 2026, the Security Logging investment is targeted to the Department's security logging focused modernization and the intrinsic enhancement of our cybersecurity posture. Our investments will build on prior year accomplishments, continue investment in enterprise shared services, enhance Department-wide coordination of cyber efforts, improve responsiveness to threats, deliver greater visibility and information shared, and improve threat detection, identification, and protection capabilities.

The FY 2027 estimated obligations include $6.85 million for Treasury's CEA Security Logging to continue consolidation efforts for the Security Operation Centers (SOCs) across Treasury. Security logging is vital to collecting, storing, and analyzing logs that help detect, investigate, and respond to security events. These efforts would enhance compliance with OMB memorandum M-21-31, ensuring all logs are accessible and visible to the department's highest-level operations center. Logging and incident response capabilities improvements require scaling the cloud-based logging environment used by the TSSSOC to operate efficiently and process security events and system logs across all Treasury offices, bureaus, and Treasury shared services. Looking forward, focused investments in organizational resiliency will be necessary to strengthen threat analysis, provide Security Operations Center (SOC) support for sustained cyber-attacks, and establish, operate, and maintain the Treasury logging platform.

Cybersecurity Enhancement Account (CEA) - Universal Encryption

Description:

The Department's investment in Universal Encryption supports our commitment to fully achieve encryption protocols outlined in Executive Order 14028 and subsidiary guidance (i.e., Office of Management and Budget [OMB], Cybersecurity Infrastructure and Security Agency [CISA], and others). Our investment focuses on full adoption of encryption of data at rest (DAR) and data in transit (DIT) for all Treasury systems and will address the unique challenges of our environment, proposed solutions, and the implementations necessary to address each system for compliance with encryption standards and requirements.

Previously part of the Cybersecurity Enhancement Account (CEA) 015-000200319 Investment.

Investment Obligations: (In Millions of $):

Type	FY 2025 Actuals	FY 2026 Estimated Obligations	FY 2027 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including internal labor (Govt FTE))	0.00	0.00	0.00	0.00	0%
Sub-Total O&M Obligations (Including Internal Labor (Govt FTE))	0.00	0.00	0.00	0.00	0%
Total Obligations	0.00	0.00	0.00	0.00	0%

Purpose, Accomplishments, Future Objectives:

The FY 2027 President's Budget and FY24 and FY25 appropriations did not include investments in Universal Encryption.

Cybersecurity Enhancement Account (CEA) - Zero Trust Architecture

Description:

Zero Trust Architecture (ZTA) investment priorities at Treasury seek to minimize implicit trust and reinvigorate least privilege through a continual verification of each user, device, application, and transition. The investment approach requires the Department to enhance visibility and threat detection at the application level to improve its ability to support continuous threat analysis, detection, and response, and enable the analysis of encrypted traffic. Compartmentalization, micro segmentation, and reinforcing enforcement of continuous identity verification and conditional access policies will improve our resistance to fraudulent tampering of privileged accounts. Our objective is a universal, default security posture of "never trust, always verify" across our entire technology stack.

Previously part of the Cybersecurity Enhancement Account (CEA) 015-000200319 Investment.

Investment Obligations: (In Millions of $):

Type	FY 2025 Actuals	FY 2026 Estimated Obligations	FY 2027 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including internal labor (Govt FTE))	6.52	17.22	2.14	-15.08	-88%
Sub-Total O&M Obligations (Including Internal Labor (Govt FTE))	13.48	7.11	9.20	2.09	29%
Total Obligations	20.01	24.32	11.34	-12.99	-53%

Purpose, Accomplishments, Future Objectives:

The CEA ZTA investment focuses on an enterprise-wide investment approach to build stronger protections and further benefit the bureaus in their cybersecurity goals. Treasury seeks to minimize implicit trust and reinvigorate least privilege through a continual verification of each user, device, application, and transactions. Treasury leverages the ZTA investment to provide additional human capital to support management of service providers, as well as development, testing, and deployment of the applications that have the security controls integrated into them. This investment also supports the Treasury Zero Trust enterprise identity access solution, known as Common Approach to Identify Access Management (CAIA), for all external federal partners who access the Enterprise Content Management (ECM) SharePoint platform for shared services.

In FY 2026, CEA – ZTA investments are targeted to the building the Department's skilled Federal engineering capability providing direct services and reducing the need to procure additional contracted service and delivers engineering capability to include Technical Advisory, Solution Development, AI & Data Enablement, Infrastructure Modernization, and Embedded Technical Support.

The FY 2027 estimated obligations include $11.34 million to minimize 'implicit trust' and strengthen 'least privilege' principles. The ZTA approach is a paradigm shift from verifying once at the perimeter to continual verification of each user, device, application, and transaction. For FY 2027, Treasury plans to sustain ZTA-aligned IT services, functions, and systems. Funding will support the engineering work spanning across the five ZTA pillars (Identify, Device, Network, Application and Workload, and Data) established through NIST and CISA's Zero Trust Maturity Model.

Enterprise Systems Identify Management (ESIM)

Description

The Enterprise Systems Identity Management (ESIM) Investment provides enterprise technical and programmatic ICAM requirements, services, systems and solutions for Personal Identity Verification (PIV) credentialing, multi-factor authentication (MFA), Identity and Access Management (IdAM), and Public Key Infrastructure (PKI). These compliant services and solutions enable bureaus to achieve Federal ICAM compliance, meet mandated ICAM requirements for PIV cards, Logical Access Control Systems (LACS) for local, remote, public facing, and mobile device network access; and Physical Access Control Systems (PACS) for facilities. These capabilities improve security and efficiency, promote interoperability, and enhance user experiences with streamlined enterprise processes including, but not limited to: Single Sign-On, Treasury Enterprise Authentication Service (TEAS), IAM and centralized directory through the SailPoint consolidation initiative, Credential and Privileged account management services, and PKI for authentication, encryption, and digital signatures.

Investment Obligations: (In Millions of $):

Type	FY 2025 Actuals	FY 2026 Estimated Obligations	FY 2027 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including internal labor (Govt FTE))	84.71	128.363	128.652	0.289	0.23%
Sub-Total O&M Obligations (Including Internal Labor (Govt FTE))	33.13	5.46	5.058	-0.402	-7.36%
Total Obligations	117.84	133.823	133.71	-0.113	-0.08%

Purpose, Accomplishments, Future Objectives:

The ESIM capital investment consolidates funding that supports Treasury's sustainment of Homeland Security Presidential Directive 12 (HSPD-12), Federal Identity, Credential, and Access Management (FICAM), MFA, TEAS, SailPoint Identity Security Cloud (ISC) consolidation initiative, which includes the enterprise directory service and PKI requirements. Supporting 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 ESIM phased implementation provides the following across 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, and standards
- Improved interoperability
- Expanded use of PIV encryption and digital signature certificates (ensuring adoption of multi-factor authentication)
- Elimination of redundancy

Treasury/ESIM 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 both privileged and unprivileged users. These goals have helped the Department align with the required OMB and FICAM goals. ESIM has updated the Department strategic roadmap and planned for the following investment goals:

Goal 1 - Identity and Access Management (IdAM): Migrate Treasury's Identity & Access Management (IAM) service to a hybrid model, centralizing identity, and access management through SailPoint ISC as a shared service (SaaS), while continuing to support exempted High-Value Asset (HVA) applications on

the existing on-premises CAIA SailPoint Identity IQ (IIQ) environment.

- Identify and onboard additional privileged accounts for managed service customers including service/non-human accounts.
- Consolidate existing SailPoint IIQ instances into a centralized hybrid IdAM solution to improve visibility, streamline policy enforcement, and lower operational costs.

Goal 2 - Expand usage of the Enterprise Derived Credential issuance capability to support authentication to Treasury infrastructure from mobile devices across Treasury through FY 2026.

- The CA API Gateway is being leveraged to securely enable Entrusts Derived PIV Credentials (DPC) as a pathway to provide DO IT with DPC serial numbers.
- Derived PIV Encryption Credentials expansion to allow federal employees to encrypt, decrypt, and protect sensitive data when using mobile devices. This will provide secure email (S/MIME), document encryption, and secure data exchange completion through FY 2026.

Goal 3 - Enterprise solution for tracking and monitoring the internal PKI certificates generated and in use within each bureau in FY 2028.

- Leverage existing efforts already underway at IRS to implement certificate lifecycle management and extend as a shared service to all bureaus.
- Enterprise certificate discovery and lifecycle management reduces operational risk, strengthens security, and improves compliance across the organization. Certificates are distributed across Treasury servers, applications, cloud workloads, network devices, and user endpoints, which makes manual tracking unreliable and creates risk of outages, failed integrations, and security gaps caused by expired, unknown, or misconfigured certificates.
- A centralized certificate management solution will provide continuous discovery, inventory, policy enforcement, automated renewal, and reporting, giving leadership visibility into certificate-related risk while reducing administrative burden on IT and security teams.
- The realized result will be improved service availability, stronger cryptographic governance, faster audit readiness, and lower total cost of ownership by replacing manual processes with standardized, automated lifecycle management.

Goal 4- Implement a Physical Access Secure System (PASS) for Treasury.

- Initiate a pilot solution which will enable Treasury employees and contractors as well as visitors to request access Treasury facilities (FY 2027).
- Following the pilot, PASS will be assessed, and return on investment (ROI) will be determined. Expansion across the enterprise will be based on these findings.
- PASS will drastically improve safety and security, enhance operational efficiency, increase integration and interoperability, enhance incident response and emergency readiness, improve compliance and audit readiness, and optimize resource and cost.

Treasury 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, ESIM Operations and Maintenance tasks include OMB, FISMA, and Cyber reporting specific to identity, credential and access management.

The ESIM accomplishments and planned objectives include the following:

- CDM IdAM Managed Services successfully completed the Enterprise SailPoint Identity IQ (TCCM) and IRS' BEARS SailPoint to SailPoint integration in FY 2026
- Implemented 10 applications to the Treasury Enterprise Federation / Single Sign-On (SSO) service to support phishing resistance MFA, Zero Trust Architecture (ZTA), and third-party providers (CSPs) ID.me and Login.gov authentication in FY 2025-2026

- For Treasury MFA overall (including enterprise and public identities): the MFA target for FY 2026 increased from 89% to 91% as the current operational MFA status remains consistent at 91%. FY 2027 is targeted for a +1% increase given resource shortages to support deployments due to changes from DRP further impacted by the business process complexities associated with some of the deployments and funding risks due to budgetary constraints for application owners.
- Supported, maintained, and operated an additional 80 production applications in FY 2025-2026
- Configured ChatGPT/OpenAI Enterprise service to leverage TEAS/CAIA for PIV & Derived PIV Authentication in FY 2026
- Implemented Login.gov IAL2 option for HR Connect and ITM applications in Production environment in FY 2026
- Planning to implement FOIAXpress and OFAC Public Licensing in Production environment in FY 2026
- Provided support to the Entrust Transport Layer Security (TLS) transition to the Sectigo Certificate Authority (CA) as the new publicly trusted certificate authority to issue public-facing Treasury web certificates.
- Maintain above 95% PIV card issuance rate and providing replacements for the PIV in time sensitive activities
- Maintain 100% PIV required privileged account access and 97% PIV required unprivileged access
- Migrate the enterprise Identity & Access Management (IAM) service to SailPoint Identity Secure Cloud (ISC) SaaS as shared service for centralized Identity Governance (IGA) and Lifecycle Management (LCM)
    - Consolidate the Department's four SailPoint instances (ESIM_TCCM, BFS_CAIA, IRS_BEARS and OCC) SailPoint IIQ) into a Hybrid approach for a centralized Identity and Access Management Solution
    - Centralize bureau Active Directory Domains and SaaS/cloud access provisioning
    - Holistic view of user identity and access profile across all environments
    - AI-driven identity governance, policies, workflows, and analytics
    - SailPoint ISC to be mandated source for all Treasury applications
- Implementation of an Enterprise PKI certificate management monitoring solution in FY 2027
- Conducted extensive market research: Developed a detailed requirements matrix to shape the design and development of Treasury's new physical access solution, which was incorporated in the system procurement package.
- Spearheaded consolidation efforts, in close partnership with Treasury facilities and the Office of Security Programs (OSP) to implement more robust security protocols at DO facilities and enhance Treasury's PACS capabilities that increase operational visibility and oversight to protect Treasury's most important asset, its people
- Implement a pilot enterprise Physical Access Secure System (PASS) for employees and contractors to request access to facilities in FY 2027.

Major Non-IT Investments

Department-wide Systems and Capital Investments Program (DSCIP) - Main Treasury Building and Freedman's Bank Building

Description:

Address life safety, security, code compliance, deferred maintenance, and critical building systems risk at the Main Treasury Building and the Freedman's Bank Building through phased repairs, modernization, and capital improvements that preserve mission operations and historic assets.

Investment Obligations: (In Millions of $):

Type	FY 2025 Actuals	FY 2026 Estimated Obligations	FY 2027 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	$14.439	$13.410	$20.907	$7.497	55.91%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))					
Total Obligations	$14.439	$13.410	$20.907	$7.497	55.91%

Purpose, Accomplishments, Future Objectives:

This investment addresses deferred maintenance, security, code compliance, and critical building systems risk at the Main Treasury Building (MT) and the Freedman's Bank Building (FBB). The FY 2027 request reflects a limited subset of previously identified needs and builds on prior-year efforts to repair the MT building's exterior envelope while adding funding for major interior repairs and upgrades. Requested resources will support replacement of major mechanical systems, perimeter fencing security upgrades, and capital repairs involving electrical systems, ADA compliance, elevators, historic preservation, and overall building condition and aesthetics. These investments support Treasury's long-term strategy to maintain and modernize its owned facilities, preserve irreplaceable historic assets, and avoid critical system failures that could disrupt mission-essential operations.

Treasury will continue a phased approach to modernization so that the MT building and FBB remain occupied and fully operational during construction. FY 2027 funding is intended to advance replacement of aging HVAC and chilled water infrastructure that, in many cases, has exceeded its useful life and has experienced repeated breakdowns, building damage, and costly repairs. The MT building houses the chilled water plant for the Treasury complex, and because the chillers provide the vast majority of cooling for headquarters operations, failure of this system could potentially shut down daily operations and critical IT networks housed on site. Funding will also support replacement of air handling units, computer room air conditioning units, and fan coil units; project design, inspection, and consultation; deferred maintenance and historic preservation work; and planning and design for perimeter fencing and pedestrian screening upgrades that strengthen site security, force protection, resiliency, and mission assurance for MT and FBB personnel and systems.

Treasury Operations have continued to make measurable progress in restoring and preserving these facilities. In FY 2025, phase 4 of the MT façade repair and preservation effort, covering the east side of the building, was completed in December 2025, along with 25 percent of phase 5 in the north and south courtyards; the west and north elevations in the south courtyard were also completed in

December 2025. Treasury also advanced more than 56 completed and ongoing projects to address damaged plaster and aged or discolored paint in the MT building, completed design drawings for four new cooling towers as part of the first year of a seven-year mechanical modernization plan, and launched the study and design for modernization of the MT fire alarm system with mass notification integration. Looking ahead, Treasury plans to continue the phased replacement of aging mechanical systems, award a competitive contract for design and replacement of the chillers, advance security enhancements at MT, and reduce deferred maintenance at both MT and FBB. This strategy reflects a risk-based, fiscally disciplined approach intended to improve reliability, reduce service disruptions, and maintain safe, resilient, and functional facilities for Treasury operations.