Cybersecurity Enhancement Account

Program Summary by Budget Activity

Dollars in Thousands

Cybersecurity Enhancement Account	FY 2015	FY 2016	FY 2017	FY 2016 to FY 2017	
Appropriated Resources	Enacted	Enacted	Request	$ Change	% Change
New Appropriated Resources:					
Internal Revenue Service	0	0	62,084	62,084	0.00%
Treasury-wide	0	0	47,743	47,743	0.00%
Subtotal New Appropriated Resources	**$0**	**$0**	**$109,827**	**$109,827**	**0.00%**
Total Budgetary Resources	**$0**	**$0**	**$109,827**	**$109,827**	**0.00%**

Summary

The Cybersecurity Enhancement Account (CEA) is a new dedicated account designed to bolster the Department's cybersecurity posture and mitigate cybersecurity threats to the U.S. financial infrastructure.

Due to increasing cyberattacks on critical government systems Treasury aims to mitigate this escalating risk by creating a new and centralized cybersecurity account. CEA supports the Treasury Department Strategic Goal 3 to "Fairly and effectively reform and modernize federal financial management, accounting, and tax systems," Strategic Goal 4 to "Safeguard the financial system and use financial measures to counter national security threats," and Strategic Goal 5 to "Create a 21st-century approach to government by improving efficiency, effectiveness, and customer interaction."

The creation of a centralized program and dedicated funding source for cybersecurity will enhance Department-wide coordination of cybersecurity efforts and improve the Department's responsiveness to cybersecurity threats. It will also provide leadership with greater visibility into cybersecurity efforts and further encourage information sharing across Bureaus. The program will improve the identification of these threats and better protect information systems from attack. With high-level leadership support, the program will also provide a platform to enhance efficiency, communication, collaboration, and transparency around a common goal—improving not only the cybersecurity of the Department of the Treasury, but also that of the nation's financial sector.

In FY 2017, the program includes investments in two budget activities (Treasury-wide and the Internal Revenue Service (IRS)). Spending on existing activities remains in the base budgets of each bureau. As the program matures, the goal is to integrate additional cybersecurity investments to fully leverage centralized cybersecurity leadership and expertise across the Department.

The $48 million in Department-wide funding focuses on critical improvements to Treasury-wide systems including the Treasury Secure Data Network, the Fiscal Service Trusted Internet Connections, and the other systems that have been identified as High Values Assets. The investments focus on identifying and protecting information systems; detecting threat actors; and responding to and recovering from cyber incidents. A portion of the resources will also support a dedicated innovation fund for evolving high impact cyber investments throughout the Department.

The $62 million in IRS investments focus on two main initiatives: Cyber Defense and e-Authentication. The IRS will enhance the security of its overall networks via the use of a cyber threat forensics capability, implementation of a comprehensive patch management system, and the adoption of government-wide information security continuous monitoring (ISCM) tools as parts of a layered defense. In this Budget request, the IRS invests in the technology that allows for timely risk assessments, strong prevention techniques, and analysis of data that can identify and develop solutions for stolen identity theft refund fraud.

Treasury Cybersecurity Enhancement Account FY 2017 Budget Highlights

Dollars in Thousands

Cybersecurity Enhancement Account	FTE	Amount
FY 2016 Enacted	**-**	**-**
Program Changes:		
Program Increases:	80	$109,827
IRS Program Increases		
Cyber Defense	16	$54,732
e-Authentication	19	$7,352
Treasury-wide Program Increases		
Pooled Innovation Fund for Evolving High Impact Cyber Investments	-	$10,000
Encrypt Sensitive Data at Rest and in Motion	-	$7,440
User Access Controls for Sensitive Applications	-	$5,727
Digital Infrastructure Security Team	22	$5,000
Digital Infrastructure Security Team (existing DO S&E program funded in the CEA)	6	$2,000
Treasury Secure Data Network (TSDN) System Upgrades and Security Enhancements	4	$4,717
Detect System Vulnerabilities and Unauthorized Data Transfers	-	$3,360
Enhance Incident Response and Forensics Capabilities	-	$2,325
Proactive Cyber Risk and Threat Identification	3	$2,098
Mitigate Cyber Threats to U.S. Financial Infrastructure	8	$1,651
Proxying Capability at the Fiscal Service Trusted Internet Connections (TICs) for Encrypted Traffic Inspection	-	$1,375
IT Cybersecurity Enhancements (existing DO S&E program funded in the CEA)	2	$1,050
Web Domain Encryption	-	$1,000
Total FY 2017 Request	**80**	**$109,827**

FY 2017 Budget Adjustments

IRS Program Increases

Cyber Defense +$54,732,000 / +16 FTE

This investment provides a set of capabilities that protect the IRS's sensitive data and enhances the security posture of its IT infrastructure. It provides funding to secure data leading to the prevention and elimination of vulnerabilities associated with sensitive but unclassified data; to conduct external site reviews ensuring security controls are in place; to implement a consistent, government-wide set of information security continuous monitoring tools; and to provide a comprehensive incident response capability bolstering the resilience of mission critical IRS operations and their enabling technologies.

e-Authentication +$7,352,000 / +19 FTE

This investment funds the design and implementation of a common service to verify user identity, register individuals, and provide and validate their credentials allowing taxpayers expanded access to IRS data through the use of mobile devices, cloud computing, and collaborative technology.

Treasury-wide Program Increases:

Pooled Innovation Fund for Evolving High Impact Cyber Investments +$10,000,000 / +0 FTE

To ensure that new and ever-evolving threats can be rapidly addressed before they are exploited, Treasury requests resources for a pooled innovation fund designed for Department-wide high impact cyber initiatives. Treasury leadership will manage the fund, to include receiving solicitations from across the Department and managing and dispersing resources based on criteria and need at Treasury offices and bureaus.

Encrypt Sensitive Data at Rest and in Motion +$7,440,000 / +0 FTE

In addition to protecting information residing on HVAs through access control, Treasury has also identified several opportunities to protect these systems' data at rest and in motion. This initiative area would support strong encryption of data at rest within HVA databases as well as encrypt data in transit via email and public-facing websites. This would also enable secure cloud computing by establishing a cloud environment certified at the Federal Risk and Authorization Management Program's (FedRAMP) High security baseline. This initiative will also protect sensitive data through enhanced deployment of application firewalls and expanded user awareness training, which would lessen the risk of malicious and unintentional data breaches, respectively.

User Access Controls for Sensitive Applications +$5,727,000 / +0 FTE

Funding will strengthen the identification and authentication requirements for users logging on to individual Treasury applications. Strengthening these systems will decrease the likelihood that an intruder on the network will be able to access sensitive information regarding the public, the economy and the Treasury workforce that is housed in these applications by implementing strong authentication at both the application level and the network level for applications identified as High Value Assets (HVAs).

Digital Infrastructure Security Team +$7,000,000 / +28 FTE

The FY 2016 Consolidated Appropriations Act provides $2,000,000 and six FTE in the Departmental Offices (DO) Salaries and Expenses (S&E) account to establish a Digital Infrastructure Security Team (DIST). Because of the Treasury-wide cybersecurity focus of this initiative, Treasury proposes to fund this initiative in the CEA in FY 2017. To build on the $2,000,000 provided in the FY 2016 Consolidated Appropriations Act in the Departmental Offices (DO) Salaries and Expenses (S&E) account, Treasury requests an additional $5,000,000 and 22 FTE, which will form a centralized cohort of web/cyber experts to protect and transform Treasury's digital services. They will have a specific focus on a secure system that promotes ease of use and system cost-effectiveness, as well as possesses a robust virtual cybersecurity infrastructure to protect Treasury's cyber assets, especially those assets with the greatest impact to citizens. Treasury's digital government strategy will continue to be guided by four principles:

- Prioritizing the safe and secure delivery and use of digital services and protecting information and privacy;
- Enabling secure access to high-quality digital government information and services anywhere, anytime, on any device;
- Unlocking the power of government data to spur innovation and improve the quality of services; and
- Procuring and managing secure devices, applications, and data in smart and affordable ways.

The digital service experts on the team will bring best practices in the disciplines of cybersecurity, design, software engineering, and product management to bear on the agency's most important services Treasury will increase operational and technical controls related to essential digital services functions, including security and privacy oversight, web application security, vulnerability assessment, predictive intelligence analysis, privacy analysis, and security coding and testing. This initiative will protect the data and infrastructure that supports U.S. citizens, while improving accessibility and maintaining transparency.

Treasury Secure Data Network (TSDN) System Upgrades and Security Enhancements +$4,717,000 / +4 FTE

This investment will fund critical improvements to the TSDN in three areas:

- Treasury requests hardware and technical support to transform TSDN into a private cloud at a remote data center. Through virtualization, the network will be more secure and facilitate faster patching of newly discovered vulnerabilities. Replacing this aging hardware with a cloud-based model will also improve mission productivity for system users, who are carrying out Treasury's most sensitive functions;
- This investment will increase incident response after-hours system maintenance and improve identification of anomalous and/or malicious behavior. This investment in hardware, software, technical support and FTE will increase the NOC/SOC capabilities for the TSDN and enhance security monitoring of the TSDN perimeter to a level commensurate with the system's sensitivity; and
- This request will provide advanced toolsets for automated monitoring, as well as a dedicated analyst to review outputs from these toolsets. These capabilities will enable better detection of anomalous internal TSDN traffic, such as unauthorized attempts to access information and suspicious exfiltration of data. These additional safeguards will also enable compliance with several areas of Executive Order 13587, which instructs agencies operating classified networks to appropriately share and safeguard classified information on computer networks.

Detect System Vulnerabilities and Unauthorized Data Transfers +$3,360,000 / +0 FTE

The longer a breach goes unnoticed, the higher the probability that its severity will increase. For this reason, detection of anomalous and/or malicious activity must be spotted quickly. Increased deployment of data loss prevention tools to Treasury's sensitive enterprise information systems will improve the Department's ability to detect unauthorized access of information and track its movement across the network. Additionally, Treasury will adopt advanced intrusion detection methods and systems used by credit card companies to detect anomalous behavior to improve Treasury's ability to detect malicious actors within its networks.

Enhance Incident Response and Forensics Capabilities +$2,325,000 / +0 FTE

In the event that malicious activity is discovered on Treasury's networks, rapid response to and recovery from said activity is largely reliant on being able to examine past network traffic to understand where the adversary has traveled within the network, what information has been compromised, and how to mitigate and minimize the damage. Treasury needs to extend its retention of key data sources in order to support forensics and investigations of cyber incidents. Treasury seeks to enhance its respond and recover capabilities by extending network traffic capture and increase its capacity to aid bureaus during cyber incident investigations. This will result in a faster response and recovery time in the event of a cyberattack.

Proactive Cyber Risk and Threat Identification +$2,098,000 / +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 have been engineered and developed securely from the outset. Additionally, this group will carry out penetration tests to uncover vulnerabilities in Treasury's systems before they are discovered or exploited by adversaries.

Mitigate Cyber Threats to U.S. Financial Infrastructure +$1,651,000 / +8 FTE

Treasury requests funds and personnel to expand Treasury's capabilities to promote the security and resilience of the financial services sector. (Treasury is the sector-specific lead agency under Presidential Policy Directive 21: Critical Infrastructure Security and Resilience.) The request will allow Treasury and its partners, including other federal agencies, to expand work with the financial services sector to improve the sharing of cybersecurity information, promote the use of best practices, and respond to cyber incidents.

- Information Sharing. Over the past several years, malicious cyber activity has increased, and the financial services sector has been one of the major areas of concern. The number and extent of threats to financial services networks has grown significantly. To guard against these threats, it is vital to share timely and actionable cybersecurity information among the public and private sectors. Working closely with the Department of Homeland Security, the Federal Bureau of Investigation, and the Intelligence Community, Treasury develops timely and actionable information sharing products tailored specifically to the financial services sector. However, Treasury needs to expand and enhance its efforts to match the rapid increase in malicious cyber activity;
- Best Practices. Treasury also is responsible for promoting the use of best practices among the financial services sector. These best practices help improve baseline security levels. Treasury works to ensure that the needs and interests of the financial services sector are represented as such guidelines are developed and communicates opportunities for firms to participate in their development directly or through trade associations or consortia. Treasury requires additional specialized staff with knowledge or experience from the financial services sector who are experienced in how to engage the wider financial services community in the development, implementation, and promotion of voluntary cybersecurity standards and best practices in the sector and can operate from Treasury's neutral perspective of promoting security, but not a specific technology; and
- Incident Response. Treasury is responsible for coordinating with firms and other agencies to respond to significant cyber incidents affecting the financial services sector. The number of significant cyber incidents impacting the financial services sector continues to rise. Therefore, Treasury must expand its capabilities to plan for and respond to major incidents through a strong and growing cybersecurity exercise program for the financial services sector and the development of appropriate incident response plans.

Proxying Capability at the Fiscal Service Trusted Internet Connections (TICs) for Encrypted Traffic Inspection +$1,375,000 / +0 FTE

Internet traffic is increasingly composed of encrypted messages that Treasury is unable to scan for threats. The procurement of additional hardware, software and Fiscal Service support will allow for 100 percent inspection of all in-bound and out-bound encrypted internet traffic and support compliance with Data Loss Prevention (DLP) policies.

IT Cybersecurity Enhancements +$1,050,000 / +2 FTE

The FY 2016 Consolidated Appropriations Act provides $1,050,000 and two FTE in the DO

S&E account for security enhancements to classified networks and expansion of DO's Wireless Intrusion Prevention System. Because of the cybersecurity focus of this initiative, Treasury proposes to fund this initiative in the CEA in FY 2017.

Web Domain Encryption +$1,000,000 / +0 FTE

This request meets compliance requirements for the OMB mandate M-15-13, requiring that all publically accessible federal websites and web services only provide service through a secure connection. Treasury will use these funds to ensure compliance of all new services and websites, as well as complete the transition of legacy sites.

Explanation of Budget Activities

Internal Revenue Service ($62,084,000 from direct appropriations)

The Department requests dedicated funding for IRS to strengthen the security posture of its IT infrastructure and to improve authentication technologies allowing taxpayers expanded access to web-based IRS account data.

Treasury-wide ($47,743,000 from direct appropriations)

The Treasury Department requests funds that have a Treasury-wide focus to bolster the Department's cybersecurity posture and mitigate cybersecurity threats to the U.S. financial infrastructure.

Legislative Proposals

The Treasury Cyber Program has no legislative proposals.