Cybersecurity Enhancement Account

Program Summary by Budget Activity

Dollars in Thousands

Cybersecurity Enhancement	FY 2017	FY 2018	FY 2019	FY 2018 TO FY 2019	
Account	**Enacted**	**Annualized CR**	**Request**	**$ Change**	**% Change**
Cybersecurity Enhancement Account	$47,743	$47,419	$25,208	($22,211)	-46.84%
Total Program Operating Level	**$47,743**	**$47,419**	**$25,208**	**($22,211)**	**100.00%**
Direct FTE	1	19	19	0	0.00%
Total FTE	**1**	**19**	**19**	**0**	**0.00%**

Note: The FY 2017 Enacted column reflects levels appropriated in H.R. 255, the Consolidated Appropriations Act of 2017. For further details on the execution of these resources see the 2019 Budget *Appendix* chapter for the Department of the Treasury.

Summary

The Department's strategic plan guides program and budget decisions for the Cybersecurity Enhancement Account (CEA). The FY 2019 Budget Request supports two of the Treasury's FY 2018-2022 strategic goals: Promote Financial Stability and Achieve Operational Excellence.

Trillions of dollars are accounted for and processed by the Department of the Treasury's information technology (IT) systems, and therefore, they are a constant target for sophisticated threat actors. To more proactively and strategically protect Treasury systems against cybersecurity threats, the FY 2019 budget requests $25.208 million for the CEA. The account identifies and supports Department-wide investments for critical IT improvements, including the systems identified as High Value Assets (HVAs). Furthermore, the centralization of funds allows Treasury to more nimbly respond in the event of a cybersecurity incident as well as leverage enterprise-wide services and capabilities across the components of the Department.

By managing CEA centrally, Treasury elevates the importance of such initiatives and provides Treasury leadership, OMB, and Congress with better transparency into cybersecurity activities across the Department. Enhanced transparency also improves Department-wide coordination of cybersecurity efforts and improves the Department's response and recovery capabilities. With high-level support, the program provides a platform to enhance efficiency, communication, transparency, and accountability around the mission.

FY 2019 Budget Highlights

Dollars in Thousands

Cybersecurity Enhancement Account	FTE	Amount
FY 2018 Annualized CR	**19**	**$47,419**
Changes to Base:		
Non-Recurring Costs	0	($22,629)
Evolving High Impact Fund	0	($14,899)
Enchancements to the Treasury Secure Data Network	0	($3,671)
Data Loss Protection Analytics Capabilities	0	($1,202)
Encrypted Traffic Inspection and Data Loss Prevention at the Fiscal Service Trusted Internet Connections (TIC)	0	($685)
Malware Content Filter	0	($2,172)
Program Increases:	0	$418
One-time Changes of Other Initiatives	0	$418
Subtotal Changes to Base	0	($22,211)
Total FY 2019 Base	**19**	**$25,208**
Total FY 2019 Request	**19**	**$25,208**

FY 2019 Budget Adjustments

Adjustments to Request

Non-Recurring Costs

Evolving High Impact Fund -$14,899,000 / -0 FTE

The Evolving High Impact Fund was funded at $14.9 million in FY 2017 for three years to ensure that new and ever-evolving threats can be rapidly addressed before they are exploited. Treasury leadership manages the fund, to include receiving solicitations from across the

Department and managing and allocating resources based on criteria and need at Treasury offices and bureaus. Treasury proposes in FY 2019 to discontinue the Evolving High Impact Fund to prioritize investment in other high priority areas and the operations and maintenance of continuing investments.

Enhancements to the Treasury Secure Data Network (TSDN) -$3,671,000 / -0 FTE

The FY 2019 level reflects the funding required to maintain investments made in FY 2017 and FY 2018. Funding will continue the strategic continuation of the multi-year plan to ensure that CEA-funded investments to the Treasury-wide SECRET collateral network support: increased overall stability and integrity; continued implementation of enhancements to modernize infrastructure; improved Disaster Recovery program and capability; increased timeliness of incident response and recovery; improved responsiveness and detection to cybersecurity threats; and enhanced security monitoring by the Government Security Operations Center.

The TSDN enhancements will also provide advanced toolsets for automated monitoring, as well as analyst review of outputs from these toolsets. These funds will also improve security operations, configuration management, and reporting.

Data Loss Protection Analytics Capabilities -$1,202,000 / -0 FTE

The FY 2019 level reflects the funding required to maintain investments made in FY 2017 and FY 2018. This funding supports enhancements to the Treasury enterprise security operations center analytical capabilities. These capabilities will enable faster detection and containment of attacks on Treasury's IT assets.

Encrypted Traffic Inspection and Data Loss Prevention at the Fiscal Service Trusted Internet Connections (TIC) -$685,000 / -0 FTE

The FY 2019 level reflects the funding required to maintain investments made in FY 2017 and FY 2018. This capability, installed at Treasury's enterprise internet gateways, enhances Treasury's ability to detect, investigate, and respond to unauthorized attempts to access and remove sensitive taxpayer and financial data from the Treasury network and bureau networks.

Malware Content Filter -$2,172,000 / -0 FTE

The FY 2019 level reflects the funding required to maintain investments made in FY 2017 and FY 2018. This capability, installed at Treasury's enterprise internet gateways, allows Treasury to identify and remove malicious attachments and links from web and email traffic before they reach the Treasury network. This reduces the risk of compromise for the entire Treasury network, as well as systems housed on that network, including High Value Assets.

Program Increases +$418,000 / +0 FTE

One-time Changes of Other Initiatives +$418,000, +0 FTE

This line reflects the net of six minor changes to CEA initiatives from the FY 2018 Annualized CR. These initiatives are: High Value Assets, Cybersecurity Infrastructure, Incident Response and Recovery, Cyber Risk and Threat Identification, Mitigation of Cyber Threats to Financial Services Sector, and Cybersecurity for Classified Networks.

Explanation of Budget Activities

Cybersecurity Enhancement Account ($25,208,000 from direct appropriations)

The purpose of CEA is to strategically mitigate cybersecurity risks through a centralized program with Department-wide impact. Due to the increasing number and sophistication of cyberattacks, Treasury leadership has prioritized cybersecurity and supports the centralization of department-wide cybersecurity initiatives through the CEA account and budget activity. Current bureau-level cybersecurity spending remains in the base budgets of each bureau. With the publication of the Treasury Strategic Plan for FY 2018-2022, Treasury will work this year to baseline performance against the new strategic objectives. This may result in additional performance measure changes in the FY 2020 budget.

Legislative Proposals

The Cybersecurity Enhancement Account has no legislative proposals.

Performance by Budget Activity

		FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Budget Activity	**Performance Measures**	**Actual**	**Actual**	**Actual**	**Target**	**Target**
CEA	Number of major incidents	N/A	N/A	N/A	I	TBD
CEA	Number of reported incidents	N/A	N/A	N/A	I	TBD
CEA	Percentage of Tier I High Value Assets (HVA) with an overdue Risk and Vulnerability Assessment (RVA) or Security Architecture Review (SAR)	N/A	N/A	N/A	B	TBD
CEA	Risk Management Assessment Overall Rating	N/A	N/A	N/A	B	TBD

Key: B - Baseline I – Performance Indicator

Description of Performance

The CEA was established as a new account in FY 2017. As capabilities funded by the CEA become operational, Treasury will capture baseline data for the following metrics in order to establish targets for the FY 2020 budget submission.

<u>Number of major incidents</u>: The number of major incidents, as defined in OMB M-18-02, 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.

<u>Number of reported incidents</u>: The number of cybersecurity incidents reported by Treasury to US-CERT in a given fiscal year. This is a measure of how effective Treasury's defenses are at mitigating all security threats, as well as an indicator of how often Treasury is being targeted by malicious actors. If the number of reported incidents rises while the number of major incidents remains steady, it may indicate an effective cybersecurity program.

<u>Percentage of Tier I High Value Assets (HVA) with an overdue Risk and Vulnerability Assessment (RVA) or Security Architecture Review (SAR)</u>: The percentage of Treasury's top tier high value assets scheduled for a third party risk assessment, but that did not undergo one on time. This is a measure of how often Treasury's most important systems are being actively reviewed and assessed for weaknesses that could be exploited by an adversary.

<u>Risk Management Assessment Overall Rating</u>: This is an assessment performed by OMB to evaluate agencies' overall cybersecurity risk management capabilities. It consists of a risk management rating and a maturity rating. This is a measure of how well Treasury is managing risk across the enterprise as well as the maturity level of the program.