Cybersecurity Enhancement Account

Program Summary by Budget Activity

Dollars in Thousands

Budget Activity	FY 2016 Enacted	FY 2017 Annualized CR	FY 2018 Request	FY 2017 TO FY 2018 $ Change	FY 2017 TO FY 2018 % Change
Cybersecurity Enhancement Account	$0	$0	$27,264	$27,264	NA
Total Program Operating Level	**$0**	**$0**	**$0**	**$0**	**NA**
Direct FTE	0	0	19	19	NA
Total FTE	**0**	**0**	**19**	**19**	**NA**

Summary

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 Budget requests $27.264 million for the Cybersecurity Enhancement Account (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 cyber 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.

The CEA strengthens cybersecurity at Treasury and the nation's financial sector. This request is in addition to current bureau-level cybersecurity activities which remain in the base budgets of each Treasury bureau. As the CEA matures, Treasury will continue to look for targeted opportunities to provide shared and cost-effective enterprise solutions to improve cybersecurity defenses of Treasury and the U.S. financial sector.

FY 2018 Budget Highlights

Dollars in Thousands

Cybersecurity Enhancement Account	FTE	Amount
FY 2017 Annualized CR	**0**	**$0**
Program Increases:	19	$27,264
Malware Content Filter	0	$2,474
Data Loss Protection at the Fiscal Service Trusted Internet Connections (TIC)	0	$2,135
Enhanced Incident Response and Recovery Capabilities	4	$5,046
Cybersecurity Enhancements for Classified Networks	3	$1,050
Encrypted Traffic Inspection at the Fiscal Service Trusted Internet Connections (TIC)	0	$805
Enhancements to the Treasury Secure Data Network	0	$5,000
Proactive Cyber Risk and Threat Identification	3	$1,948
Improving the Cybersecurity of High Value Assets (HVA)	1	$3,537
Enhancements to Cybersecurity Infrastructure	0	$3,618
Mitigation of Cyber Threats to United States Financial Services Sector	8	$1,651
Total FY 2018 Request	**19**	**$27,264**

FY 2018 Budget Adjustments

Adjustments to Request

Malware Content Filter +$2,474,000 / +0 FTE

Treasury will fund web and email traffic inspection in virtual environments at the Treasury Enterprise Trusted Internet Connections. This allows dynamic analysis of potentially harmful email and web traffic in a controlled environment, enabling the Treasury enterprise security operations center to identify and remove malicious attachments and links before they reach the Treasury network. This will reduce the risk of compromise for the entire Treasury network, as well as systems housed on that network, including High Value Assets.

Data Loss Protection at the Fiscal Service Trusted Internet Connections (TIC) +$2,135,000 / +0 FTE

Funds will expand and accelerate implementation of Data Loss Protection at Treasury's Enterprise TICs and at select High Value Assets, enabling Treasury to detect the exfiltration of sensitive information by either threat actors or malicious insiders. This will allow Treasury to directly counter the threat of data loss through episodic/coordinated exfiltration. This will enhance Treasury's ability to detect, investigate, and respond to unauthorized attempts to access and remove sensitive taxpayer and financial data from the Treasury and bureau networks.

Enhanced Incident Response and Recovery Capabilities +$5,046,000 / +4 FTE

This request funds enhancements to response and recovery capabilities at Treasury's enterprise security operations center (SOC), the lead entity for Department-wide cybersecurity incident response and recovery actions, resulting in a faster response and recovery time. Traditionally this entails: retroactive examination of network traffic; assessment of adversarial movement within the network; determination of the level of information compromise; implementation of mitigations and countermeasures; and reconstitution/resurrection of damaged systems. This request also includes funding for deployment of an endpoint incident response capability, giving the enterprise SOC the ability to respond to incidents at the workstation level throughout the Department in a matter of minutes and hours rather than days and weeks.

Cybersecurity Enhancements for Classified Networks +$1,050,000 / +3 FTE

This request supports enhanced monitoring for the Treasury-wide collateral classified network, including security controls testing, monitoring of system security to include detection of and response to unauthorized user or anomalous network activity, as well as the secure implementation of identity and credential access management that provides a more secure environment for processing highly sensitive information. Funding also improves Treasury's ability to continuously monitor the network and detect and remediate security vulnerabilities, thereby reducing the risk of security incidents.

Encrypted Traffic Inspection at the Fiscal Service Trusted Internet Connections (TIC) +$805,000 / +0 FTE

Encryption is required to protect the confidentiality of sensitive network transactions. However, adversaries use encryption to conceal their command/control traffic and exfiltration activity. Treasury must be able to inspect encrypted network traffic for these threats. Enterprise TICs, housed at Fiscal Service, enhance Treasury's ability to detect, investigate, and respond to unauthorized attempts to access and remove sensitive data from the enterprise-wide Treasury network.

Enhancements to the Treasury Secure Data Network +$5,000,000 / +0 FTE

Funding will be allocated to the Treasury-wide SECRET collateral network to: increase overall stability; increase the timeliness of incident response and recovery; enhance security monitoring by the Government Security Operations Center; and provide advanced toolsets for automated monitoring, as well as analyst review of outputs from these toolsets.

Proactive Cyber Risk and Threat Identification +$1,948,000 / +3 FTE

The foundation of a strong cybersecurity program is proper identification of risk and threat vectors, and appropriate documentation of those risks and threats to enable decision making. This will be accomplished in part through strong security assessment and authorization of enterprise systems. Treasury will also establish a dedicated group of security experts to validate that systems across Treasury have been engineered and developed securely from the outset. Additionally, this group will carry out penetration tests to uncover vulnerabilities in systems throughout Treasury, including High Value Assets, before they are discovered or exploited by adversaries.

Improving the Cybersecurity of High Value Assets (HVA) +$3,537,000 / + 1 FTE

HVAs are information systems that Treasury has systematically designated as mission-critical and are the most common targets for computer network attacks. Cybersecurity improvements include the implementation of encryption for data in-transit—including public-facing web traffic in accordance with OMB M-15-13— and data at-rest. For FY 2018, this request includes funding to increase the resiliency of Treasury's HVA population through Risk and Vulnerability Assessments and Security Architecture Reviews. Funding will also be used to validate that, in the event of an intrusion, the affected HVAs have been properly cleaned and secured.

Enhancements to Cybersecurity Infrastructure +$3,618,000 / +0 FTE

Treasury will implement user access controls for sensitive applications and High Value Assets, including greater use of multi-factor authentication through Personal Identity Verification (PIV) cards. This funds operation and maintenance for those activities, and includes funding for improved security architecture design in conjunction with the Department of Homeland Security's Continuous Diagnostics and Mitigation program, Phase II. This design will result in enhanced security for privileged users across the Department, as well as identify and reduce operational risks in Treasury's access control architecture.

Mitigation of Cyber Threats to United States Financial Services Sector +$1,651,000 / +8 FTE

Increasing cyber-attacks against financial institutions could lead to a loss in confidence in these institutions and to significant economic impacts. As the government agency charged with coordinating with the financial sector on cybersecurity issues, Treasury seeks to expand its role as the Sector Specific Agency for the financial services sector under Executive Order 13636 Improving Critical Infrastructure Cybersecurity. The goal is to improve the public-private sharing of cybersecurity information, promote the use of best practices, and respond to cybersecurity incidents. In contrast with other initiatives in this budget request that support cybersecurity enhancements to Treasury Information Technology systems, this initiative seeks to mitigate cybersecurity threats to the U.S. financial infrastructure.

Explanation of Budget Activities

Cybersecurity Enhancement Account ($27,264,000 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 exception of the project to mitigate cybersecurity threats to the U.S. financial infrastructure, all projects have the common purpose of strengthening the security of Treasury's IT assets. 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. Treasury will work with OMB to select performance measures.

Legislative Proposals

The Cybersecurity Enhancement Account has no legislative proposals.