Cybersecurity Enhancement Account

Program Summary by Budget Activity

Dollars in Thousands

Budget Activity	FY 2023 Operating Plan	FY 2024 Annualized CR	FY 2025 Request	FY 2024 to FY 2025	
				$ Change	% Change
Cybersecurity Enhancement Account (CEA)	$100,000	$100,000	$150,000	$50,000	50%
Subtotal, CEA	**$100,000**	**$100,000**	**$150,000**	**$50,000**	**50%**
Recovery from Prior Years	$71	$0	$0	$0	NA
Unobligated Balances Brought Forward	$57,461	$86,612	$86,000	($612)	-1%
Subtotal Other Resources	**$57,532**	**$86,612**	**$86,000**	**($612)**	**-1%**
Total Budgetary Resources	**$157,532**	**$186,612**	**$236,000**	**$49,388**	**26%**
Direct FTE	13	34	34	0	0%
Total Full-time Equivalents (FTE)	**13**	**34**	**34**	**0**	**0%**

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

Summary

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 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 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**

Budget Adjustments

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 2024) +$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) enterprise logging solution 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. 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.

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 detection at the application level to improve its ability to support continuous threat analysis, detection, and 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.

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.

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.

Legislative Proposals

The Cybersecurity Enhancement Account has no legislative proposals.

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.

Performance Highlights

Budget Activity	Performance Measure	FY 2021 Actual	FY 2022 Actual	FY 2023 Actual	FY 2024 Target	FY 2025 Target
CEA	Number of Major Incidents	1	1	2	DISC	DISC
CEA	Number of Reported Incidents	246	205	277	DISC	DISC
CEA	Enterprise Multi-Factor Authentication Adoption	N/A	N/A	N/A	B	B
CEA	Transitioning Enterprise Logging Data	N/A	N/A	N/A	B	B
CEA	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%

CEA	Percentage of High and/or Critical Findings from RVAs or SARs on Tier I HVAs that are closed by the end of the FY (%)	80%	100%	92%	80%	80%

Key: DISC - Discontinued; B - Baseline

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.

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.