Cybersecurity Enhancement Account

Program Summary by Budget Activity

Dollars in Thousands

Budget Activity	FY 2021 Operating Plan	FY 2022 Annualized CR	FY 2023 Request	FY 2022 to FY 2023 $ Change	FY 2022 to FY 2023 % Change
Cybersecurity Enhancement Account (CEA)	18,000	18,000	215,000	197,000	1094.44%
Subtotal, CEA	**$18,000**	**$18,000**	**$215,000**	**$197,000**	**1094%**
Recovery from Prior Years	1,500	2,000	2,000	0	0.00%
Unobligated Balances Brought Forward	26,463	17,923	17,403	(520)	-2.90%
Total Program Operating Level	**$27,963**	**$19,923**	**$19,403**	**($520)**	**100.00%**
Direct FTE	4	10	21	11	110.00%
Total Full-time Equivalents (FTE)	**4**	**10**	**21**	**11**	**110.00%**

Summary

To support the Department's proactive and strategic approach to protecting and hardening the Treasury's Information Technology (IT) infrastructure against cyber criminals and nation state actors, the FY 2023 budget request includes $215 million for the Cybersecurity Enhancement Account (CEA) to protect and defend sensitive agency systems and information and strengthen the role of the Treasury Chief Information Officer (CIO) in identifying, responding, and protecting against cyber threats. The request supports Treasury's enterprise-wide investments, as well as $12 million for bureau specific investments that will extend and reinforce the security protections sought by CIO.

The FY 2023 Budget request provides critical cybersecurity resources to support Treasury's efforts to comply with the Executive Order 14028 (EO), Improving the Nation's Cybersecurity as well as Office of Management and Budget (OMB) Memorandums, specifically M-21-31 Improving the Federal Government's Investigative and Remediation Capabilities (security logging) and M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. CEA's funding 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, universal encryption, and multi-factor authentication (MFA).

The CEA is positioned as a centralized account to support enterprise-wide cyber services and to further enhance cyber capabilities, providing a platform to enhance efficiency, communication, transparency, and accountability around the Treasury's mission. The FY 2023 request elevates the importance of such initiatives and provides Treasury leadership, OMB, and Congress with a more holistic vantage point of cybersecurity activities across the Department. With the increase in cyber requirements and cascading deadlines, the Department is centralizing cybersecurity initiative leadership and oversight to gain operational efficiencies, ensure transparency and achieve enterprise-wide compliance for IT infrastructure. The enterprise-wide investment approach benefits the bureaus in their cybersecurity goals to create unified approach to cyber spending and stronger protections across the Department.

The investments within the CEA continue to align with the National Institute of Standards and Technology (NIST) Cybersecurity core framework and reporting standards. This includes common cybersecurity activities and outcomes that are gaining use industry-wide: Identify, Protect, Detect, Respond, and Recover.

Budget Highlights

Dollars in Thousands

	FTE	Amount
FY 2022 Annualized CR	**10**	**$18,000**
Changes to Base:		
Non-Recurring Costs	(10)	(18,000)
Subtotal Changes to Base	(10)	(18,000)
FY 2023 Current Services	**0**	**$0**
Program Changes:		
Program Increases:	21	215,000
Zero Trust Architecture Implementation	9	86,452
Security Logging Requirements	0	23,329
Cloud Enterprise Investment[1]	0	22,500
Universal Encryption	0	16,467
Multi-Factor Authentication	0	10,978
Other Cybersecurity Priorities	9	43,050
Bureau Specific Investments		
Cloud Adoption - Bureau of the Fiscal Service (Fiscal Service)	0	9,674
FISMA Assessment Readiness Team - Departmental Offices Salaries and Expenses (DO SE)	3	1,850
Logging Requirements - Treasury Inspector General for Tax Administration (TIGTA)	0	700
Subtotal Program Changes	**21**	**$215,000**
FY 2023 President's Budget Request	**21**	**$215,000**

[1]The $22.5 million program increase for the Cloud Enterprise Investment includes enhancing and upgrading cloud security capabilities across the Department, including related IRS cyber activities.

Budget Adjustments

Non-Recurring Costs ……..…. -$18,000,000 / -10 FTE

This amount represents non-recurring initial investments.

Program Increases ……+$215,000,000 / +21 FTE

Zero Trust Architecture Implementation +$86,452,000 / +9 FTE

This investment 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. Reinforcing implementation of continuous identity verification and access policies, aligned with Zero Trust, will improve the Department's resistance to fraudulent tampering of privileged accounts.

Implementation of Zero Trust will initially be driven by focusing on the near-term actions required by OMB M-22-09, such as changes to password policies, building a new data categorization model, and making one "internal" system accessible over the Internet. Treasury will proceed with the transition to ZTA by planning projects on a pillar-by-pillar basis (Identity, Device, Network, Application, Data, as well as Monitoring/Visibility, Automation, and

Governance). Priority projects will be based on the risk reduction that will result, as well as the anticipated gain in Zero Trust Maturity they will provide weighed against the cost. Implementation of ZTA will require personnel resources with skillsets for managing the service providers to develop, test, and deploy the applications that have integrated security controls.

Security Logging Requirements +$23,329,000 / +0 FTE

Supports Treasury's compliance efforts related to the security logging requirements outlined in OMB Memorandum M-21-31. This guidance requires all logs of security information captured, to be accessible and visible for the highest-level security operations center (SOC) at the Department. This will require expansion of the Treasury Shared Services Secure 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 the 39 Treasury Shared Services.

The FY 2023 budget request for Security Logging Requirements will be used in the following ways:

- Support appropriate acquisition of subject matter expertise for the development of an enterprise, centralized logging solution that leverages a single architecture and allows for segmentation of Bureau data, and presents efficiencies in collecting and distributing necessary information to external partners (e.g., CISA, FBI, etc.)
- Stand-up the initial capabilities (resource support, development, migration, etc.) within the Treasury enterprise cloud program, Workplace Community Cloud (WC2)
- Support initial storage requirements to centralize enterprise shared service program logs, with targeted expansion of architecture and migration of Bureaus logs to the centralized cloud-based storage solution
- Expansion of enterprise license capacity to support centralized log management and the on-ramping of Bureaus from legacy licensing and log storage environments

There are many factors that will impact on the costs associated with implementation of the security logging requirements. These factors include but are not limited to legacy licensing; contract structures; resources for O&M; and holistic storage requirements. The complexity of a federated bureau environment also proposes a unique challenge to ensure compliance.

Cloud Enterprise Investment +$22,500,000 / +0 FTE

This investment is for cloud enterprise cyber security enhancements and upgraded capabilities to meet ever growing security and compliance risks. The Treasury enterprise cloud program enhances security controls, monitors capabilities, and increases threat protections by providing a common cloud operating platform for Departmental workloads inclusive of all the of the security elements driven by EO 14028 and subsidiary guidance. This will allow the bureaus to integrate into Treasury's holistic security umbrella with a single pane of glass view for operational security elements such as the TSSOC.

Treasury continues to improve, entice, and further accelerate enterprise-wide cloud adoption through investment in cloud environments.

The FY 2023 budget request will support improvements in the following areas:

- Identity Pillars - Includes migrations of cloud users to Azure Active Directory (AD) and implementation of Azure Defender for endpoints and users. Azure AD will enable the enterprise shared service cloud program to centralize and streamline governance and management of WC2 privileged accounts, and includes advanced threat protections such as automated detection, remediation and reporting of unusual activity using latest threat detection and analytics.
- Network and Environment Segregation - Includes an architecture ZTA maturity assessment and implementation plan for both Treasury shared services cloud environments against NIST Zero Trust reference Architectures. Implementation will focus on security control enhancements to achieve the near-term ZTA vision and alignment to NIST container-based control security requirements.
- Cloud Monitoring Tenant - Includes increased cloud telemetry, implementation for Trusted Internet Connection (TIC) 3.0 requirements, and consolidation of logging environments to reduce ongoing O&M costs and adopt the latest advances in log analysis. Additional security operations and threat hunting support will operationalize the data creating security dashboards to show potential security issues which require investigation.

Universal Encryption +$16,467,000 / +0 FTE

Supports Treasury's commitment to fully comply with the encryption protocols outlined in EO 14028 and subsidiary supporting material from OMB, CISA, NIST and other cybersecurity oversight entities. Encryptions allows information and data to be converted into code to prevent unauthorized access. This funding level is necessary to develop a more aggressive approach to these cyber protections which contributes to the adoption of ZTA.

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. It is anticipated that no changes will be made to the DNS infrastructure to enable encryption, and that the work will focus on transitioning applications to use HTTPS for secure communication with users. Treasury is also implementing Data at Rest (DAR) and Date in Transit (DIT) encryption across its entire IT portfolio.

Multi-Factor Authentication +$10,978,000 / +0 FTE

This investment is for Multi-Factor Authentication (MFA), which is a critical part of the Federal Government's security baseline and integral component of Treasury's solutions to prevent unauthorized access by adversaries including nation state actors.

EO 14028 directed agencies to remove passwords and fully adopt MFA to the maximum extent by November 2021. While Treasury has made substantial progress with the implementation of MFA capabilities, there is significant work to be done including compliance with subsequent memos impacting MFA like M-22-09, which places significant emphasis on MFA. The FY 2023 funding levels support Treasury's work to protect data at rest and in transit, which may include

personal identification of financial assets; collaborate with industry partners, and to also align with the FISMA requirements driven by CISA.

Other Cybersecurity Priorities +$43,050,000 / +12 FTE

In FY 2023, Treasury will continue to make progress on ongoing critical cybersecurity investments that are in various Development, Modernization and Enhancement (DME) and initial Operation and Maintenance (O&M) phases. 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 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 Treasury. Priority investments include but are not limited to:

- Supply Chain Risk Management Enhancements (SCRM)
- Enterprise Cyber Risk Management (ECRM)
- Governance, Risk and Compliance (GRC)
- High Value Assets (HVA)
- Enterprise Threat and Vulnerability Management (ETVM)
- Vulnerability Disclosure Policy (VDP) Platform
- Ongoing SolarWinds Infrastructure and Post Incident Investments:
  - Threat intelligence providing proactive posture with regards to emergent threat (Post Incident)
  - Enterprise Application Security Improvements (Post Incident)
  - Annual Threat Hunt (Post Incident)
  - Hardware Security Modules (HSM) for generation and storage of security certificates (Infrastructure)

Bureau Specific Investment +$12,224,000 / +3 FTE

Cloud Adoption- Bureau of the Fiscal Service (Fiscal Service) +$9,674,000 / +0 FTE

This investment will accelerate Fiscal Service's Cloud Adoption from aging, costly platforms to optimize cloud-based architecture that will enhance the resiliency of Fiscal Service's systems and remediate Fiscal Service audit deficiencies. This applies to Fiscal Service's specific portfolio of applications and systems. Many of Fiscal Service's HVAs that support the National Critical Financial Infrastructure (NCFI) 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 substantial contractual costs that is anticipated to continue increasing over time. Consistent with the EO 14208, this funding will allow Fiscal Service to move over 60 FISMA systems to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). It will also enhance the business continuity and disaster recovery of these systems.

FISMA Assessment Readiness Team- Departmental Offices Salaries and Expenses (DO SE) $1,850,000 / +3 FTE

This investment will establish an Assessment Readiness Team (ART) which will be responsible for conducting independent assessments of security policies, programs, and operations

throughout Treasury to identify gaps in a bureau's security posture and close them before they can be exploited by cyber criminals and nation state actors. The ART will be responsible for conducting security control assessments ensuring incident detection controls are employed and identifying associated deficiencies to detect capabilities across Treasury systems. These assessments will be used to improve Treasury's cybersecurity maturity model against technical, management and operational controls.

Logging Requirements- Treasury Inspector General for Tax Administration (TIGTA) +$700,000 / +0 FTE

This investment supports TIGTA's plans to meet EO 14028 and subsequent OMB M-21-31. TIGTA will continue strengthening and operating its enterprise logging solution to meet current and future demands to:

- Collect security event and system logs in real time for threat detection and compliance use cases.
- Analyze logs in real time to detect attacks and other activities of interest.
- Investigate incidents to determine their potential severity and impact on a business.
- Report on these activities.
- Store relevant events and logs.

This will also enable TIGTA to perform the data collection needed to meet the requirements and automate the identification of unauthorized disclosure or access (UNAX) while also vastly improving the cyber detection capabilities. At the same time, it will meet on-going demands for improved efficiencies around cyber incident detection and response. The request will fund 12 months of operations.

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 these Department's strategic goals and objectives uninterrupted. The CEA aligns with the following Treasury strategic goal and objectives as presented in the FY 2022- 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 2019 Actual	FY 2020 Actual	FY 2021 Actual	FY 2022 Target	FY 2023 Target
Number of Major Incidents	0	1	1	0	0
Number of Reported Incidents	152	280	246	150	150
Percentage of Tier I High Value Assets (HVA) 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	57	80	80	75	75

Description of Performance

This year, CEA is working to align budget activities and performance measures to the new objectives in the Treasury FY 2022 – 2026 Strategic Plan. This work will include benchmarking performance and may result in changes to performance measures in the FY 2024 budget.

Number of Major Incidents:
The number of major incidents, as defined in OMB 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. The FY 2023 request includes additional funding to mitigate weaknesses identified and investments that support critical IT improvements. The FY 2022 and 2023 performance target of zero major incidents reported will be met through continued work to harden cybersecurity protocols, implementation of new cyber technology, interagency collaboration, increased training for cyber personnel, and customer feedback.

Number of Reported Incidents:
Each fiscal year, Treasury tracks the number of cybersecurity incidents reported to the United States Computer Emergency Readiness Team (US-CERT). In FY 2021, Treasury witnessed a lower number of incidents being reported, this is indicative of enhanced detection and mitigation capabilities. The FY 2022 and FY 2023 targets will remain flat.

Percentage of High and/or Critical Findings from Risk and Vulnerability Assessment (RVAs) or Security Architecture Review (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 (POAMs) within the fiscal year. Treasury has consistently recorded a 100 percent completion rate for system assessments and currently has a 100% closure rate for associated findings and POAMs. It was decided that the FY 2022 and 2023 targets will remain flat from FY 2021 numbers due to the likelihood of findings from HVA assessments requiring long-term remediation efforts.