Cybersecurity Enhancement Account

Program Summary by Budget Activity

Dollars in Thousands

Budget Activity	FY 2024 Operating Plan	FY 2025 Operating Plan	FY 2026 Request	FY 2025 to FY 2026 $ Change	FY 2025 to FY 2026 % Change
Cybersecurity Enhancement Account	$194,800	$36,500	$59,000	$22,500	62%
Subtotal, Organization Title	**$194,800**	**$36,500**	**$59,000**	**$22,500**	**62%**
Unobligated Balances from Prior Years	$86,313	$218,979	$218,979	$0	0%
Subtotal Other Resources	**86,313**	**$218,979**	**$218,979**	**$0**	**0%**
Total Budgetary Resources	**$281,113**	**$255,479**	**$277,979**	**$22,500**	**8.8%**
Direct FTE	20	28	28	0	0%
Total Full-time Equivalents (FTE)	**20**	**28**	**28**	**0**	**0%**

Summary

The FY 2026 President's Budget request of $59 million for the Cybersecurity Enhancement Account (CEA) was formulated to support the Department's continued efforts focused on operational risk reduction. The FY 2026 request also supports implementing cybersecurity best practices, standards and objectives provided by the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). These new directives also prioritize cloud-based security, security operations center (SOC) enhancements, and security logging.

Consistent with prior years, 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.

Budget Highlights

Dollars in Thousands

	FTE	Amount
FY 2025 Operating Plan	**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**

Budget Adjustments

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. While cloud infrastructure offers scalability and predictability, ongoing challenges require adaptive strategies to observe, detect, and respond effectively to evolving threats. Treasury's investment objectives in FY2026 for cloud enterprise adoption include:

- Strengthening web security through dedicated services and proactive 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, Treasury requests funding to address critical cybersecurity projects that do not fit neatly into one of the other categories. As Treasury plans to further consolidate commodity technology across the Department to improve Treasury's cybersecurity risk posture and streamline cybersecurity operations, our request includes funding for operations of an enterprise-wide Configuration Management Database (CMDB), an enterprise-wide Governance, Risk, and Compliance (GRC) platform, and contract consolidation, among others. Given the complex nature of cybersecurity, continuous program maturation is necessary to enhance visibility into threats, vulnerabilities, and security risks affecting the agency. 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 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" (e.g., consolidation of duplicative information technology systems).

For FY 2026, Treasury continues 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.

Legislative Proposals

CEA has no legislative proposals.