Department of the Treasury Cybersecurity Enhancement Account

Congressional Budget Justification

FY 2026

Table of Contents

Section I – Budget Request

A – Mission Statement

To maintain a strong economy by promoting conditions that enable 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. Treasury's role in geopolitical affairs and the global financial system has garnered immense interest from criminal and nation state threat actors. Treasury must therefore make strategic investments in consolidation of cybersecurity across the Department and continue 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 2026 President's Budget request of $59 million for the Cybersecurity Enhancement Account (CEA) was formulated to sustain the Department's progress in reducing operational risk. The FY 2026 request supports implementing cybersecurity best practices, standards and objectives provided by the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). These directives also prioritize cloud-based security, security operations center (SOC) enhancements, and security logging. The premise of this request is also guided by the Administration's goal of reducing the national debt and realizing savings and efficiencies, supported via the consolidation of cybersecurity activities across the Department.

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 strategy 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.

Table 1.1 – Appropriations Detail

Dollars in Thousands

Appropriated Resources	FY 2024 Operating Plan		FY 2025 Operating Plan		FY 2026 Request		FY 2025 to FY 2026 % Change	
New Appropriated Resources	**FTE**	**AMOUNT**	**FTE**	**AMOUNT**	**FTE**	**AMOUNT**	**FTE**	**AMOUNT**
Cybersecurity Enhancement Account	20	$194,800	28	$36,500	28	$59,000	0.0%	61.6%
Subtotal New Appropriated Resources	**20**	**$194,800**	**28**	**$36,500**	**28**	**$59,000**	**0.0%**	**61.6%**
Other Resources								
Unobligated Balances from Prior Years	0	$86,313	0	$218,979	0	$218,979	NA	0%
Subtotal Other Resources	**0**	**$86,313**	**0**	**$218,979**	**0**	**$218,979**	**NA**	**0%**
Total Budgetary Resources	**20**	**$281,113**	**28**	**$255,479**	**28**	**$277,979**	**0.0%**	**8.8%**

Table 1.2 – Budget Adjustments

Dollars in Thousands

	FTE	Amount
FY 2025 Enacted	**28**	**$36,500**
Changes to Base:		
Maintaining Current Levels (MCLs):	0	$34
Pay Annualization (FY 2025 2.0% average pay raise)	0	$34
Subtotal Changes to Base	0	$34
FY 2026 Current Services	**28**	**$36,534**
Program Changes:		
Program Efficiencies	**0**	**(34)**
Absorption of MCLs	0	(34)
Program Increases	**0**	**$22,500**
Cloud Adoption	0	$229
Other Cybersecurity Priorities	0	$7,716
Security Logging Requirements	0	$8,268
Zero Trust Architecture	0	$6,287
Subtotal Program Changes	**0**	**$22,466**
FY 2026 President's Budget Request	**28**	**$59,000**

C – Budget Increases and Decreases Description

Maintaining Current Levels (MCLs) .....+$34,000 / +0 FTE

Pay Annualization (2.0% in 2025) +$34,000 / +0 FTE

Funds are requested for annualization of the January 2025 2.0% average pay raise.

Program Efficiencies..... -$34,000 / 0 FTE

Absorption of MCLs -$34,000 / +0 FTE:

CEA will absorb the MCLs.

Program Increases .....+$22,500,000 / +0 FTE

Cloud Enterprise Investment +$229,000 / +0 FTE

Treasury requests FY 2026 funding for cloud enterprise cybersecurity operations required to meet growing security risks, as Treasury continues to drive cloud adoption across the Department, promote consolidation in the enterprise multi-cloud environment, and drive enhancements to web properties. Treasury's investment objectives in FY2026 for cloud enterprise adoption include:

- Strengthened web security through dedicated services and proactive website monitoring, reducing attack risks like DDoS and script vulnerabilities while ensuring swift response capabilities.

Other Cybersecurity Priorities +$7,716,000 / +0 FTE

For FY 2026, the Department of the Treasury requests funding to support critical cybersecurity initiatives that do not align directly with other CEA categories. As Treasury continues efforts to consolidate commodity technology across the Department—aimed at strengthening the Department's cybersecurity risk posture and streamlining operations—this request includes funding for the operation of an enterprise-wide Configuration Management Database (CMDB), an enterprise-wide Governance, Risk, and Compliance (GRC) platform, and contract

consolidation, among other priorities. Given the complexity of cybersecurity, ongoing program maturation is essential to enhance visibility into threats, vulnerabilities, and security risks impacting the Department. Priority investments include, but are not limited to:

- Governance, Risk, and Compliance
- Enterprise Configuration Database
- Incident Response

Security Logging +$8,268,000 / +0 FTE

Treasury requests FY 2026 funding to sustain existing security logging capabilities and continue to enhance compliance with OMB memorandum M-21-31, ensuring all logs are accessible and visible to the department's highest-level operations center. This requires scaling the cloud-based logging environment used by the Treasury Shared Services Security Operations Center (TSSSOC) to efficiently receive, store, analyze, and process security event and system logs across all Treasury offices, bureaus, and Treasury shared services.

Zero Trust Architecture Implementation +$6,287,000 / +0 FTE

Zero Trust Architecture (ZTA) seeks 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. 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" (e.g., consolidation of duplicative information technology systems).

For FY 2026, Treasury plans to sustain 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:

- Operations for Treasury's Enterprise Endpoint Detection and Response solution.
- Security Operations Center for the Treasury Secure Data Network (TSDN).
- Enhanced capabilities to detect and manage compromise, data exfiltration, malicious activity, and ransomware.

The CEA will continue to be used as a centralized account for the design, development, and evolution of enterprise-wide cybersecurity capabilities and services so as the Department continues ongoing reviews of the cyber posture, funds may need to be reallocated to address emerging threats.

Table 1.3 – Object Classification (Schedule O) Obligations

Dollars in Thousands

Object Classification	FY 2024 Actual Obligations	FY 2025 Estimated Obligations	FY 2026 Estimated Obligations
11.1 - Full-time permanent	3,108	4,444	4,444
11.9 - Personnel Compensation (Total)	**3,108**	**4,444**	**4,444**
12.0 - Personnel benefits	1,118	1,328	1,328
Total Personnel and Compensation Benefits	**$4,226**	**$5,772**	**$5,772**
21.0 - Travel and transportation of persons	27	0	0
23.3 - Communications, utilities, and miscellaneous charges	0	5,203	9,013
25.1 - Advisory and assistance services	35,346	15,235	15,869
25.2 - Other services from non-Federal sources	0	850	5,825
25.3 - Other goods and services from Federal sources	10,339	1,350	6,192
25.7 - Operation and maintenance of equipment	267	3,590	7,832
26.0 - Supplies and materials	395	0	0
31.0 - Equipment	11,834	4,500	8,497
Total Non-Personnel	**$58,209**	**$30,728**	**$53,228**
Total Obligations	**$62,434**	**$36,500**	**$59,000**
Full-time Equivalents (FTE)	**20**	**28**	**28**

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, $59,000,000 to remain available until September 30, 2028: 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 $6,500,000 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.-- This account is operating under the Full-Year Continuing Appropriations and Extensions Act, 2025 (Division A of Public Law 119-4).	

E – Legislative Proposals

CEA has no legislative proposals.

Section II – 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 2026 President's Budget Request:

Dollars in Thousands

NIST Reporting Categories					
CEA Investments	**Identify**	**Protect**	**Detect**	**Respond**	**Total**
Zero Trust Architecture	**-**	**12,908,256**	**1,066,723**	**1,762,066**	**15,737,045**
Security Logging	**-**	**19,368,416**	**-**	**-**	**19,368,416**
Other Cybersecurity Priorities	**18,949,196**	**3,476,207**	**-**	**690,516**	**23,115,919**
Cloud Adoption	**-**	**778,620**	**-**	**-**	**778,620**
Grand Total	**18,949,196**	**36,531,499**	**1,066,723**	**2,452,583**	**59,000,000**

Total amounts for each NIST category include the allocation of base resources $36.534M.