Cybersecurity Enhancement Account

Program Summary by Budget Activity

Dollars in Thousands

Budget Activity	FY 2025 Operating Plan	FY 2026 Enacted	FY 2027 Request	FY 2026 to FY 2027 $ Change	FY 2026 to FY 2027 % Change
Cybersecurity Enhancement Account	$36,500	$59,000	$59,000	0	0%
Subtotal, Cybersecurity Enhancement Account	**$36,500**	**$59,000**	**$59,000**	**0**	**0%**
Unobligated Balances from Prior Years	$218,979	$156,056	$89,148	(66,909)	-43%
Prior Year Recoveries	$0	$500	$500	0	0%
Subtotal Other Resources	**$218,979**	**$156,056**	**$89,148**	**(66,909)**	**-43%**
Total Budgetary Resources	**$255,479**	**$215,056**	**$148,148**	**(66,909)**	**-31%**
Direct FTE	28	68	68	0	0%
Total Full-time Equivalents (FTE)	**28**	**68**	**68**	**0**	**0%**

Note: FY 2025 Other Resources and Full-time Equivalents (FTE) reflect actuals.

Summary

The FY 2027 President's Budget request of $59 million for the Cybersecurity Enhancement Account (CEA) was formulated to support the maturation of cybersecurity protections, consolidation efforts and tools implementing cybersecurity best practices, standards and objectives provided by the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). CEA also continues to align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and investments to OMB-driven initiatives to ensure traceability between funding outlays and concrete outcomes.

Funding through CEA continues to be essential in supporting the Department's ability to combat threats and increase operational resilience of systems to ensure continued execution of our mission. In FY 2026, under the leadership of the Treasury Chief Information Officer (CIO), the Department is enhancing its specialized technology capabilities through the formation of an Engineering Center of Excellence (CoE). The goal is to instill the engineering rigor that underpins all AI and emerging technology adoption efforts that Treasury's systems require to meet mission, cybersecurity, and performance requirements using best practices including Agile, Development, Security and Operations (DevSecOps), and Digital Engineering.

The FY 2026 base adjustment includes funding to support engineering positions (+40 limited term positions) within the CoE to accelerate its secure technology initiatives by delivering and improving cybersecurity of the technology solutions departmentwide. The investment is estimated at $10 million, which would be absorbed within current levels by reducing the CIO's dependency on contractor support thus lowering contract expenditures. Treasury will continue to build its capacity to combat sophisticated cyber threats by maturing security operations, reducing risk exposure, and increasing operational resilience.

Budget Highlights

Dollars in Thousands

	FTE	Amount
FY 2026 Enacted	**28**	**$59,000**
Changes to Base:		
Other Adjustment		
Artificial Intelligence/Cyber Engineers - Treasury Engineering Center of Excellence	40	$10,000
Realignment of non-labor resources	0	($10,000)
Maintaining Current Levels (MCLs):	0	$15
Pay Annualization (FY 2026 1.0% average pay raise)	0	$15
Subtotal Changes to Base	40	$15
FY 2027 Current Services	**68**	**$59,015**
Program Changes:		
Program Efficiencies	0	($15)
Absorption of MCLs	0	($15)
Subtotal Program Changes	0	($15)
FY 2027 President's Budget Request	**68**	**$59,000**

Note: Support for the engineering staff will be absorbed through the realignment of funds related to reduced contract spending.

Budget Adjustments

Changes to Base…… +0 / +40 FTE

Artificial Intelligence/Cyber Engineers – Treasury Engineering Center of Excellence +$10,000 / + 40 FTE

The FY 2026 base adjustment includes funding to support engineering positions (+40 limited term positions) within the CoE to accelerate its secure technology initiatives by delivering and improving cybersecurity of the technology solutions departmentwide. The investment is estimated at $10 million.

Realignment of non-labor resources -$10,000 / -0 FTE

The CoE investment of an estimated $10 million will be absorbed within current levels by reducing the CIO's dependency on contractor support thus lowering contract expenditures. Treasury is driving cost effectiveness through consolidation efforts and eliminating redundancies.

Maintaining Current Levels (MCLs) .....+$15,000 / +0 FTE

Pay Annualization (1.0% in 2026) +$15,000 / +0 FTE

Funds are requested for annualization of the January 2026 1.0% average pay raise.

Program Efficiencies .....-$15,000 / -0 FTE

Absorption of MCLs -$15,000 / -0 FTE:

CEA will absorb the MCLs

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

Security Logging +$13,271,000 / +0 FTE

Treasury requests FY 2027 funding to continue consolidation efforts for the Security Operation Centers (SOCs) across Treasury. Security logging is vital to collecting, storing, and analyzing logs that help detect, investigate, and respond to security events. These efforts would enhance compliance with OMB memorandum M-21-31, ensuring all logs are accessible and visible to the department's highest-level operations center. Logging and incident response capabilities improvements require scaling the cloud-based logging environment used by the Treasury Shared Services Security Operations Center (TSSSOC) to operate efficiently and process security events and system logs across all Treasury offices, bureaus, and Treasury shared services.

Other Cybersecurity Priorities +$4,498,000 / +0 FTE

For FY 2027, 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

Zero Trust Architecture Implementation +$2,816,000 / +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. For FY 2027, Treasury plans to sustain ZTA-aligned IT services, functions, and systems. Funding will support work spanning across the five ZTA pillars (Identify, Device, Network, Application and Workload, and Data) established through NIST and CISA's Zero Trust Maturity Model. Treasury investments include the following areas:

- 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.

Cloud Enterprise Investment +$1,915,000 / +0 FTE

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

Legislative Proposals

CEA has no legislative proposals.

Performance Highlights

Performance Measure	FY 2023 Actual	FY 2024 Actual	FY 2025 Actual	FY 2026 Target	FY 2027 Target
Enterprise Multi-Factor Authentication Adoption	N/A	86	91	91	92
Transitioning Enterprise Logging Data	N/A	2.4PB	3.0PB	3.6PB	4.2PB
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
Percentage of High and/or Critical Findings from RVAs or SARs on Tier I HVAs that are closed by the end of the FY (%)	92	100	100	80	80

Key: NA – Not Applicable

Note: Enterprise MFA Adoption and Transitioning Enterprise Logging Data metrics were baselined in FY 2024. Petabytes of data (PB)

Description of Performance

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.

Enterprise Multi-Factor Authentication Adoption: Treasury has established this 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. In FY 2025, coordination with bureau stakeholders throughout Treasury was able to achieve significant data normalization through decommissioning and consolidation of systems to align with Treasury MFA objectives. Additionally, in FY2025 more systems integrated with the Treasury Enterprise Authentication Service (TEAS) than originally projected further supporting exceeding the original MFA target.

Transitioning Enterprise Logging Data: This measure will track Treasury's progress in transitioning enterprise logging data from bureau locations to the cloud. FY 2025 growth driven by adherence to OMB-21-31 and Congressional Cloud First mandates.

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 2026 and FY 2027 targets should remain flat from FY 2025 levels due to the likelihood that long-term remediation efforts would be required based on findings from HVA assessments