Cybersecurity Enhancement Account

Program Summary by Budget Activity

Dollars in Thousands

Budget Activity	FY 2020 Operating Plan	FY 2021 Operating Plan	FY 2022 Request	FY 2021 to FY 2022 $ Change	FY 2021 to FY 2022 % Change
Cybersecurity Enhancement Account	20,538	18,000	$132,027	114,027	633.5%
Total Program Operating Level	**$20,538**	**$18,000**	**$132,027**	**$114,027**	**633.5%**
Direct FTE	3	6	10	4	66.7%
Total Full-time Equivalents (FTE)	**3**	**6**	**10**	**4**	**66.7%**

Summary

The Department's strategic plan guides program and budget decisions for the Cybersecurity Enhancement Account (CEA).

To proactively and strategically protect Treasury Information Technology (IT) systems against cybersecurity threats, the FY 2022 budget request includes $132.027 million for the CEA. The total President's Budget requests $114.027 million to mitigate weaknesses identified through the SolarWinds incident at Treasury plus an additional $18 million for new and continued investments that support the critical IT improvements.

The FY 2022 discretionary request identified a cyber reserve of $750 million. The President's Budget allocates these resources to nine agencies that were significantly impacted by the SolarWinds incident, one of which is the Department of Treasury. The purpose of the funding is to address immediate response needs and does not focus on wholesale replacement of IT systems at this time. The funding request targets critical cybersecurity needs at these nine agencies which prioritizes basic cybersecurity enhancements, including: cloud security, Security Operations Center (SOC) enhancements, encryption, Multi-Factor Authentication (MFA), increased logging functions, and enhanced monitoring tools. Treasury is also bolstering its cybersecurity posture with investments that provide a comprehensive assessments to identify the breadth and depth of this attack, along with containment and post-incident analysis to ensure the appropriate response is deployed to both protect and minimize the impacts of such attacks in the future.

Treasury will use the CEA to centrally fund the assessment, response, recovery, and mitigation efforts to prevent or respond to instances where threat actors have the ability to pose a great risk to the Treasury IT infrastructure. The CEA is a multi-year account and managing CEA centrally allows Treasury to be more agile in its response to cybersecurity incidents and threats as well as leverage enterprise-wide services and capabilities. This account allows for enhanced efficiency, communication, transparency, and accountability around the mission of strengthening Treasury's cybersecurity posture. Treasury elevates the importance of such initiatives and provides Treasury leadership, OMB, and Congress with better transparency into cybersecurity activities across the Department.

The investments within the CEA account 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. Treasury believes the NIST's framework provides better clarity into the strategic focus of the Department's cybersecurity investments, aligns with accepted industry standards, guidelines, and practices, and allows Treasury to more effectively respond to government-wide reporting requirements.

Budget Highlights

Dollars in Thousands

	FTE	Amount
FY 2021 Operating Plan	**6**	**$18,000**
Changes to Base:		
Non-Recurring Costs	(6)	(18,000)
Subtotal Changes to Base	(6)	(18,000)
FY 2022 Current Services	**0**	**$0**
Program Changes:		
Program Increases	10	132,027
Identify the Business Context, Resources & Cybersecurity Risk	3	31,842
Protect the Delivery of Critical Infrastructure Services	3	50,433
Detect Cybersecurity Events	2	18,713
Respond to Detected Cybersecurity Incidents	2	21,258
Recover by Maintaining Resilience and Restoration Plans	0	9,781
Total FY 2022 President's Budget Request	**10**	**$132,027**

*The budget includes $114.027 million designated to strengthen Treasury's cybersecurity posture and address the impacts of the SolarWinds incident.

Budget Adjustments

Program Increases .....+$132,026,534 / +10 FTE

Identify the Business Context, Resources & Cybersecurity Risk +$31,841,424 / +3 FTE

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

Risk Management Framework (RMF) Automation Tool +$2,100,672 / +0 FTE

This is a continuation of a prior year request. While the FY 2021 request supports deployment in Departmental Offices (DO) and some Bureaus, the FY 2022 request plans to expand capabilities to all other Bureaus, including IRS.

The RMF Automation Tool initiative will replace the Treasury Federal Information Security Modernization Act (FISMA) Treasury Federal Information Management System (TFIMS). TFIMS is Treasury's system to track metadata, artifacts, and interconnections between systems. However, TFIMS currently operates largely as a document storage solution. It does not offer workflows or process automation and has limited reporting capabilities. The RMF Tool will automate a broad range of services for comprehensive, full integrated risk management, including controls scorecard measurement, dashboard reporting, and the generation of RMF System Assessment and Accreditation (SA&A) artifacts. Pivoting to digitally based processes will improve FISMA compliance without increasing security personnel costs. SA&A package generation within Treasury presently averages over 6

months. The RMF's automation and workflow capabilities will reduce costs and improve efficiency based on analysis of cybersecurity personnel workloads. It will also provide an integrated suite of ongoing authorization capabilities. The tool would be deployed within DO first and then progressively rolled out to Treasury Bureaus.

Enterprise Cyber Risk Management (ECRM) +$2,395,967 / +1 FTE
The Enterprise Cyber Risk Management (ECRM) initiative will continue to evolve Treasury's approach to managing risks across the enterprise and will begin a continuous review of all of Treasury's critical networks, systems, and data. ECRM enhances existing risk management processes through continuous planning, identification, categorization, prioritization, reporting, assessing, scoring, and remediation. Bureaus currently capture their system risk information into TFIMS. The ECRM ingests data from TFIMS, High Valued Assets (HVAs), Continuous Diagnostic and Monitoring (CDM) and other data sources at the department level to create an aggregated enterprise level cybersecurity risk register. This capability does not currently exist and implementing this process will enable Treasury to better understand the specific security needs of its most critical vulnerabilities, while gaining new insight as to how those vulnerabilities and mitigation strategies lower the risk across the larger federal enterprise. The funding and FTEs will support a continuous review of all enterprise risks which enables Treasury to achieve a better understanding of systems' cyber vulnerabilities and the associated costs. ECRM will also enable Treasury to better prioritize risks and quantify the levels of effort and magnitude needed to reduce risk exposure.

Supply Chain Risk Management Enhancements (SCRM) +$1,135,361 / +2 FTE
Supply chain risk management (SCRM) has become an increasingly critical cybersecurity issue The FY 2019 National Defense Authorization Act prohibited agencies from procuring or renewing contracts for equipment, systems or services that use certain covered telecommunications. During a recent GAO audit, seven findings related to Treasury's SCRM program were identified that must be addressed. The SCRM initiative will establish a process for Treasury to identify the types of hardware/software and third parties being utilized throughout Treasury and identify associated risks. This funding and FTEs will support efforts to identify SCRM risks and threats as well as provide needed support to bureaus in the form of guidance, facilitation of requirements, analysis, and tracking/oversight for software and hardware acquisitions.

NIST Cross-Functional Investments (Identify the Business Context, Resources & Cybersecurity Risk) +26,209,424 / +0 FTE
The following investments are allocated across multiple NIST framework categories for improving critical infrastructure cybersecurity.

Post-Incident Response +$5,397,500 / +0 FTE
Additional details about this investment is available at the end of this section.

Threat Hunting, Treasury-wide Log Collection, Management and Certificate Security for Identification Management +$20,811,924 / +0 FTE
Additional details about this investment is available at the end of this section.

Protect the Delivery of Critical Infrastructure Services +$50,432,839 / +3 FTE

Goal: Develop and implement appropriate safeguards to ensure delivery of critical services.

Cloud-Based Security +$7,500,000 / +0 FTE

Investments in cloud-based security will focus on the sufficient security of systems and information that have been moved to cloud-based platforms. This includes; assessing potential cloud services for alignment with established Federal Risk Authorization Management Program (FedRAMP) security baselines, acquiring tools to enhance the security of cloud-based applications, granting agency Authority to Operate (ATO) for systems and service with an existing FedRAMP ATO, and the granting of ATOs to cloud service providers.

High Value Assets (HVA) +$2,834,536 / +2 FTE

In FY 2017, Treasury began funding Risk Vulnerability Assessments (RVA) and Security Architectural Reviews (SAR) within the CEA Account. This has allowed Treasury to analyze key systems more frequently than the SARs/RVAs performed by the Department of Homeland Security (DHS). To date, Treasury has conducted 11 RVAs/SARs (9 in FY 2020 and 2 in FY 2021) outside of the DHS process. This request is estimated to fund approximately 18 additional assessments. These assessments include a review of Treasury's critical networks, systems, and data through a continuous cycle of planning, identification, categorization, prioritization, reporting, assessment, and remediation. This cycle enables Treasury to better understand the security needs of its most critical assets and how these assets fit into the larger Federal enterprise. The increase in funding and FTEs will support continuous reviews of all critical assets, systems, information, and data, which will help Treasury better understand what is on their network, what is valuable to their stakeholders, and what is valuable to individuals with malicious intent.

Infrastructure +$2,037,000 / +0 FTE

IT infrastructure improvements will include expanding the security controls for enterprise applications through secured license upgrades, expanded data processing and storage, and new recovery capabilities. This will help to protect the conversion of Active Directory Trusts to Federation, the hardening of shared service applications which provides for the authorization, and the authentication and single sign-on functionalities for applications and incident managements tools.

Centralized Key Management Services (CKMS) +$740,197 / +0 FTE

In the Cybersecurity Act of 2015, agencies were directed to encrypt information at rest and in transit. While increasing encryption ensures that data is being processed and stored securely, it also creates new requirements for managing the encryption keys required to access this data and increases the number of keys to be inventoried and managed. Further, Treasury may decide that segmenting keys by system, service, or mission function may be advantageous. As decisions are made to segment keys, tracking and maintaining inventory becomes increasingly complex.

This initiative is a second-year investment building upon a CEA FY 2021 request to design, procure, and implement a service for Treasury and its Bureaus to manage encryption keys centrally. The initial 12-month pilot will have been completed using CEA FY 2021 funds.

This request will be used to fund the subsequent 18 months needed to reach initial operating capabilities. Once operational, CKMS will provide Treasury with the ability to automate key management and quickly revoke keys should they be compromised. The ability to quickly revoke keys is important to keeping Treasury systems and data safe; it extends to the overall IT Operations environment, since expiring certificates/keys can contribute to availability failures.

NIST Cross-Functional Investments (Protect the Delivery of Critical Infrastructure Services) +37,321,106 / +1 FTE

The following investments are allocated across multiple NIST framework categories for improving critical infrastructure cybersecurity.

Post-Incident Response +$5,397,500 / +0 FTE
Additional details about this investment is available at the end of this section.

Treasury Shared Services Secure Operations Center (TSSSOC) +$8,707,267 / +1 FTE
Additional details about this investment is available at the end of this section.

Threat Hunting, Treasury-wide Log Collection, Management and Certificate Security for Identification Management +$23,216,339 / +0 FTE
Additional details about this investment is available at the end of this section.

Detected Cybersecurity Events +18,712,493 / +2 FTE

Goal: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

NIST Cross-Functional Investments (Detect Cybersecurity Events) +18,712,493 / +2 FTE

The following investments are allocated across multiple NIST framework categories for improving critical infrastructure cybersecurity.

Treasury Shared Services Secure Operations Center (TSSSOC) +$8,707,267 / +2 FTE
Additional details about this investment is available at the end of this section.

Threat Hunting, Treasury-wide Log Collection, Management and Certificate Security for Identification Management +$10,005,226 / +0 FTE
Additional details about this investment is available at the end of this section.

Respond to Detected Cybersecurity Incidents +$21,258,493 / +2 FTE

Goal: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

Incident Analysis +2,546,000 / +0 FTE

This investment is designated for Treasury's efforts in investigative, forensics, advisory and strategic support in response to ongoing cybersecurity incident response. DO will also strategically source additional professional support services to maintain daily operational needs and capabilities for incident response activities.

NIST Cross-Functional Investments (Respond to Detected Cybersecurity Incidents) +18,712,493 / +2 FTE

The following investments are allocated across multiple NIST framework categories for improving critical infrastructure cybersecurity.

Treasury Shared Services Secure Operations Center (TSSSOC) +$8,707,267 / +2 FTE

Additional details about this investment is available at the end of this section.

Threat Hunting, Treasury-wide Log Collection, Management and Certificate Security for Identification Management +$10,005,226 / +0 FTE

Additional details about this investment is available at the end of this section.

Recover by Maintaining Resilience and Restoration Plans +$9,781,285 / +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.

Enterprise Wide Cyber Exercise and Instrumentation +$998,000 / +0 FTE

This initiative will plan, conduct, and report results from a large-scale cyber exercise across Treasury, in addition to implementing security instrumentation that empowers incident responders to share a common system view. This would be the first enterprise wide cybersecurity exercise conducted by Treasury and would test existing incident plans to ensure that plans recover vital services in the order needed.

Treasury will also test to ensure that components work together effectively in the face of a large-scale cyber incident and ensure that existing instrumentation within Treasury (e.g. Splunk, SCCM, Active Directory, etc.) are normalized to report consistent information.

This initiative aims to improve visibility into cybersecurity efforts, encourage information sharing across Bureaus, identify potential gaps in present plans, and reduce inconsistencies between systems to provide Treasury leadership with a Department-wide view while working to protect information systems from attack and recover critical functionality.

Containment +5,092,000 / +0 FTE

These investments, to rebuild a clean environment, will provide full confidence to mission support activities. Safeguarding against threats requires investments to rebuild Treasury's compromised environment to mitigate threat of lateral movement/burrowing by adversaries.

NIST Cross-Functional Investments (Recover by Maintaining Resilience and Restoration Plans) +$3,691,285 / +0 FTE

The following investments are allocated across multiple NIST framework categories for improving critical infrastructure cybersecurity.

Threat Hunting, Treasury-wide Log Collection, Management and Certificate Security for Identification Management +$3,691,285 / +0 FTE

Additional details about this investment is available at the end of this section.

NIST Cross-Functional Investments

The following investments are allocated across multiple NIST framework categories for improving critical infrastructure cybersecurity.

- **Post-Incident Response,**

  This will enhance cybersecurity posture by addressing the IT architecture with investments in zero trust implementation, expanded SOC capabilities and data scanning tools for better threat analysis. The functions of this investment align with the Identify and Protect categories.

- **Treasury Shared Services Secure Operations Center (TSSSOC),**

  Treasury's Security Operations Centers (SOCs) are presently set up with GSOC to monitor the security for the perimeter of the Treasury enterprise's Trusted Internet Connections (TIC), while Bureaus are responsible for their own SOCs which monitor Bureau-specific perimeters and systems. All of Treasury's Bureaus utilize at least a portion of the 39 shared service services from the Treasury Franchise Fund. These services include programs that form the backbone of Treasury's HR systems (HR Connect) and security credentials (TEICAM). Currently, there is no dedicated SOC responsible for monitoring these shared services systems. This investment will establish the new SOC capabilities and FTEs will be supporting these efforts for implementation and ongoing monitoring.

  Presently, these systems utilize siloed approaches to incident response, log/vulnerability analysis, and system monitoring. While each system individually has some of these capabilities, no single entity has a mission to comprehensively manage them. This creates possible security gaps. As a result, past alerts have been missed, coordination problems exacerbated, and incident response time lengthened. For example, when security incidents occur that impact multiple systems, IT teams need additional time to manually consolidate data to obtain decisions from authorizing officials. Any delay in response time increases security risks for the shared services programs, some of which manage massive amounts of important data, such as HR Records and identity management. To cite a specific example, on August 29, 2019, an Enterprise Application Cybersecurity (EAC) system was improperly made Internet accessible. No alerts or alarms went off when Internet traffic started going to the system. EAC only possesses system-specific monitoring capabilities, and GSOC only monitors the Department's perimeter. All traffic had gone through Network Address Translation at Fiscal Service and consisted of valid, internal IPs. At the perimeter, GSOC did not possess system-specific workflow knowledge to discern "good" versus "bad" traffic, so they also did not raise any alarms. In this instance, Treasury was able to mitigate the problem, but any time an internal facing system is hacked or becomes exposed to the internet numerous potential risks can occur, including unauthorized access or data loss. The functions of the TSSSOC investment align with the Protect, Detect and Respond categories.

- **Threat Hunting, Treasury-wide Log Collection, Management and Certificate Security for Identification Management,**

  The funding and FTEs will be used to address the critical cybersecurity needs across the Treasury network enterprise to support the deployment and implementation of advanced network traffic protocol analysis, dynamic and static malware analysis, and applicable forensic analytics. This funding will also support the threat intelligence providing proactive posture with regards to emergent threats. Investments in annual exercises to identify threats in targeted systems provides for automated incident investigations and accelerates triage and response to operational incidents with advanced reporting and resource, and access to threat analysts. This will also assist in automating prevention and detection of malware, exploits, and in-process attacks through enhanced endpoint visibility. The functions of this investment align with the Identify, Detect and Respond categories.

Legislative Proposals

The Cybersecurity Enhancement Account has no legislative proposals.

Strategic Alignment

In accordance with the Government Performance and Results Act Modernization Act (GPRAMA) of 2010, the Department of the Treasury is currently developing the FY 2022 – 2026 Departmental Strategic Plan. The Strategic Plan is scheduled for publication in 2022. The Annual Performance Plan will be updated in the FY 2023 President's Budget to reflect new departmental strategic goals and objectives.

Performance Highlights

Performance Measure	FY 2018 Actual	FY 2019 Actual	FY 2020 Actual	FY 2021 Target	FY 2022 Target
Number of Major Incidents	0	0	1	0	1
Number of Reported Incidents	225	152	206	150	150
Percentage of Tier I HighValue 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	N/A	57	80	75	75
Risk Management Assessment Overall Rating %	68	68	75	DISC	DISC

Key: Disc - Discontinue

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.

On December 12, 2020, the Department of the Treasury notified the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) of a major security incident as a result of the Department's deployment of the SolarWinds Orion software product. The Department has completed compromise assessments, and all SolarWinds Orion products continue to remain offline across the Treasury Enterprise environment. The FY 2022 request includes additional funding to mitigate weaknesses identified through the SolarWinds incident and for investments that support critical IT improvements.

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 2020, Treasury witnessed a greater number of incidents being reported, this is indicative of increased threat activity coupled with enhanced detection and mitigation capabilities. The enhanced capabilities factored into the elevated target projection for FY 2020. Natural variation in actual results also played a role in the variation from FY 2019 to FY 2020. The FY 2021 target was decreased to reflect improved ability to validate incidents prior to submission. It was decided that the FY 2022 target should remain flat from FY 2021 numbers.

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% completion rate for system assessments and currently has a 77% closure rate for associated findings and POAMs. This focus helps to ensure that the proper POAMs are in place for all assessed systems and that they are being acted upon in a timely manner. The investment will focus on remediation of vulnerabilities, as well as increased review and reporting on corrective actions to resolve all findings and recommendations discerned during the assessment process. It was decided that the FY 2022 target should remain flat from FY 2021 numbers.

Additionally, the FY 2020 Risk Management Rating of 70 percent was exceeded through mitigation of known vulnerabilities and deployment of additional cyber capabilities. This performance measure was discontinued for FY 2021.