Department of the Treasury Cybersecurity Enhancement Account

Congressional Budget Justification and Annual Performance Report and Plan

FY 2020

Table of Contents

Section I – Budget Request

A – Mission Statement
Bolster the Department's cybersecurity posture.

B – Summary of the Request
The Department's strategic plan guides program and budget decisions for the Cybersecurity Enhancement Account (CEA). The FY 2020 Budget Request supports Treasury's FY 2018-2022 Strategic Goal: 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 2020 budget requests $18.0 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	FY 2018		FY 2019		FY 2020		FY 2019 to FY 2020			
Appropriated Resources	Enacted*		Annualized CR		Request		Change		% Change	
New Appropriated Resources	**FTE**	**AMOUNT**	**FTE**	**AMOUNT**	**FTE**	**AMOUNT**	**FTE**	**AMOUNT**	**FTE**	**AMOUNT**
Cybersecurity Enhancement Account	8	$24,000	19	$24,000	11	$18,000	(8)	($6,000)	-42.11%	-25.00%
Total Budgetary Resources	**8**	**$24,000**	**19**	**$24,000**	**11**	**$18,000**	**(8)**	**($6,000)**	**-42.11%**	**-25.00%**

* FY 2018 FTE and Other Resources are Actuals. This column reflects levels appropriated in P.L. 115-141, the Consolidated Appropriations Act of 2018. For further details on the execution of these resources see the 2020 Budget Appendix chapter for the Department of the Treasury.

1.2 – Budget Adjustments Table

Dollars in Thousands

Cybersecurity Enhancement Account	FTE	Amount
FY 2019 Annualized CR	**19**	**$24,000**
Changes to Base:		
Non-Recurring Costs	(11)	($22,349)
OCIP Re-alignment to DO SE	(8)	($1,651)
Subtotal Changes to Base	(19)	($24,000)
Total FY 2020 Base	**0**	**$0**
Program Changes:		
Program Increases:	11	$18,000
Improving HVA Cybersecurity	0	$3,800
Proactive Cyber Risk and Threat Identification	0	$966
Cybersecurity Enhancements	7	$2,407
Enhanced Incident Response and Recovery Capabilities	2	$10,428
Enhancements to Cybersecurity Infrastructure	2	$399
Total FY 2020 Request	**11**	**$18,000**

C – Budget Increases and Decreases Description

Non-Recurring Costs ..... -$24,000,000 / -19 FTE

FY 2019 Non-Recurring Investments -$22,349,000 / -11 FTE

This amount represents non-recurring initial investments.

OCIP Re-alignment to DO SE -$1,651,000 / -8 FTE

The Office of Critical Infrastructure Protection and Compliance Policy (OCIP) investment has been realigned to the Departmental Offices Salaries and Expenses account.

Program Increases ..... +$18,000,000 / +11 FTE

Improving High Value Asset (HVA) Cybersecurity +$3,800,000 / +0 FTE

The HVA Cybersecurity initiative builds on prior investments to secure Treasury's top tier HVAs and data at rest encryption solutions for payment platforms, tax processing systems, and collection processing systems, as well as enhanced user authentication for these systems. It will deliver enhanced data assurance capabilities, minimizing accessibility of highly sensitive data in the event of compromises to multi-layered defenses and storage solutions.

Proactive Cyber Risk and Threat Identification +$966,000 / +0 FTE

This initiative significantly improves network visibility, threat identification, incident response time, data aggregation, and data management by Treasury's enterprise cybersecurity operations center. It provides high definition monitoring of IT assets and activities, and detailed visibility across the enterprise and into bureau networks. This initiative will result in faster detection, response, and recovery time in the event of an advanced persistent threat attack, other malicious activities, or negligent acts.

Cybersecurity Enhancements +$2,407,000 / +7 FTE
This request improves cybersecurity situational awareness through the implementation of processes and automated tools that support cyber information sharing department-wide and eliminates organizational stovepipes that negatively impact the Department's cybersecurity posture. Enhanced situational awareness will provide Department-wide awareness of breaches and attack information. It will increase the effectiveness of cybersecurity functions and achieve efficiencies through the elimination of redundant efforts.

Enhanced Incident Response and Recovery Capability +$10,428,000 / +2 FTE
This initiative improves the Department's ability to identify, respond to, and recover from cyber threats through the implementation of solutions that support early detection and avoidance of currently unknown threats. Activities include retroactive examination of network traffic; assessment of adversarial movement; determination of information compromise; implementation of mitigations and countermeasures; and reconstitution. The initiative will reduce the risk of incident occurrence, minimize their impact, and decrease recovery time.

Enhancements to Cybersecurity Infrastructure +$399,000 / +2 FTE
This initiative will enhance encryption, enterprise-wide identity management, and network monitoring and scanning. It is critical to the Department's cyber posture due to the increases in volume, sophistication, frequency, impact, and brazenness of global cyber threats and recent privacy breaches (including financial institutions). It will result in higher level of assurance for data integrity and access management.

1.3 – Operating Levels Table

Dollars in Thousands

Bureau Name Object Classification	FY 2018 Enacted	FY 2019 Annualized CR	FY 2020 Request
11.1 - Full-time permanent	$2,480	$2,480	$1,447
11.5 - Other personnel compensation	$38	$38	$21
11.9 - Personnel Compensation (Total)	**$2,518**	**$2,518**	**$1,468**
12.0 - Personnel benefits	$727	$727	$446
Total Personnel and Compensation Benefits	**$3,245**	**$3,245**	**$1,914**
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	$4,342	$4,342	$4,461
25.2 - Other services from non-Federal sources	$1,271	$1,271	$4,546
25.3 - Other goods and services from Federal sources	$1,733	$1,733	$834
25.7 - Operation and maintenance of equipment	$500	$500	$916
26.0 - Supplies and materials	$173	$173	$172
31.0 - Equipment	$12,657	$12,657	$5,078
Total Non-Personnel	**$20,755**	**$20,755**	**$16,086**
New Budgetary Resources	**$24,000**	**$24,000**	**$18,000**
FTE	**8**	**19**	**11**

Note: FY 2018 FTE are actuals

D – Appropriations Language and Explanation of Changes

Appropriations Language	Explanation of Changes
DEPARTMENT OF THE TREASURY DEPARTMENTAL OFFICES *Federal Funds* CYBERSECURITY ENHANCEMENT ACCOUNT (INCLUDING TRANSFER OF FUNDS) *For salaries and expenses for enhanced cybersecurity for systems operated by the Department of the Treasury, $18,000,000, to remain available until September 30, 2022: Provided, That amounts made available under this heading shall be in addition to other amounts available to Treasury offices and bureaus for cybersecurity.* Note.—A full-year 2019 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, 2019 (Division C of P.L. 115–245, as amended). The amounts included for 2019 reflect the annualized level provided by the continuing resolution.	

E – Legislative Proposals

The Cybersecurity Enhancement Account has no legislative proposals.

Section II – Annual Performance Plan and Report

A – Strategic Alignment

The 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.

B – Budget and Performance by Budget Activity

2.1.1 Cybersecurity Enhancement Account Resources and Measures

Dollars in Thousands

Resource Level	FY 2014 Actual	FY 2015 Actual	FY 2016 Actual	FY 2017 Actual	FY 2018 Actual	FY 2019 Annualized CR	FY 2020 Request
Appropriated Resources	0	0	0	$8,442	$26,410	$24,000	$18,000
Budget Activity Total	**0**	**0**	**0**	**$8,442**	**$26,410**	**$24,000**	**$18,000**
FTE	**0**	**0**	**0**	**0**	**8**	**19**	**11**

Performance Measure	FY 2014 Actual	FY 2015 Actual	FY 2016 Actual	FY 2017 Actual	FY 2018 Actual	FY 2018 Target	FY 2019 Target	FY 2020 Target
Number of Major Incidents	N/A	N/A	N/A	N/A	0	2	2	2
Number of Reported Incidents	N/A	N/A	N/A	N/A	225	276	280	280
Percentage of Tier I High Value Assets (HVA) where Risk and Vulnerability Assessment (RVA) or Security Architecture Review (SAR) are completed on time	N/A	N/A	N/A	N/A	100%	100%	100%	100%
Risk Management Assessment Overall Rating	N/A	N/A	N/A	N/A	68%	40%	60%	70%

Cybersecurity Enhancement Account (CEA) Budget and Performance

($18,000,000 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.

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 2020 performance target of two major incidents reported will be met through increased training, implementation of technology, interagency collaboration and customer feedback.

Number of Reported Incidents: The number of cybersecurity incidents reported by Treasury to the United States Computer Emergency Readiness Team (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. The incidence of intrusion events at Treasury has not remained constant over time, and our projections must be used as a baseline to measure against. As reflected in the *Actual* value column, there was an actual reduction in incidents for FY 2018 in comparison to those projected by Treasury. This is likely the result of changes in the reporting criteria applied during the course of the year. As new incident recognition investments are implemented within Treasury throughout FY 2019, the target goals for FY 2019 are expected to show an increase in recognized incidents of up to 25 percent from FY 2018 actuals, applying the same criteria, within the FY 2019 timeframe. Allowing for increasing preventative measures, FY 2020 should remain flat from FY 2019 numbers. The FY 2019 and FY 2020 targets of 280 reported incidents, representing a 25 percent increase in the visibility of incidents, will be met through training, implementation of technology, and interagency collaboration.

Percentage of Tier I High Value Assets (HVA) with Risk and Vulnerability Assessment (RVA) or Security Architecture Review (SAR) completed on time: The percentage of Treasury's top tier high value assets, which were scheduled for a third party risk assessment, for which the assessments were completed on time. This is a measure of the extent to which Treasury's most important systems are being actively reviewed and assessed for weaknesses that could be exploited by an adversary. The FY 2020 performance target of 100 percent (of the current annual target of 5 HVA systems to be assessed) will be met through continuing current staffing levels and interagency collaboration. Although Treasury has been able to meet its HVA assessment goals thus far, additional challenges are foreseen for the short-, mid- and long-terms. Pending changes may result in a reduced number of Department of Homeland Security- (DHS-) funded RVA and SAR assessments. As a result of this change, continued success at the 100 percentage level will require the Department to offset the DHS reduction by funding additional 3rd party RVA/SAR assessments to meet OMB compliance requirements, ensuring that Treasury HVAs are appropriately identified and can be mitigated from cyber risks with potentially significant impacts to the Federal enterprise and/or national economy. Factors such as the likely greater complexity imposed in Federal requirements and mandates for assessments/reviews, as well as an ongoing re-evaluation of HVA systems, requires continuing investment in a well-founded HVA management structure, which Treasury has been addressing through its Cybersecurity Enhancement Account (CEA) program.

Risk Management Assessment Overall Rating: 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. The Risk Management Assessment rating is based on agency responses to the reporting metrics of the Federal Information Security Modernization Act of 2014 (FISMA). In December 2018, the Office of Management and Budget revised the FISMA reporting metrics, eliminating several measures that had been factored into the Risk Management Assessment calculus. As a result of these changes to the reporting metrics, agency Risk Management Assessment ratings are expected to decline. Treasury has accounted for this by setting a performance target for FY 2019 that is slightly below the actual rating achieved in FY 2018, with a rebound anticipated in FY 2020 based on cybersecurity enhancement investments that are planned to mature by that time. This is a measure of how well Treasury is managing risk across the enterprise as well as the maturity level of the program. The FY 2020 target Risk Management Rating of 70 percent will be met through increased training, implementation of technology, and continued federal support.

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.