Cybersecurity Enhancement Account

Program Summary by Budget Activity

Dollars in Thousands

Budget Activity	FY 2019 Operating Plan	FY 2020 Enacted	FY 2021 Request	FY 2020 to FY 2021 $ Change	FY 2020 to FY 2021 % Change
Cybersecurity Enhancement Account	$25,208	$18,000	$18,000	$0	0.00%
Total Program Operating Level	**$25,208**	**$18,000**	**$18,000**	**$0**	**0.00%**
Direct FTE	12	11	6	(5)	-45.45%
Total Full-time Equivalents (FTE)	**12**	**11**	**6**	**(5)**	**-45.45%**

Summary

The Department's strategic plan guides program and budget decisions for the Cybersecurity Enhancement Account (CEA). The FY 2021 Budget Request supports Treasury's FY 2018-2022 Strategic Goal: Achieve Operational Excellence.

To more proactively and strategically protect Treasury systems against cybersecurity threats, the FY 2021 budget requests $18.0 million for the CEA. 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. The CEA 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 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.

Over the past year, Treasury has recognized the utility of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework. In order to better align the CEA account with NIST's push for a Government-wide Cybersecurity risk framework, the FY 2021 President's Budget reflects initiatives organized around the NIST Framework Core. While in previous budget submissions CEA included initiatives organized around specific investments (e.g., High Value Assets), the FY 2021 President's Budget is instead organized around common cybersecurity activities and outcomes that are gaining use industry-wide: Identify, Protect, Detect, Respond, and Recover. Treasury's goal in making this methodology shift is to provide better clarity into the strategic focus of the Department's cybersecurity investments, align with accepted industry standards, guidelines and practices, and allow Treasury to track more effectively against government-wide reporting requirements.

Budget Highlights

Dollars in Thousands

	FTE	Amount
FY 2020 Enacted	**11**	**$18,000**
Changes to Base:		
Non-Recurring Costs	(11)	($18,000)
Subtotal Changes to Base	(11)	($18,000)
FY 2021 Current Services	**0**	**$0**
Program Changes:		
Program Increases:	6	$18,000
Identify the Business Context, Resources & Cybersecurity Risk	1	$5,083
Protect the Delivery of Critical Infrastructure Services	3	$8,008
Detect Cybersecurity Events	1	$550
Respond to Detected Cybersecurity Incidents	1	$3,359
Recover by Maintaining Resilience and Restoration Plans	0	$1,000
FY 2021 President's Budget Request	**6**	**$18,000**

Budget Adjustments

Program Increases……+$18,000,000 / +6 FTE

Identify the Business Context, Resources & Cybersecurity Risk +$5,083,000 / +1 FTE

Goal: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

Cybersecurity Risk Model, +$1,291,000

The Cybersecurity Risk Model initiative will define and implement a risk model for assessing and quantifying risk. This includes defining risk criteria and developing a risk quantification tool. This initiative will identify, quantify, access, prioritize, and report on Enterprise Cyber Risks found across the Treasury Department. This project aligns with the *Improving HVA Cybersecurity* initiative from the FY 2020 Budget.

Risk Management Dashboard, +$1,291,000

The end-state of the initiative will provide access to risk data and the ability to analyze such data from multiple sources. Without this central dashboard, data from the System Detection Analysis & Risk Reporting (S-DARR) tool, Treasury FISMA Inventory Management System (TFIMS), HVA data, and the CDM dashboard cannot be easily digested, making assessing risks more time consuming and inaccurate. The Risk Management Dashboard will deliver an enterprise risk analysis and scoring capability allowing personnel to manage risks through clear, centralized rankings. This project aligns with the *Proactive Cyber Risk and Threat Identification* initiative from the FY 2020 Budget.

Risk Management Framework (RMF) Automation Tool, +$2,501,000

The Risk Management Framework Automation Tool automates a broad range of services for comprehensive integrated risk management practices and replaces the outdated Treasury FISMA Information Management System (TFIMS). Automation would include controls scorecard measurement, dashboard reporting, and the generation of Risk Management Framework (RMF) System Assessment and Accreditation (SA&A) artifacts. This project aligns with the *Proactive Cyber Risk and Threat Identification* initiative from the FY 2020 Budget.

Protect the Delivery of Critical Infrastructure Services +$8,008,000 / +3 FTE
Goal: Develop and implement appropriate safeguards to ensure delivery of critical services.

HVA Security Enhancements, +$3,205,000
This request supports additional investment for HVA management per the Department of Homeland Security's (DHS) Binding Operational Directive (BOD) 18-02, which coordinates DHS's approach to securing the federal government's High Value Assets (HVAs) from cybersecurity threats. The HVA Program establishes a governance framework for Departmental HVAs in accordance with federal mandates. DHS performs a select few Risk and Vulnerability (RVA) Assessments for Treasury. However, Treasury HVAs face constraints that impede a full inventory: DHS is not available to support additional assessments, and multiple Treasury sites cannot conduct off-hours assessments as required due to system sensitivity and criticality. Treasury has elected to perform discretionary RVAs and Security Architecture Reviews (SAR) where DHS HVA RVAs are not feasible. This initiative provides support for these additional assessments. These assessments will be compliant with OMB, DHS, and National Institute of Standards and Technology requirements and standards. This project aligns with the *Improving HVA Cybersecurity* initiative from the FY 2020 Budget.

Data Centric Security and Encryption, +$281,000
Over the past several years, technological advancements have made many emergent technologies a reality. This has changed the landscape of cybersecurity. Likewise, advancements in artificial intelligence, social engineering, and quantum computing over the next several years could require upgrades to traditional defenses and methods. This initiative would provide resources to develop strategies and take steps to address emerging threats that are not imminent today in order to push protections closer to the data, consistent with the concept of Zero Trust that was recommended by the House Committee on Oversight and Reform following the Office of Personnel Management breach. This project aligns with the *Enhancements to Cybersecurity Infrastructure* initiative from the FY 2020 Budget.

Treasury Identity Enterprise Services (TIES), +$1,074,000
TIES is an identity management system that provides enterprise-class services for centrally managing employee and contractor identities/user accounts, credentials, and access to systems at the Department level. Centralizing these functions allows Treasury to consolidate duplicative identity management processes, provides the potential for increased usage of automation tools across the Department, and improves Treasury's ability to audit and report on cybersecurity posture. The tools and services provided by Continuous Diagnostics and Mitigation (CDM) Phase 2 provide Treasury with an opportunity to implement TIES. This further aligns Treasury identity management with OMB M-19-17. This project aligns with the *Enhancements to Cybersecurity Infrastructure* initiative from the FY 2020 Budget.

Centralized Key Management Services (CKMS), +$865,000
This initiative will design, procure, and implement a centralized Treasury-wide key management service. The Department shares sensitive data across networks and multiple bureaus and is using encryption to mitigate risk to data at rest and in transit. In order to be truly effective at mitigating risk, encryption must be paired with strong cryptographic key management. Utilizing a centralized key management service will allow Treasury to bring all facets of crypto key management, including hardware, software, and processes, into one location.

This is increasingly important as the number of encryption keys continue to grow based on updated encryption requirements, as outlined in Cybersecurity Information Sharing Act of 2015. This project aligns with the *Enhancements to Cybersecurity Infrastructure* initiative from the FY 2020 Budget.

Cloud Access Security Broker (CASB), +$2,583,000
The Treasury Department, in accordance with various government-wide initiatives and industry practices, is migrating many of its internal systems to cloud-based systems using Platform as a Service (PaaS) and Software as a Service (SaaS). Treasury utilizes dozens of cloud environments. Every new cloud solution creates an aperture between our on premise solutions and these dozen cloud services through which a bad actor can enter and disrupt Treasury's mission. A Cloud Access Security Broker (CASB) will sit between Treasury Bureaus and cloud service providers to enforce security, compliance, and governance policies for and between the dozens of cloud applications used by Treasury. This project aligns with the *Enhancements to Cybersecurity Infrastructure* initiative from the FY 2020 Budget.

<u>Detect Cybersecurity Events +$550,000 / +1 FTE</u>
Goal: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

Cybersecurity Threat Hunting Analysis, +$550,000
The Government Security Operations Center (GSOC) collects a rich set of Treasury data from which to perform cyber threat identification. These datasets, however, provide only a subjective, narrow view from which to fully understand specific cyber threat activities and nation state cyber threat actors. This investment provides Treasury with access to commercial sources to supply the indicators and toolsets Treasury needs to identify malicious behavior within its datasets. Providing GSOC analysts with additional tools and a larger set of data via intelligence feeds would significantly enhance insight and understanding of cyber threat actors' command and control, infrastructure, and capabilities. This project aligns with the *Enhanced Incident Response and Recovery Capabilities* initiative from the FY 2020 Budget.

<u>Respond to Detected Cybersecurity Incidents +$3,359,000 / +1 FTE</u>
Goal: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

Enhanced Treasury Cyber/Fraud Management Capabilities, +$3,359,000
While the Department has robust incident management protocols in place on a per information system basis, Treasury's cross-system and inter-Bureau incident management needs to be better equipped to handle the interconnectivity and interdependence of the modern IT environment. This initiative drives the Department's ability to manage incidents related to cybersecurity and fraud by creating a cross-functional incident response team housed at the GSOC to improve inter-Bureau communication and systems integration to enable the team to quickly and efficiently respond to incidents. The Cyber/Fraud Fusion Incident Response will provide the ability to support analysis and triage of cybersecurity and fraud incidents with the goals of increasing detection, reducing potential dwell time between the detection and containment, and reducing the overall impact of an incident to the Treasury. This project aligns with the *Enhanced Incident Response and Recovery Capabilities* initiative from the FY 2020 Budget.

Recover by Maintaining Resilience and Restoration Plans +$1,000,000 / +0 FTE
Goal: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

HVA Security Enhancements, +$1,000,000
As noted in the HVA Security Enhancements initiative, the next phase of capabilities includes the remediation of assessment findings where the risks involved pose vulnerabilities to the enterprise. This will allow for the mitigation of enterprise level cyber risk discovered through the RVA/SAR assessments and/or other Enterprise Risk Management Activities and provide better visibility of Treasury's current cyber posture. This project aligns with the *Improving HVA Cybersecurity* initiative from the FY 2020 Budget.

Legislative Proposals

The Cybersecurity Enhancement Account has no legislative proposals.

Performance Highlights

Budget Activity	Performance Measure	FY 2017 Actual	FY 2018 Actual	FY 2019 Actual	FY 2020 Target	FY 2021 Target
CEA	Number of Major Incidents	N/A	0	0	2	0
CEA	Number of Reported Incidents	N/A	225	152	280	150
CEA	Percentage of High and/or Critical Findings from RVAs or SARs on Tier I HVAs that are closed by the end of the FY	N/A	N/A	57%	65%	75%
CEA	% of Cross-Agency Priority (CAP) Cybersecurity Key Performance Indicators (KPIs) that Treasury meets/exceeds OMB performance targets	N/A	60%	60%	B	80%

Description of Performance

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: Each fiscal year, Treasury tracks the number of cybersecurity incidents reported to the United States Computer Emergency Readiness Team (US-CERT). This measures the effectiveness of Treasury's defenses at mitigating security threats and indicates how often Treasury is being targeted by malicious actors. In FY 2019, Treasury had a greater ability to do more thorough analysis prior to declaring an incident. This drove some of the decreases in reported incidents. Natural variation in actual results also played a role in the variation from FY 2018 to FY 2019. As such, the FY 2021 target has been decreased to be in line with FY 2019 actuals.

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 recurring HVA review and assessment process.

Cross-Agency Priority (CAP) Cybersecurity Key Performance Indicator (KPI) Targets Met: The President's Management Agenda identifies CAP Goals to target those areas where multiple agencies must collaborate to effect change. In December 2018, OMB revised the CAP KPIs, eliminating several component measures that had been factored into the performance goals in FY 2018. The FY 2021 target of 80 percent will be met through mitigation of known vulnerabilities and deployment of additional cyber capabilities.