Department of the Treasury Cybersecurity Enhancement Account

Congressional Budget Justification and Annual Performance Plan and Report

FY 2025

Table of Contents

Section I – Budget Request

A – Mission Statement

To maintain a strong economy by promoting conditions that enable equitable and sustainable economic growth at home and abroad, combating threats to and protecting the integrity of the financial system, and managing the U.S. Government's finances and resources effectively. A secure, reliable, and resilient technical ecosystem at Treasury is critical to the agency mission. While Treasury has historically benefited from maintaining a modest public presence, our role in geopolitical affairs and the global financial system has garnered interest from criminal and nation state threat actors. Treasury must therefore continue to make strategic investments in reducing operational and reputational risks to its applications, platforms, and infrastructure, as intrusions and disruptions have great potential to impose organizational harm.

B – Summary of the Request

The FY 2025 President's Budget request of $150 million for the Cybersecurity Enhancement Account (CEA) was formulated to support the Department's continued efforts focused on operational risk reduction. The request includes $6 million for bureau-specific investments for mission-specific needs that must be achieved to integrate with Treasury's enterprise cybersecurity services. Guiding Treasury's FY 2025 request are the milestones articulated in Executive Order 14028 (EO 14028), *Improving the Nation's Cybersecurity*, as well as the numerous Office of Management and Budget (OMB) memorandums including M-21-31 *Improving the Federal Government's Investigative and Remediation Capabilities*, M-22-09 *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* and M-23-18 *Defending Critical Infrastructure and Shaping Market Forces to Drive Security and Resilience*. The FY 2025 request also supports compliance efforts associated with Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) guidance that sets new cybersecurity standards and objectives. These new directives also prioritize cloud-based security, security operations center (SOC) enhancements, and security logging.

Consistent with prior year funding, the CEA will be used as a centralized account for the design, development, and evolution of enterprise-wide cybersecurity capabilities and services. An enterprise approach allows Treasury to enhance efficiency, communication, transparency, and accountability around the mission. A cross-cutting approach to managing the CEA investments allows the Department to elevate the importance of the associated technical initiatives and provide Treasury leadership, OMB, and Congress with a more holistic vantage point of cybersecurity activities across the Department. The investments within the CEA continue to align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Treasury also aligns its investments to OMB-driven initiatives to ensure traceability between funding outlays and concrete outcomes.

1.1 – Appropriations Detail Table

Dollars in Thousands

Appropriated Resources	FY 2023 Operating Plan		FY 2024 Annualized CR		FY 2025 Request		FY 2024 to FY 2025 % Change	
New Appropriated Resources	**FTE**	**AMOUNT**	**FTE**	**AMOUNT**	**FTE**	**AMOUNT**	**FTE**	**AMOUNT**
Cybersecurity Enhancement Account	13	$100,000	34	$100,000	34	$150,000	0.0%	50.0%
Subtotal New Appropriated Resources	**13**	**$100,000**	**34**	**$100,000**	**34**	**$150,000**	**0.0%**	**50.0%**
Other Resources								
Recoveries from Prior Years	0	$71	0	$0	0	$0	NA	NA
Unobligated Balances from Prior Years	0	$57,461	0	$86,612	0	$86,000	NA	-0.7%
Subtotal Other Resources	**0**	**$57,532**	**0**	**$86,612**	**0**	**$86,000**	**NA**	**-0.7%**
Total Budgetary Resources	**13**	**157,532**	**34**	**$186,612**	**34**	**$236,000**	**0.0%**	**26.5%**

Note: FY 2023 Other Resources and Full-time Equivalents (FTE) reflect actuals.

1.2 – Budget Adjustments Table

Dollars in Thousands

	FTE	Amount
FY 2024 Annualized CR	**34**	**$100,000**
Changes to Base:		
Non-Recurring Costs		($17,293)
Maintaining Current Levels (MCLs):		**$2,236**
Pay Annualization (2024 5.2% average pay raise)		$76
Pay Raise (2025 2.0% average pay raise)		$89
Non-Pay (2025 2.2% non-pay inflation)		$2,071
Subtotal Changes to Base		($15,057)
FY 2025 Current Services	**34**	**$84,943**
Program Changes:		
Program Increases (DME):		**$65,057**
Enterprise Specific Investments		**$59,057**
Security Logging Requirements		$29,409
Zero Trust Architecture		$12,800
Cloud Adoption		$9,800
Other Cybersecurity Priorities		$6,048
Universal Encryption		$1,000
Bureau Specific Investments		**$6,000**
Cloud Adoption - Bureau of the Fiscal Service		$6,000
Subtotal Program Changes	**0**	**$65,057**
FY 2025 President's Budget Request	**34**	**$150,000**

C – Budget Increases and Decreases Description

Non-Recurring Costs ……..……. -$17,293,000 / -0 FTE

This amount represents non-recurring initial investments for key elements that are one-time in nature and thus sunset into FY 2025. This includes but are not limited to application migrations to the cloud, low code adoption and the wind-down of implementation activities that leveraged contractor resources (i.e., vulnerability disclosure program, application DevOps, application cyber resources, application security testing) or are related to projections for lower O&M costs (cloud security enhancements, fraud management).

Maintaining Current Levels ……+$2,236,000 / +0 FTE
Pay Annualization, (5.2% in 2024) +$76,000 / +0 FTE
Funds are requested for annualization of the 2024 5.2 percent average pay raise.

Pay Raise, (2.0% in FY 2025) +$89,000 / +0 FTE
Funds are requested for a 2.0 percent average pay raise in January 2025.

Non-Pay, (2.2% in FY 2025) +$2,071,000 / +0 FTE
Funds are requested for non-labor expenses such as travel, contracts, rent, supplies, and equipment.

Program Increases ……+$65,057,000 / +0 FTE
Security Logging, +$29,409,000 / +0 FTE
This FY 2025 investment will support Treasury's compliance with the security logging requirements outlined in OMB Memorandum M-21-31, which requires all logs to be accessible and visible for the highest-level operations center at the Department. This will require a scaling up of the cloud-based logging environment used by the Treasury Shared Services Security Operations Center (TSSSOC) to receive, store, analyze, and process security event and system logs from all Treasury offices and bureaus as well as nearly 40 Treasury shared services. With this investment, Treasury will:

- Create and monitor traps for detecting data-stream disruption.
- Implement a virtual, cloud-based facility to store and share the logs with external parties.
- Provide storage and retention for log data consistent with OMB Memorandum M-21-31 requirements.
- Analyze logs in real time to detect attacks and other activities of interest.
- Develop automated hunt and incident response playbooks that take advantage of security, orchestration, automation, and response capabilities.
- Create and implement a user behavioral analytics capability to allow for early detection of malicious behavior on all user and non-user accounts. This requires machine learning and artificial intelligence techniques to detect anomalous user actions and help combat advanced threats.

This investment is critical for Treasury's compliance with OMB Memorandum M-21-31 to successfully secure Treasury information technology systems.

Zero Trust Architecture Implementation, +$12,800,000 / +0 FTE
Zero Trust Architecture (ZTA) seeks to minimize implicit trust and reinvigorate least privilege. The ZTA approach is a paradigm shift from verifying once at the perimeter to continual verification of each user, device, application, and transaction. The impacts of the transition to ZTA are significant—not just technology reconfiguration but also adjusting our operating models to a new approach to risk management. Philosophically, we think of ZTA as:

- Enabling a new default security posture using the practice of "never trust, always verify" across the entire technology stack.
- Altering our approach for access enforcement, leveraging granular policies to assess the user identity, user device, and the categorization of the data before making an access decision.
- Shifting from defending the "macro attack surface" to the "micro protect surface."

For FY 2025, Treasury continues to design, implement, and operate a new generation of ZTA-aligned IT services, functions, and systems. Funding will support this program and include the following investments, noting that this list is subject to change to meet newly issued requirements:

- Consistent, robust, and scalable Treasury-wide ZTA with a focus on integration with Treasury cybersecurity architecture.
- Enhanced capabilities to detect and manage compromise, data exfiltration, malicious activity, and ransomware.

The FY 2025 investment in ZTA supports work towards a compliant Zero Trust maturity model. This large-scale investment approach requires Treasury to enhance visibility and threat identification at the application level to improve its ability to support continuous threat analysis, detection, response, and enable the analysis of encrypted traffic. Compartmentalization, micro segmentation, and reinforcing enforcement of continuous identity verification and access policies aligned with Zero Trust will improve the Department's resistance to fraudulent tampering of privileged accounts.

Cloud Enterprise Investment, +$9,800,000 / +0 FTE

Treasury requests FY 2025 funding for cloud enterprise cybersecurity enhancements and upgraded capabilities to meet ever growing security and compliance risks as Treasury continues to drive cloud adoption across the enterprise. With the imminent provisioning of an enterprise multi-cloud environment, Treasury will need to design, develop, and implement security patterns/guardrails to help ensure sanctioned and secure use of cloud platforms. Treasury's investment objectives in FY2025 for cloud enterprise adoption, include:

- Continued cyber enhancements for web properties (e.g., Treasury.gov, etc.) through the acquisition of dedicated security services and tolls to reduce risk of attacks through daily and proactive monitoring, increasing our ability to respond quickly, support periodic tuning, prevent DDoS attacks, and detect and mitigate script vulnerabilities.
- Maintain PaaS/SaaS solution with distinct and separate layers utilizing Acquia Cloud Platform for hosting and Drupal CMS for real-time publishing with protections to ensure high security capabilities (e.g., continuous monitoring, non-human traffic detection, etc.)
- Data, system, and application integration to support the automation of tasks and processes, to include providing modernization of legacy IT systems.
  Expanded security operations capabilities to accommodate the increased telemetry generated by cloud assets/workloads, along with developing new detection logic for cloud-specific monitoring. While we expect cloud will offer unprecedented opportunities for scalable and predictable infrastructure management, there will be both challenges and opportunities as we adapt our efforts to observe, detect, and respond to threats to our attack surface.

Other Cybersecurity Priorities, +$6,048,000 / +0 FTE

In FY 2025, Treasury will continue to make progress on ongoing critical cybersecurity investments. Continued funding of these critical investments is necessary to sustain progress made on some investments and launch new projects not previously identified.

Responding to the changing threat landscape in an interconnected environment has amplified the need for identifying and assessing the security posture of high value assets (HVAs) as well as vendors within our supply chain. Additionally, based on the complex nature of cybersecurity, ongoing maturation of these programs is necessary to enable much needed visibility into the myriad of threats, vulnerabilities, and cybersecurity risks facing our agency. These priority investments include, but are not limited to:

- Supply Chain Risk Management Enhancements
- Enterprise Cyber Risk Management
- Governance, Risk and Compliance
- High Value Assets
- Enterprise Threat and Vulnerability Management
- Vulnerability Disclosure Policy Platform
- Cyber Threat Intelligence
- Security improvements to enterprise applications
- Continued annual threat hunts in response to increased adversarial activity observed over the past year

Universal Encryption, +$1,000,000 / +0 FTE

Universal Encryption allows information and data to be encoded to prevent unauthorized access. This funding level is necessary to continue to support Treasury's commitment to fully comply with encryption protocols outlined in EO 14028 and subsidiary supporting material from OMB, CISA, NIST and other cybersecurity oversight entities.

To further protections of the internet and email traffic across its networks, Treasury uses encryption protocols to prevent adversaries from being able to intercept and capture traffic as it flows between endpoints. EO 14028 and M-22-09 prescribe a heightened level of encryption for Domain Name System (DNS) and Hypertext Transfer Protocol (HTTP) traffic that all agencies should use to increase the security of information transfer, particularly across public networks such as the Internet. This funding will continue the work that will focus on transitioning applications to use HTTP for secure communication with users.

Bureau Specific Investment, +$6,000,000 / +0 FTE

Cloud Adoption – Bureau of the Fiscal Service, +$6,000,000 / +0 FTE

The Budget request will support the Bureau of the Fiscal Service's (Fiscal Service) Mainframe and Cloud Transition Initiative to transition applications away from legacy mainframe technologies to cloud service providers. Fiscal Service will also continue to partner with the Department by leveraging $6 million through the Cybersecurity Enhancement Account (CEA) to implement modern solutions that will support the security, resiliency, and agility of these critical systems and continue to maintain the financial integrity and efficiency of our operations.

- ***High Value Assets***: Many of the Fiscal Service's HVAs are currently hosted on aging platforms based on antiquated code with cloud adoption allowing for migration of these systems to sustainable platforms.
- ***Federal Information Security Modernization Act (FISMA) Systems***: Consistent with the EO 14208, this funding will allow Fiscal Service to move 60+ FISMA systems to secure

cloud services, including Software as a Service, Infrastructure as a Service, and Platform as a Service. It will also enhance the business continuity and disaster recovery of these systems.

1.3 – Object Classification (Schedule O) Obligations

Dollars in Thousands

Object Classification	FY 2023 Actual Obligations	FY 2024 Estimated Obligations	FY 2025 Estimated Obligations
11.1 - Full-time permanent	1,682	4,500	5,250
11.5 - Other personnel compensation	115	0	0
11.9 - Personnel Compensation (Total)	**1,797**	**4,500**	**5,250**
12.0 - Personnel benefits	679	1,350	1,575
Total Personnel and Compensation Benefits	**$2,476**	**$5,850**	**$6,825**
21.0 - Travel and transportation of persons	17	0	0
23.0 - Rent, Communications and Utilities	0	5,438	8,157
25.1 - Advisory and assistance services	54,721	56,848	87,222
25.2 - Other services from non-Federal sources	0	4,183	6,275
25.3 - Other goods and services from Federal sources	1,470	2,988	4,482
25.7 - Operation and maintenance of equipment	2,067	10,771	16,157
26.0 - Supplies and materials	7	0	0
31.0 - Equipment	10,459	13,922	20,883
Total Non-Personnel	**$68,742**	**$94,150**	**$143,175**
Total Obligations	**$71,218**	**$100,000**	**$150,000**
Full-time Equivalents (FTE)	**13**	**34**	**34**

Note: Amounts reflect obligations of annually appropriated resources, carryover balances, reimbursables, and transfers.

D – Appropriations Language and Explanation of Changes

Appropriations Language	Explanation of Changes
DEPARTMENT OF THE TREASURY DEPARTMENTAL OFFICES CYBERSECURITY ENHANCEMENT ACCOUNT (INCLUDING TRANSFER OF FUNDS) *For salaries and expenses for enhanced cybersecurity for systems operated by the Department of the Treasury, $150,000,000 to remain available until September 30, 2027: Provided, That such funds shall supplement and not supplant any other amounts made available to the Treasury offices and bureaus for cybersecurity: Provided further, That of the total amount made available under this heading $6,000,000 shall be available for administrative expenses for the Treasury Chief Information Officer to provide oversight of the investments made under this heading: Provided further, That such funds shall supplement and not supplant any other amounts made available to the Treasury Chief Information Officer.* *Note.—A full-year 2024 appropriation for this account was not enacted at the time the Budget was prepared; therefore, the Budget assumes this account is operating under the Continuing Appropriations Act, 2024 and Other Extensions Act (Division A of Public Law 118-15, as amended). The amounts included for 2024 reflect the annualized level provided by the continuing resolution.*	

E – Legislative Proposals

The Cybersecurity Enhancement Account has no legislative proposals.

Section II – Annual Performance Plan and Report

A – Strategic Alignment

The CEA is focused on an enterprise approach to bolstering and securing Treasury's critical IT systems and infrastructure to prevent interruptions to the Department's strategic goals and objectives. The CEA aligns with the following Treasury strategic goals and objectives as presented in the FY 2022 - FY 2026 strategic plan:

Goal 2: Enhance National Security

- Objective 2.1 – Cyber Resiliency of Financial Systems and Institutions - Harden assets and systems of Treasury and the broader financial system to promote financial system resiliency.

B – Budget and Performance by Budget Activity

2.1.1 Cybersecurity Enhancement Account Resources and Measures

Dollars in Thousands

Resource Level	FY 2019 Actual	FY 2020 Actual	FY 2021 Actual	FY 2022 Actual	FY 2023 Actual	FY 2024 Annualized CR	FY 2025 Request
Appropriated Resources	$25,208	$20,538	$28,040	$42,073	$70,539	$100,000	$150,000
Budget Activity Total	**$25,208**	**$20,538**	**$28,040**	**$42,073**	**$70,539**	**$100,000**	**$150,000**
Full-time Equivalents (FTE)	**12**	**3**	**4**	**7**	**13**	**34**	**34**

Performance Measure	FY 2019 Actual	FY 2020 Actual	FY 2021 Actual	FY 2022 Actual	FY 2023 Actual	FY 2023 Target	FY 2024 Target	FY 2025 Target
Number of Major Incidents	0	1	1	1	2	0	DISC	DISC
Number of Reported Incidents	152	206	246	205	277	150	DISC	DISC
Enterprise Multi-Factor Authentication Adoption	N/A	N/A	N/A	N/A	N/A	N/A	B	B
Transitioning Enterprise Logging Data	N/A	N/A	N/A	N/A	N/A	N/A	B	B
Percentage of TIER I High Value Assets (HVAs) where Risk and Vulnerability Assessment (RVA) or Security Architecture Review (SAR) are Completed on Time (%)	100%	100%	100%	100%	100%	100%	100%	100%
Percentage of High and/or Critical Findings from RVAs or SARs on Tier I HVAs that are closed by the end of the FY (%)	57%	80%	80%	100%	92%	80%	80%	80%

Key: DISC - Discontinued; B - Baseline; I - Indicator

Cybersecurity Enhancement Account (CEA) Budget and Performance
($150,000,000 from direct appropriations):
The purpose of the CEA is to strategically mitigate cybersecurity risks through a centralized program with Department-wide impact. Investments support the core framework of the Department's IT infrastructure. Due to the increasing volume and sophistication of cyber-attacks, Treasury leadership continues to prioritize cybersecurity and will centralize Department-wide cybersecurity initiatives through the CEA account.

Description of Performance
Number of Major Incidents: The number of major incidents, as defined in OMB Memorandum M-19-02, reported by Treasury to Congress in a given fiscal year. This is a measure of how effective Treasury's collective defenses are at mitigating the most damaging security threats. In December 2020, Treasury notified DHS CISA of a major security incident resulting from the Department's deployment of SolarWinds Orion, a widely-used network management software. The Department has completed compromise assessments, and all SolarWinds Orion products continue to remain offline across the Treasury Enterprise environment. This measure will be discontinued in FY 2024.

Number of Reported Incidents: Treasury is constantly being targeted by a large array of threat actors, including nation states and criminal syndicates. Treasury detects and responds to these events and provides notifications of a subset of these events to the United States Computer Emergency Readiness Team at CISA for external situational awareness. Because the volume and velocity of these events is contingent upon various factors (geopolitical affairs, software vulnerabilities, new tactics/techniques), it can be difficult to forecast future impact based on year-to-year trends. This measure will be discontinued in FY 2024.

Enterprise Multi-Factor Authentication Adoption: Treasury has established this new performance measure in response to EO 14028 on "Improving the Nation's Cybersecurity." The EO directs Federal Agencies to develop and adopt stronger cybersecurity policies and practices, including fully adopting Multi-Factor Authentication (MFA). Treasury outlined a goal to implement MFA to the maximum extent feasible.

Transitioning Enterprise Logging Data: This measure will track Treasury's progress in transitioning enterprise logging data from on-premises locations to the cloud.

Percentage of High and/or Critical Findings from Risk and Vulnerability Assessments (RVAs) or Security Architecture Reviews (SARs) on Tier I High Value Assets (HVAs) that are closed by the end of the Fiscal Year (FY): This is a measure of how Treasury addresses the vulnerabilities and potentially exploitable weaknesses of its most important systems, based on its HVA assessment process. Treasury's CEA performance targets are based upon the percentage of HVA system assessments that are conducted in accordance with the HVA assessment cycle and the closure rate of resulting findings and/or Plans of Action and Milestones (POA&Ms) within the fiscal year. Treasury has consistently recorded a 100 percent completion rate for system assessments and currently has a 100 percent closure rate for associated findings and POA&Ms. This focus helps to ensure that the proper POA&Ms are in place for all assessed systems and that they are being acted upon in a timely manner. The investment will focus on remediation of

vulnerabilities, as well as increased review and reporting on corrective actions to resolve all findings and recommendations discerned during the assessment process. It was decided that the FY 2025 target should remain flat from FY 2023 levels due to the likelihood that long-term remediation efforts would be required based on findings from HVA assessments.

Section III – Additional Information

A – Summary of Capital Investments

Capital investments that support the CEA are included in the Departmental Offices plan.

A summary of capital investment resources, including major information technology and non-technology investments can be found at:
https://www.treasury.gov/about/budget-performance/Pages/summary-of-capital-investments.aspx

B - National Institute of Standards and Technology (NIST) Crosswalk

NIST crosswalks to the FY 2025 President's Budget Request:

Dollars in Thousands

NIST Reporting Categories						
CEA Investments	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**	**Total**
Zero Trust Architecture	**4,500**	**40,200**	**7,500**	**2,600**	-	**54,800**
Security Logging	-	**32,325**	-	**9,000**	-	**41,325**
Other Cybersecurity Priorities	**17,235**	**5,150**	-	**2,565**	-	**24,950**
Cloud Adoption	**2,150**	**15,375**	-	**500**	**1,400**	**19,425**
Multi-Factor Authentication	-	-	**2,500**	-	-	**2,500**
Universal Encryption	-	**1,000**	-	-	-	**1,000**
Bureau Specific Investments	-	**6,000**	-	-	-	**6,000**
BFS- Cloud Adoption		*6,000*				**6,000**
Grand Total	**23,885**	**100,050**	**10,000**	**14,665**	**1,400**	**150,000**