Department of the Treasury
Departmental Offices
FY 2025
Capital Investment Plan

Standard IT Investments 3
Treasury Shared Services Security Operations Center (TSSSOC) 3
Major IT Investments 4
Cybersecurity Enhancement Account (CEA) - Cloud Enterprise 4
Cybersecurity Enhancement Account (CEA) - Multi-Factor Authentication 6
Cybersecurity Enhancement Account (CEA) - Other Cyber Priorities 7
Cybersecurity Enhancement Account (CEA) - Security Logging 9
Cybersecurity Enhancement Account (CEA) - Universal Encryption 11
Cybersecurity Enhancement Account (CEA) - Zero Trust Architecture 12
HR LoB - HRConnect 14
Treasury Enterprise Identity, Credential and Access Management (TEICAM) 16
Major Non-IT Investments 19
Main Treasury Building and Freedman's Bank Building 19

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

FY 2023 Actuals -Total actual obligations.
FY 2024 Estimated Obligations- Anticipated obligations from all budgetary resources (e.g., balances from prior years, user fees, and FY 2023 Operating levels).
FY 2025 Estimated Obligations - Anticipated obligations from all budgetary resources (e.g., balances from prior years, user fees, and FY 2025 President's budget).

Standard IT Investments

Treasury Shared Services Security Operations Center (TSSSOC)

Description:
TSSSOC functions as the Department wide security operations center providing security monitoring, incident coordination, incident response, and reporting. TSSSOC operates 24x7x365 and actively coordinates with other federal agencies, DoD, and the IC.

Investment Obligations: (In Millions of $):

Type	FY 2023 Actuals	FY 2024 Estimated Obligations	FY 2025 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	2.26	1.09	1.09	0	0%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	15.44	14.75	15.19	0.44	2.98%
Total Obligations	17.70	15.84	16.28	0.44	2.78%

Purpose, Accomplishments, Future Objectives:

The Treasury Shared Services Security Operations Center (TSSSOC) provides leadership and oversight for the offices and bureaus across Treasury in all aspects of cybersecurity operations. 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 operations. The program also provides central coordination and reporting on cybersecurity operational metrics and programs to external agencies and sets Treasury cybersecurity operations standards and guidance. TSSSOC also provides departmental situational awareness of cybersecurity incidents and coordinates response to intrusion activity. The program also serves as a lead in implementing the Treasury Cybersecurity Strategy.

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

Major 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. Treasury's recently awarded Blanket Purchase Agreement (BPA) for cloud services (Treasury Cloud [TCloud]) will support our design, development, and implementation of security patterns and guardrails with expanded Security Operations Center (SOC) capabilities to accommodate increased telemetry from cloud assets and workloads.

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

Investment Obligations: (In Millions of $):

Type	FY 2023 Actuals	FY 2024 Estimated Obligations	FY 2025 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	20.07	25.33	15.80	-9.53	-37.61%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	0.65	1.60	9.63	8.03	501.56%
Total Obligations	20.72	26.93	25.43	-1.50	-5.57%

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 a 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 the CEA 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. The Department's focus on cloud security enhancement and upgraded capabilities to meet security and compliance risks involves 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.

The FY 2025 President's Budget includes $25.4 million for Treasury's CEA Cloud Enterprise investment with alignment to the NIST Cybersecurity Framework priorities:

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

In FY2025, 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.

- Treasury seeks to support the following initiatives with final FY2025 appropriations:
- Bureau of the Fiscal Service cloud cybersecurity modernization and the necessary human capital to support initiatives.
- Cloud security resources (engineers, ISSM, etc.) to support the FY2023 awarded enterprise TCloud contract and program.
- Application migrations from on-premises to cloud environments and/or from unique Bureau environments to the enterprise cloud platform.
- Incident response infrastructure to support coordination and communication in an uncompromised environment for response and recovery activities.
- Migration of National Security System infrastructure to the cloud.
- Operations, maintenance, and ongoing investment in a sustainable low code cloud platforms (i.e., ServiceNow, Salesforce) to support organizational capabilities, to include Cybersecurity Governance, Risk, and Compliance; CEA Administration and Governance; and Security.
- Storage support for enterprise logging collection and utilization of historic logs to support threat hunt and threat detection activities, as well as additional behavioral analytics.
- Expansion of the Department's enterprise offering for public-facing, cloud-based web hosting that includes an Akamai CDN with robust DoS and bot protections, a Drupal content management system, and additional centralized site shield, web performance and readiness/response investments that integrate with Treasury's security operations capabilities for threat detection and response.

Looking forward, CEA investments will aim to accomplish the below future objectives:

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

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 2023 Actuals	FY 2024 Estimated Obligations	FY 2025 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	0.00	5.10	0.00	-5.10	-100.00%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	0.00	0.60	2.50	1.90	316.67%
Total Obligations	0.00	5.70	2.50	-3.20	-56.14%

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. With the creation of a 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 the CEA Multi-Factor Authentication investment, 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. 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 of MFA, and strategic partnerships with industry partners to streamline MFA related procurement effort for all Treasury Bureaus and Offices.

The FY 2025 President's Budget includes $2.5 million for Treasury's CEA Multi-Factor Authentication investment with alignment to the NIST Cybersecurity Framework priorities:

- Identify the Business Context, Resources & Cybersecurity Risk Goal: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

In FY2025, CEA – Multi-Factor Authentication 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, 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.

Treasury is looking to support the following initiatives with final FY2025 appropriations:
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.

- Looking forward, CEA investments will aim to accomplish the below future objectives:
- Enhance Department-wide coordination of cybersecurity efforts and improve responsiveness to threats.
- Provide leadership with greater visibility into cybersecurity efforts and encourage information sharing.
- Improve identification of cyber threats and better protect information systems from attack.
- Provide platform to enhance communication, collaboration, and transparency.

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. 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 Cybersecurity Enhancement Account (CEA) appropriations and the ongoing performance of cybersecurity investments.

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

Investment Obligations: (In Millions of $):

Type	FY 2023 Actuals	FY 2024 Estimated Obligations	FY 2025 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	17.79	2.73	6.05	3.32	121.54%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	8.75	12.90	18.90	6.01	46.58%
Total Obligations	26.55	15.63	24.95	9.33	59.68%

Purpose, Accomplishments, Future Objectives:

The CEA investment for other cybersecurity priorities focuses on an enterprise-wide investment approach to build stronger protections and further benefit the bureaus in their cybersecurity goals. With the creation of a 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 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.

The FY 2025 President's Budget includes $25.0 million for Treasury's CEA Other Cybersecurity Priorities investment with alignment to the NIST Cybersecurity Framework priorities:

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

In FY2025, CEA – Other Cybersecurity Priorities investment is targeted to the Department's cyber priorities focused om 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.

Treasury is looking to support the following initiatives with final FY2025 appropriations:

- Establish a repeatable programmatic structure to review, assess, and govern emerging technologies (i.e., quantum, Artificial Intelligence [AI], etc.) to ensure applications of all security standards develop consistent policies, workforce planning, reporting, Bureau adherence, ethical use, etc.
- Acquisition of an enterprise EDR solution
- Workforce focused cyber awareness and other supplemental trainings
- Enhanced security compliance of a low code platform through Enhanced Adoption and Automation of Change Management/Enablement, as well as increased use of common controls.
- Evolution of the Enterprise Cyber Risk Management (ECRM) initiative which will continue to strengthen Treasury's approach to managing risks across the enterprise and instantiate a continuous review of all of its critical networks, systems, and data.

- Development of a low code Configuration Management Database (CMDB) solution, encompassing both Asset Management and Configuration Management.
- Development of a Risk Management Framework for enterprise infrastructure
- Investment in Organizational Resiliency and the associated human capital component to address current and emerging cyber priorities such as Supply Chain Risk Management (SCRM) and incident response support.
- Performance of enterprise-level FISMA readiness assessments.
- Facilitation of an Enterprise Cyber BPA ordering capability (PROTECTS)
- Investment in an Annual Threat Hunt that identifies a random sampling of Treasury systems to identify anomalies beyond traditional detection methodologies.

  Acquisition of Incident Response support, allowing for defined response timeline in the event of a compromise and need for SME and resource depth.

Looking forward, CEA investments will aim to accomplish the below future objectives:

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

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 2023 Actuals	FY 2024 Estimated Obligations	FY 2025 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	25.66	2.48	29.41	26.93	1,088.24%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	0.00	4.00	11.92	7.92	197.90%
Total Obligations	25.66	6.48	41.33	34.85	538.22%

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. With the creation of a 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 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. 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).

The FY 2025 President's Budget includes $41.3 million for Treasury's CEA Security Logging investment with alignment to the NIST Cybersecurity Framework priorities:

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

In FY2025, CEA – 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.

Treasury is looking to support the following initiatives with final FY2025 appropriations:

- Security Logging efforts to protect against Distributed Denial-of-Services (DDoS) and other cyber-attacks including 1) increase of storage for Treasury Trusted Internet Connection (TIC) packet capture data, allowing rapid forensic analysis of suspected attacks; 2) expansion of Web Application Firewall (WAF) capabilities for applications and services across the Department; and 3) implementation of indexers at the Network Colocations which will provide critical cyber visibility and analytics.
- Investment in Organizational Resiliency and the associated human capital component necessary to strengthen threat analysis, provide Security Operations Center (SOC) support for sustained cyber attacks, and establish, operate, and maintain the Treasury logging platform.
- Expansion of the SOC to provide enterprise SOC capabilities for Treasury bureaus, including Operations analysts, intake support, Threat & Research analysts, enhanced capabilities, and associated equipment.
- Investment in cloud-based log processing, storage, and platform licenses.

Looking forward, CEA investments will aim to accomplish the below future objectives:

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

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 2023 Actuals	FY 2024 Estimated Obligations	FY 2025 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	0.00	2.50	1.00	-1.50	-60.00%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	0.00	0.48	0.00	-0.48	-100.00%
Total Obligations	0.00	2.98	1.00	-1.98	-66.39%

Purpose, Accomplishments, Future Objectives:

The CEA universal encryption 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 a 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 the CEA Universal Encryption investment, the Department supports initiatives that work toward full achievement of 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.

The FY 2025 President's Budget includes $1 million for Treasury's CEA Universal Encryption investment with alignment to the NIST Cybersecurity Framework priorities:

- Protect the Delivery of Critical Infrastructure Services Goal: Develop and implement appropriate safeguards to ensure delivery of critical services.

In FY 2025, CEA – Universal Encryption investment is targeted to the Department's universal encryption 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.

Treasury is looking to support the following initiatives with final FY 2025 appropriations:

- Investment in Quantum-Resistant Cryptography that could protect the Department against cryptanalytic attacks by a quantum computer.

Looking forward, CEA investments will aim to accomplish the below future objectives:

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

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 to 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 2023 Actuals	FY 2024 Estimated Obligations	FY 2025 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	14.81	33.10	12.80	-20.30	-61.33%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	12.27	9.20	42.00	32.80	356.52%
Total Obligations	27.08	42.30	54.80	12.50	29.55%

Purpose, Accomplishments, Future Objectives:

The CEA zero trust architecture 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 a 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 the Zero Trust Architecture investment, Treasury seeks 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 to 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. Treasury leverages the Zero Trust Architecture 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.

The FY 2025 President's Budget includes $54.8 million for Treasury's CEA Zero Trust Architecture investment with alignment to the NIST Cybersecurity Framework priorities:

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

In FY 2025, CEA – Zero Trust Architecture investments are targeted to the Department's zero trust 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.

Treasury is looking to support the following initiatives with final FY2025 appropriations:

- Expansion of Treasury's cyber threat intelligence platform to include additional cyber threat intelligence feeds, additional material from existing feeds, and expand access to platform capabilities and shared data.
- Implementation of a TSSSOC lateral scanning capability across enterprise application and centralized incident response
- Acquisition of an enterprise Endpoint Detection and Response (EDR) solution
- Investment in Organizational Resiliency and the associated human capital component necessary to implement zero trust architecture across the Department's IT systems
- Bureau implementation of zero trust architecture
- Development or acquisition of Security Operations Center (SOC) services for the Treasury Security Data Network
- Expansion of Treasury's mobile Secret Internet Protocol Router (SIPR) capability
- Enterprise-wide vulnerability management efforts including the establishment of an enterprise penetration testing shared service offering and acquisition of a vulnerability management tool to track and conduct analysis of enterprise-wide critical vulnerabilities
- Development of application threat modeling capabilities to prepare for increasing resilience of systems and robustness of testing.

Looking forward, CEA investments will aim to accomplish the below future objectives:

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

HR LoB - HRConnect

Description:

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

Investment Obligations: (In Millions of $):

Type	FY 2023 Actuals	FY 2024 Estimated Obligations	FY 2025 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	12.28	18.59	18.87	0.28	1.51%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	37.14	37.05	38.26	1.21	3.27%
Total Obligations	49.42	55.64	57.13	1.49	2.68%

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.

HRConnect Top FY 2023 Accomplishments:

1. Implemented 74 HRConnect change requests to maintain regulatory compliance, improve the employee and manager experience, and provide tools to streamline and enable efficient processing for HR Specialists.
2. Maintained a steady state of 100% availability for customers.
3. Treasury HRLOB implemented multifactor authentication (MFA) for all TSSC applications and achieved M-21-31 compliance for the HRConnect High Value Asset (HVA).
4. Completed the migration of HRConnect’s data service, Workforce Analytics from on prem data centers to a FedRAMP High secure cloud hosted environment, effectively scaling and maturing the platform.
5. Delivered Integrated Talent Management (ITM) and HRConnect real-time performance plan and learning data integration.
6. Implemented new Remote/Telework Agreement Type and Program and Project Job Identifier fields and Mass Update Process, 34K positions updated.
7. Streamlined the background investigation security process across Treasury by expanding the Adjudication Tracker application to three additional bureaus.
8. Continued to modernize HRConnect delivering enhancements to improve the user experience for employees, managers, and HR Specialists.
9. Deployed a visual representation of key Time to Hire (T2H) metrics via the Treasury Workforce Dashboard to track and optimize the hiring timeline and make data-driven hiring decisions.
10. Continued employee self-service (ESS) redesign leveraging fluid concepts.
11. Supported gender identity and other preferred name representation in accordance with management directives.

Enterprise API Service Platform [MuleSoft]: Transition 15+ partners to the new API Service Framework. Launched integrations between USAS to DO and FinCEN Adjudication Tracker, ARC-FS Worklist API and SAM.gov integration to HRC to update vendor information.
In FY2023: Treasury Office of the Chief Information Officer (OCIO) recently assumed responsibility for the management of the transformation of Internal Revenue Service (IRS) Human Resource Information Technology (HRIT) applications in support of the Inflation Reduction Act. This transfer of responsibility allows the IRS CIO to focus their efforts on improving the taxpayer experience leveraging the Treasury OCIO's shared services and common platforms to facilitate the modernization of IRS HRIT systems, the rationalization pillars include: HRConnect, Integrated Talent Management, USA Staffing, Enterprise Data Management, and the Employee Portal.

A few of technical improvements, included: Nessus implementation, CAST implementation, piloted the transition of 3 environments to Oracle Managed Services compartment in Q3, improved the fire wall configurations and finalized the closure of the Memphis and Martinsburg HRC footprint.

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 2023 Actuals	FY 2024 Estimated Obligations	FY 2025 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	43.07	75.94	75.98	0.04	0.05%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	81.62	78.99	80.95	1.96	2.48%
Total Obligations	124.69	154.93	156.93	2.00	1.29%

Purpose, Accomplishments, Future Objectives:

The TEICAM Business Case consolidates funding that supports Treasury's implementation of HSPD-12, FICAM and 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 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/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) CDM II-PRIV/CRED Management
    - Continue working with the Managed Service Bureaus and Non-Managed Service Bureaus on implementation of Credential (CRED) and Privileged Access Management (PAM)
    - On-board new bureaus, such as IRS and DO Orbit Organizations (TSSOC, OFR, etc.), to the enterprise CDM Managed Service Offering (MSO)
    - Continue working with DHS CISA on the integration activities for the Federal Dashboard for Treasury's CDM Data reporting
2) Plan, test, & implement the issuance of version 8.1 PIV cards (PIV V8.1) across the enterprise in FY21-FY24
3) Expand usage of the Enterprise Derived Credential issuance capability to support authentication to Treasury services/infrastructure from mobile devices across Treasury in FY21-FY24
4) As part of the PIV-I solution, implement an application programming interface (API) connection between a Fiscal Service application used to capture applicant data and HRConnect in FY21-FY24
5) Implement an enterprise Hardware Security Module (HSM) as a service in FY22-FY24
6) Enterprise solution for tracking and monitoring the Only Locally Trusted (OLT) PKI certificates generated and in use within each bureau
7) Plan, design, and implement a modernized Treasury Enterprise Federation Service (TEFS) solution that enforces multifactor authentication and aligns with the Treasury Zero Trust Architecture (ZTA)
8) 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% PIV card issuance rate and providing replacements for the PIV in time sensitive activities;
- Maintained 100% PIV required privileged account access and 97% PIV required unprivileged access;
- CDM II privileged access management is operating with a cloud infrastructure and production at four bureaus performing O&M functions; we have commenced technical work on bringing the IRS on as the fifth and largest managed service customer;
- Treasury Enterprise Federation Service (TEFS) onboarded 12 new customers and integrated with third-party identity providers to expand citizen services and access;
- Executed a Treasury-wide BPA for citizen authentication services access to the entire enterprise, allowing for secure and fast public access to Treasury systems;
- Developed an alternative authentication solution and deployed it within 6 weeks to ensure continuity of government during the pandemic;
- Implemented a hardware security module (HSM) as a service for the Derived PIV solution and DO.

- Implementation of the department-wide PKI Only Locally Trusted (OLT) monitoring solution.

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 2023 Actuals	FY 2024 Estimated Obligations	FY 2025 Estimated Obligations	Change in $	% Change
Sub-Total DME Obligations (Including Internal labor (Govt. FTE))	9.79	3.55	5.55	2.00	56.25%
Sub-Total O&M Obligations (Including Internal Labor (Govt. FTE))	0.00	0.00	0.00	0.00	0.00%
Total Obligations	9.79	3.55	5.55	2.00	56.25%

Purpose, Accomplishments, Future Objectives:

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

Treasury’s three-step long-term strategy to continue to maintain and modernize its owned spaces: (1) secure the building’s outer envelope; (2) conduct a condition assessment to identify additional needs associated with the buildings’ continual aging and deferred maintenance; and (3) based on this assessment, conduct a holistic modernization of the building’s systems and infrastructure. Targeted investments address life safety and code compliance issues, reduce building systems risk by upgrading outdated systems, and bring both facilities into alignment with current building standards. Absent full funding to perform a complete repair and renovation of these historical buildings, available funding will be used to correct the most urgent issues. These investments are being executed with the expectation that were Treasury to pursue a full renovation and modernization, recent investments could be largely retained, achieving cost savings over the long term. These investments support a safe and healthy work environment that meets Treasury operational requirements. Project needs are mission focused and prioritized based on life-safety, security, code discrepancies, and needs that pose significant financial risk if not addressed in a timely manner.

Treasury Operations has continued to strategically focus on restoring the health of the building envelope (shell), to correct the deteriorating building structure and infrastructure. Components of the

Main Treasury building that have been repaired, replaced, or funded include new roofs (FY 2019/2021) and repairs to 40 percent of the windows (FY 2015/2017). The Freedman's Bank Building components that have been repaired, replaced, or funded/planned include new roofs (FY 2017/2019), domestic water line (FY 2020/2022), and replacement of all windows (FY 2009/2011). Funding and completion of these exterior items represent significant progress towards the preservation of the two buildings, maintaining a safe and healthy workplace, and reducing damage to the interior plaster and paint. The contract for the first phase (west façade) of the Main Treasury exterior restoration project was awarded late in FY 2021 and completed during FY 2022. Exterior restoration work continued through 2023 with the completion of phase 2 (south) and phase 3 (north) north façades. In FY 2024, assuming adequate funding, Phase 4 work will commence and, in FY 2025, with this requested funding, work on Phase 5 will commence.

The MT Building houses the entire chilled water plant for the Main Treasury Complex. A five cell cooling tower feeds four water cooled centrifugal chillers providing a total cooling capacity of 2,050 tons. The chillers are located in a mechanical room under the northwest lawn. The four chillers provide over 98% of the cooling required for the entire Treasury Headquarters complex; therefore, the plant is operated 24/7, 365 days per year. The Freedman's Bank Building (FBB) does not generate chilled water but rather uses chilled water from the main plant distributed by a dedicated secondary chilled water pump which serves most air handling units directly. The Chilled Water System is over 30 years old and has a wide variety of repair needs including bearings, motors, valves, distribution piping, insulation, controls, and other repairs. The system has redundancy for repairs. However, with all of the components aging at the same time the occurrence of repair needs combined with the time to repair diminishes the reliability of the redundant capacity. It is imperative that these items are repaired/replaced before the available redundancy is lost. A system breakdown would indefinitely shutdown the Treasury Complex's daily operations. This first-year cost of a multi-year project includes design for this effort.

There is currently a backlog of damaged paint and plaster as well as frayed carpet throughout MT and FBB. Some of the paint and plaster damage is due to water intrusion. These funds will supplement other funding to address the backlog in repairing these problems and implementing a regular schedule of maintenance. The damaged paint and plaster are unsightly and pose potential health and safety risks, while the frayed carpet is a safety hazard.