Cybersecurity Enhancement Account

Program Summary by Budget Activity

Dollars in Thousands

	FY 2022	FY 2023	FY 2024	FY 2023 to FY 2024	
Budget Activity	**Operating Plan**	**Operating Plan**	**Request**	**$ Change**	**% Change**
Cybersecurity Enhancement Account (CEA)	$80,000	$100,000	$215,000	$115,000	115.00%
Subtotal, CEA	**$80,000**	**$100,000**	**$215,000**	**$115,000**	**115.00%**
Recovery from Prior Years	$1,005	$0	$0	$0	0.00%
Unobligated Balances Brought Forward	$18,595	$57,461	$58,000	$539	0.94%
Subtotal, Other Resources	**19,600**	**$57,461**	**$58,000**	**$539**	**0.94%**
Total Program Operating Level	**$99,600**	**$157,461**	**$273,000**	**$115,539**	**73.38%**
Direct FTE	10	30	53	23	76.67%
Total Full-time Equivalents (FTE)	**10**	**30**	**53**	**23**	**76.67%**

Summary

The FY 2024 President's Budget request of $215 million for the Cybersecurity Enhancement Account (CEA) was formulated to support the Department's continued efforts focused on risk reduction. The request includes $45 million for bureau-specific investments related to mission-specific needs that must be achieved to integrate with Treasury's enterprise cybersecurity services.

Guiding Treasury's FY 2024 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 and M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. The FY 2024 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), which is the continued de facto industry framework for cybersecurity programs. Treasury also aligns its investments to OMB-driven initiatives, so that there is traceability between the funding outlays and concrete outcomes.

Budget Highlights

Dollars in Thousands

	FTE	Amount
FY 2023 Operating Plan	**30**	**$100,000**
Changes to Base:		
Non-Recurring Costs		($93,150)
Maintaining Current Levels (MCLs):		**$298**
Pay Annualization (4.6% average pay raise)		$67
Pay Raise (5.2% average pay raise)		$231
Subtotal Changes to Base		($92,852)
FY 2023 Current Services	**30**	**$7,148**
Program Changes:		
Program Increases:	**23**	**$207,852**
Enterprise Specific Investments:		**$163,190**
Cloud Enterprise Investment	18	$59,744
Zero Trust Architecture Implementation	2	$43,232
Security Logging		$35,448
Other Cybersecurity Priorities	3	$24,766
Bureau Specific Investments:		**$44,662**
Zero Trust Architecture - Bureau of the Fiscal Service		$30,375
Cloud Adoption - Bureau of the Fiscal Service		$11,637
Zero Trust - Alcohol and Tobacco Tax and Trade Bureau		$2,500
Other Cyber Priorities - Bureau of the Fiscal Service		$150
Subtotal Program Changes	**23**	**$207,852**
FY 2024 President's Budget Request	**53**	**$215,000**

Budget Adjustments

Changes to Base ……………………………………..………..………-$93,150,000 / -0 FTE

Non-Recurring Costs, -$93,150,000 / -0 FTE

This amount represents non-recurring initial investments.

Maintaining Current Levels ……………………………………………….+$298,000 / +0 FTE

Pay Annualization, +$67,000 / +0 FTE

Funds are requested for annualization of the FY 2023 4.6 percent average pay raise.

Pay Raise, +$231,000 / +0 FTE

Funds are requested for a 5.2 percent average pay raise in January 2024.

Program Increases ……………………………………………………+$207,852,000 / +23 FTE

Cloud Enterprise Investment, +$59,743,600 / +18 FTE

Treasury requests FY 2024 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.

In addition, the Department will need to expand its security operations capabilities to accommodate the increased telemetry generated by cloud assets/workloads, along with developing new detection logic for cloud-specific monitoring. While Treasury expects cloud will offer unprecedented opportunities for scalable and predictable infrastructure management, there will be discernible impacts on Treasury's ability to observe, detect, and respond to threats to its attack surface.

Zero Trust Architecture Implementation, +$43,231,600 / +2 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 current 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 Treasury's 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 2024, Treasury continues to understand, manage, and design a new generation of ZTA-aligned IT services, functions, and systems to meet security needs. Funding will support this program and include the following investments, noting that this list is subject to change to meet newly issued requirements:

- A consistent, robust, and scalable Treasury-wide Zero Trust Architecture with a focus on integration with the Treasury Cybersecurity Architecture.
- Enhanced capabilities to detect and manage traffic compromise, data exfiltration, malicious activity, and ransomware, with an eye toward the technical exposure from the SolarWinds incident.

The FY 2024 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.

Security Logging, +$35,448,000 / +0 FTE
This FY 2024 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 expansion of the Treasury Shared Services Security Operations Center (TSSSOC) enterprise logging solution to be able 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 facility to share the logs with CISA, the Federal Bureau of Investigation, and other authorities required.
- 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 in Treasury's pursuit to comply with OMB Memorandum M-21-31 to successfully secure Treasury information technology systems.

Other Cybersecurity Priorities, +$24,765,840 / +3 FTE

In FY 2024, 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
- HVAs
- Enterprise Threat and Vulnerability Management
- Vulnerability Disclosure Policy Platform
- Cyber Threat Intelligence
- Security improvements to our enterprise applications
- Continued annual threat hunts, to verify total eviction of the SolarWinds threat actor

Bureau Specific Investments, +$44,662,960/ +0 FTE

Zero Trust Architecture, Cloud Adoption, and Other Cyber Priorities – Bureau of the Fiscal Service, +$42,162,960 / +0 FTE

The budget request will *accelerate* the Bureau of the Fiscal Service's (Fiscal Service's) Cloud Adoption away from aging, costly platforms to low code, cloud-based architecture to, in part, remediate Fiscal Service audit deficiencies. This applies to Fiscal Service's specific portfolio of applications and systems including:

- ***HVAs***: Many of the Fiscal Service's HVAs that support the National Computer Forensic Institute are currently hosted on aging platforms based on antiquated code. For example, one of these platforms is the Fiscal Service Mainframe, which costs $45.9 million annually and carries substantial contractual costs that are anticipated to continue increasing over time.

- ***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.

Additionally, this supports:

- ***Identity Assurance:*** Common Approach to Identity Assurance licensing costs for millions of public citizens that access Fiscal Service systems each year. This investment in Zero Trust is necessary to achieve the required identity assurance levels for public-facing applications.
- ***Training:*** Necessary training on advanced cyber tools and techniques so appropriate safeguards are in place to ensure effective delivery of critical infrastructure services.

Zero Trust – Alcohol and Tobacco Tax and Trade Bureau, +$2,500,000 / +0 FTE
This budget request will improve Alcohol and Tobacco Tax and Trade Bureau's ability to detect and respond to sophisticated threats by making investments in the following areas:

- Additional endpoint detection and response licenses.
- Hardware/software to increase overall network traffic visibility, as well as to gain the capability to analyze and visualize anomalies for potential threats in the traffic; and
- Upgrade Security Information and Event Management hardware/software to allow for greater log storage retention and the ability to collect additional sources of log files for detection and forensic purposes.

Legislative Proposals

The Cybersecurity Enhancement Account has no legislative proposals.

Strategic Alignment

The CEA is focused on an enterprise approach to bolstering and security of Treasury's critical IT systems and infrastructure to meet the Department's strategic goals and objectives uninterrupted. 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.

Goal 3: Protect Financial Stability and Resiliency

- Objective 3.1 – Financial System Vulnerabilities - Identify and address current and emerging vulnerabilities to the stability of the U.S. and global financial systems to support more sustainable and equitable growth.

Performance Highlights

Performance Measure	FY 2018	FY 2019	FY 2020	FY 2021	FY 2022	FY 2022	FY 2023	FY 2024
	Actual	Actual	Actual	Actual	Actual	Target	Target	Target
Number of Major Incidents	0	0	1	1	1	0	0	DISC
Number of Reported Incidents	225	152	206	246	205	150	150	DISC
Enterprise Multi-Factor Authentication Adoption	N/A	N/A	N/A	N/A	N/A	N/A	N/A	B
Transitioning Enterprise Logging Data	N/A	N/A	N/A	N/A	N/A	N/A	N/A	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 1 HVAs that are closed by the end of the FY	N/A	57%	80%	80%	100%	75%	80%	80%

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

Description of Performance

This year, CEA is working to align budget activities and performance measures to the new objectives in the Treasury FY 2022 - FY 2026 Strategic Plan. This work will include benchmarking performance and may result in changes to performance measures in the FY 2025 budget.

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, 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. The FY 2024 request includes additional funding to mitigate weaknesses identified through the SolarWinds incident and for investments that support critical IT improvements.

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 so many different factors (geopolitical affairs, software vulnerabilities, new tactics/techniques), it can be difficult to forecast future impact based on year-on-year trends.

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 2024 target should remain flat from FY 2022 numbers due to the likelihood of findings from HVA assessments requiring long-term remediation efforts.