

Department of the Treasury  
Cybersecurity Enhancement  
Account

Congressional Budget  
Justification and Annual  
Performance Report and Plan

FY 2019

# Table of Contents

<b>Section I – Budget Request</b> .....	<b>3</b>
A – Mission Statement.....	3
B – Summary of the Request .....	3
1.1 – Appropriations Detail Table .....	3
1.2 – Budget Adjustments Table.....	4
C – Budget Increases and Decreases Description.....	4
1.3 – Operating Levels Table.....	5
D – Appropriations Language and Explanation of Changes .....	6
E – Legislative Proposals.....	6
<b>Section II – Annual Performance Plan and Report</b> .....	<b>7</b>
A – Strategic Alignment .....	7
B – Budget and Performance by Budget Activity .....	7
2.1.1 – Cybersecurity Enhancement Account Resources and Measures .....	7
C – Changes in Performance Measures .....	8
<b>Section III – Additional Information</b> .....	<b>9</b>
A – Summary of Capital Investments.....	9

## Section I – Budget Request

---

### A – Mission Statement

Bolster the Department’s cybersecurity posture and mitigate cybersecurity threats to the U.S. financial infrastructure.

### B – Summary of the Request

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.

### 1.1 - Appropriations Detail Table

Dollars in Thousands

Cybersecurity Enhancement Account Appropriated Resources	FY 2017		FY 2018		FY 2019		FY 2018 to FY 2019			
	Enacted		Annualized CR		Request		Change		% Change	
New Appropriated Resources	FTE	AMOUNT	FTE	AMOUNT	FTE	AMOUNT	FTE	AMOUNT	FTE	AMOUNT
Cybersecurity Enhancement Account	1	\$47,743	19	\$47,419	19	\$25,208	0	(\$22,211)	0.00%	-46.84%
<b>Total Budgetary Resources</b>	<b>1</b>	<b>\$47,743</b>	<b>19</b>	<b>\$47,419</b>	<b>19</b>	<b>\$25,208</b>	<b>0</b>	<b>(\$22,211)</b>	<b>0.00%</b>	<b>-46.84%</b>

Note:

1. FY 2017 FTE are actuals.
2. 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.

## 1.2 – Budget Adjustments Table

Dollars in Thousands

Cybersecurity Enhancement Account	FTE	Amount
<b>FY 2018 Annualized Continuing Resolution</b>	<b>19</b>	<b>\$47,419</b>
<b>Changes to Base:</b>		
Non-Recurring Costs	0	(\$22,629)
Evolving High Impact Fund	0	(\$14,899)
Enhancements 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)
<b>Total FY 2019 Base</b>	<b>19</b>	<b>\$25,208</b>
<b>Total FY 2019 Request</b>	<b>19</b>	<b>\$25,208</b>

## C – Budget Increases and Decreases Description

**Program Decreases .....-\$22,629,000 / +0 FTE**

**Non-Recurring Costs -\$22,629,000 / +0 FTE**

**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 -\$3,253,000 / -0 FTE**

The FY 2019 level reflects the funding required to maintain investments made in FY 2017 and FY 2018. These funding levels will allow for 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.

**1.3 – Operating Levels Table**

Dollars in Thousands

Bureau Name Object Classification	FY 2017 Enacted	FY 2018 Annualized CR	FY 2019 Request
11.1 - Full-time permanent	2,480	2,463	2,499
11.5 - Other personnel compensation	35	35	36
<b>11.9 - Personnel Compensation (Total)</b>	<b>2,515</b>	<b>2,498</b>	<b>2,535</b>
12.0 - Personnel benefits	727	722	770
<b>Total Personnel and Compensation Benefits</b>	<b>\$3,242</b>	<b>\$3,220</b>	<b>\$3,304</b>
21.0 - Travel and transportation of persons	24	24	24
23.3 - Communications, utilities, and miscellaneous charges	55	55	55
25.1 - Advisory and assistance services	14,204	14,106	6,271
25.2 - Other services from non-Federal sources	8,870	8,810	1,836
25.3 - Other goods and services from Federal sources	8,018	7,964	2,504
25.7 - Operation and maintenance of equipment	500	497	499
26.0 - Supplies and materials	173	172	173
31.0 - Equipment	12,657	12,571	10,542
<b>Total Non-Personnel</b>	<b>\$44,501</b>	<b>\$44,199</b>	<b>\$21,904</b>
<b>New Budgetary Resources</b>	<b>\$47,743</b>	<b>\$47,419</b>	<b>\$25,208</b>
<b>FTE</b>	<b>1</b>	<b>19</b>	<b>19</b>

Note:

1. FY 2017 FTE are actuals.

2. 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

**D – Appropriations Language and Explanation of Changes**

Appropriations Language	Explanation of Changes
<p style="text-align: center;">DEPARTMENT OF THE TREASURY DEPARTMENTAL OFFICES <i>Federal Funds</i></p> <p style="text-align: center;"><b>CYBERSECURITY ENHANCEMENT ACCOUNT</b> (INCLUDING TRANSFER OF FUNDS)</p> <p><i>For salaries and expenses for enhanced cybersecurity for systems operated by the Department of the Treasury, \$25,208,000, to remain available until September 30, 2021: Provided, That amounts made available under this heading shall be in addition to other amounts available to Treasury offices and bureaus for cybersecurity.</i></p> <p>Note.—A full-year 2018 appropriation for this account was not enacted at the time the budget was prepared; therefore, the budget assumes this account is operating under the Continuing Appropriations Act, 2018 (Division D of P.L. 115–56, as amended). The amounts included for 2018 reflect the annualized level provided by the continuing resolution.</p>	

**E – Legislative Proposals**

The Cybersecurity Enhancement Account has no legislative proposals.

## Section II – Annual Performance Plan and Report

### A – Strategic Alignment

The project to mitigate cyber threats to the U.S. financial services sector supports the following Department of the Treasury’s FY 2018-2022 Strategic Plan objective for Strategic Goal 2, to promote financial stability:

- Objective 2.4 – Financial Sector Critical Infrastructure and Cybersecurity: Enhance security, improve resiliency, and reduce the risk of significant cybersecurity and other incidents to the financial sector’s critical infrastructure, domestically and internationally.

All other projects have the common purpose of strengthening the security of Treasury’s IT assets and supports the following strategic objective for Strategic Goal 5, to achieve operational excellence:

- Objective 5.2 – Treasury Infrastructure: Better enable mission delivery by improving the reliability, security, and resiliency of Treasury’s infrastructure.

Additionally, these projects will ensure compliance with both OMB and Executive Orders involving the security of government IT assets. To achieve these objectives, Treasury is deploying a multi-pronged approach of strategically procuring hardware and software, streamlining business processes while expanding security monitoring, and ensuring accountability at all levels.

### B – Budget and Performance by Budget Activity

#### 2.1.1 Cybersecurity Enhancement Account Resources and Measures

Dollars in Thousands

Resource Level	FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
	Actual	Actual	Actual	Actual	Actual	Annualized CR	Request
Appropriated Resources	0	0	0	0	\$8,442	\$47,419	\$25,208
<b>Budget Activity Total</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>\$8,442</b>	<b>\$47,419</b>	<b>\$25,208</b>
<b>FTE</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>1</b>	<b>19</b>	<b>19</b>

Measure	FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	FY 2017	FY 2018	FY 2019
	Actual	Actual	Actual	Actual	Actual	Target	Target	Target
Number of major incidents	N/A	N/A	N/A	N/A	N/A	N/A	I	TBD
Number of reported incidents	N/A	N/A	N/A	N/A	N/A	N/A	I	TBD
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	N/A	N/A	N/A	B	TBD
Risk Management Assessment Overall Rating	N/A	N/A	N/A	N/A	N/A	N/A	B	TBD

Key: B - Baseline; I – Performance Indicator

## **Cybersecurity Enhancement Account (CEA) Budget and Performance**

*(\$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.

### **C – Changes in Performance Measures**

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.

<b>Performance Measure or Indicator</b>	<b>Change and Justification</b>
1. Number of Major Incidents  (New Performance Indicator)	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.
2. Number of Reported Incidents  (New Performance Indicator)	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.
3. Percentage of Tier I High Value Assets (HVA) with an overdue Risk and Vulnerability Assessment (RVA) or Security Architecture Review (SAR)  (New Performance Measure)	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.

Performance Measure or Indicator	Change and Justification
4. Risk Management Assessment Overall Rating  (New Performance Measure)	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.

With the publication of Treasury's Strategic Plan for FY 2018-2022, Treasury will work in FY 2018 to baseline performance against the new strategic objectives. This may result in additional performance measure changes in the FY 2020 budget.

### **Section III – Additional Information**

---

#### **A – Summary of Capital Investments**

Capital investments that support CEA are included in the Departmental Offices plan. A summary of capital investment resources, including major information technology and non-technology investments can be found at:

<http://www.treasury.gov/about/budget-performance/Pages/summary-of-capital-investments.aspx>

This website also contains a digital copy of this document.