Department of the Treasury Cybersecurity Enhancement Account

Congressional Budget Justification and Annual Performance Report and Plan

FY 2021

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 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 going forward 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.

1.1 – Appropriations Detail Table

Dollars in Thousands

Appropriated Resources	FY 2019 Operating Plan		FY 2020 Enacted		FY 2021 Request		FY 2020 to FY 2021 % Change	
New Appropriated Resources	**FTE**	**AMOUNT**	**FTE**	**AMOUNT**	**FTE**	**AMOUNT**	**FTE**	**AMOUNT**
Cybersecurity Enhancement Account	12	$25,208	11	$18,000	6	$18,000	-45.5%	0.0%
Total Budgetary Resources	**12**	**$25,208**	**11**	**$18,000**	**6**	**$18,000**	**-45.5%**	**0.0%**

Note: FTE = Full-time Equivalent employment

1.2 – Budget Adjustments Table

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**

C – Budget Increases and Decreases Description

Non-Recurring Costs ..... -$18,000,000 / -11 FTE

FY 2020 Non-Recurring Investments -$18,000,000 / -11 FTE

This amount represents non-recurring initial investments.

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. The Cybersecurity Risk Model initiative will identify, quantify, access, prioritize, and report on Enterprise Cyber Risks found across the Treasury Department. The Cybersecurity Risk Model will also quantify and prioritize Enterprise Cyber risk. This will allow the Department to prioritize mitigation of risks associated with cyber attacks based on their likelihood of occurrence. Treasury's implementation of the Cybersecurity Risk Model will also help meet mandated requirements set by OMB, NIST and DHS. 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 investment will reduce the manual workload required to separately assess the Department's risk profile and allow Treasury's cybersecurity staff to see an accurate, current picture of cybersecurity risk and vulnerability vectors. This insight and improved understanding of the Department's risk posture will further Treasury's ability to continue to make critical IT decisions and cybersecurity investments with the proper risk vectors in mind going forward. 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 replace 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. As an example, an average SA&A artifact is over 400 pages long. The RMF will provide an integrated suite of ongoing authorization capabilities to streamline the process of creating, maintaining, and reviewing SA&A artifacts. Across Treasury, there are over 1,600 Federal employees who have responsibilities with respect to preparation of SA&A artifacts, and who could see reductions in their Cybersecurity-related tasks of up to 10 percent. Based on a conservative reduction of 5 percent, a total possible estimated person-hour workload reduction would still exceed 25,000 hours. 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.

High Value Asset (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 coordinated 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 those additional assessments. These assessments will be compliant with OMB, DHS, and National Institute of Standards and Technology requirements and standards. Capabilities implemented to date include the implementation of HVA governance framework, which includes the annual recurring requirement for the identification of Treasury HVAs, and the execution of additional RVAs and SARs. This next phase falls under the Recover NIST CSF category—for more information please refer to the Recover section below. The next phase of capabilities includes the development and implementation of an HVA risk management framework, RVA and SAR evaluation methodology, the execution of RVAs and SARs across the department, as well as 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.

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. For example, the increases in computational power from practical quantum computing at scale would have a significant impact on several cryptographic algorithms currently in wide use. This initiative would analyze IT advancements and the evolving threat environment as it pertains specifically to the Treasury Department. It would seek to understand how new technological advancements may impact Treasury's systems (specifically Treasury HVAs) and work to develop strategies to safeguard the data entrusted to the Department. 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. Decentralized identity solutions housed across Bureaus have created data silos, non-standardized processes, and inconsistent identity management capabilities that lack efficiency and necessary support for automated provisioning. Altogether, the lack of a centralized identity solution increases Treasury's vulnerability to security threats across the landscape and hinders Treasury's ability to achieve overall cost savings in identity management. 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. In addition to

tracking new keys, Treasury also needs to continue to track updates to existing keys. Key rotation reduces the time a potentially compromised key is active. Coupled together, newly encrypted platforms and ongoing key rotations for existing encryption services result in an exponentially growing volume of encryption keys. Keeping up with this volume would call for unsustainable amounts of manpower to maintain synchronicity across multiple bureau sites. A centralized key management service would be agnostic to hosting provider and allow Treasury's bureaus to centrally manage encryption keys, as well as automate and quickly revoke keys in case of compromise. This will contribute to an increase in the number of keys inventoried and managed while reducing availability failures as a result of expiring certificates/keys. 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. The CASB will allow Treasury to extend the security controls of our on-premises infrastructure to the cloud. Manually governing each of these solutions separately would require a time-consuming implementation. Implementing a CASB is critical for Treasury to efficiently adopt cloud services in a secure fashion. If this initiative is not funded, Treasury will struggle to implement appropriate security controls in a cost effective and reliable fashion. Lack of a CASB will slow Treasury's adoption of cloud, bringing security and mission risk to the Department and its Bureaus. 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
Cyber threat hunting is an active cyber defense activity using data collected by Treasury, in contrast to traditional threat management measures which investigate after warning of a threat. 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. The commercial industry offers a variety of data in a variety of formats that cover the spectrum of cyber threat intelligence. This includes registration information for domains and IP addresses that could be malicious and passive DNS data collected around the globe. Integrating a fuller, more comprehensive dataset into the daily analytic cyber threat hunt process would increase situational awareness and cyber threat

preparedness while enabling earlier threat detection to defend the Treasury enterprise. This project aligns with the *Enhanced Incident Response and Recovery Capabilities* initiative from the FY 2020 Budget.

Respond to Detected Cybersecurity Incidents +$3,359,000 / +1 FTE
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. With Treasury's increased profile and role in the National Security apparatus, understanding linkages between systems and being able to quickly identify and combat cybersecurity threats is increasingly important. Differences in security posture within and outside of Treasury increase vulnerability of Treasury High Value Assets (HVAs) across the enterprise. 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. Every minute of delay means more data exfiltrated or destroyed, and improving incident response capability can mitigate and reduce overall impact to the Treasury mission. If this initiative is not funded, Treasury will continue to lack the necessary process and tools to manage incidents that cross-cut multiple Bureaus and information systems despite the ever-increasing sophistication, frequency, impact and brazenness of global cyber threats. 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.

1.3 Object Classification (Schedule O) Obligations

Dollars in Thousands

Object Classification	FY 2019 Actual Obligations	FY 2020 Estimated Obligations	FY 2021 Estimated Obligations
11.1 - Full-time permanent	1,736	1,909	1,235
11.5 - Other personnel compensation	28	0	0
11.9 - Personnel Compensation (Total)	**1,764**	**1,909**	**1,235**
12.0 - Personnel benefits	552	570	369
Total Personnel and Compensation Benefits	**$2,316**	**$2,480**	**$1,604**
21.0 - Travel and transportation of persons	1	0	0
23.3 - Communications, utilities, and miscellaneous charges	0	82	1,343
25.1 - Advisory and assistance services	25,671	10,307	14,039
25.2 - Other services from non-Federal sources	3	0	1,033
25.3 - Other goods and services from Federal sources	973	1,034	738
25.7 - Operation and maintenance of equipment	1,783	9,627	2,660
26.0 - Supplies and materials	10	0	0
31.0 - Equipment	1,838	276	3,438
32.0 - Land and structures	0	147	0
Total Non-Personnel	**$30,279**	**$21,473**	**$23,251**
Total Obligations	**$32,595**	**$23,953**	**$24,855**
Full-time Equivalents (FTE)	**12**	**11**	**6**

Amounts Reflect obligations of annually appropriated resources, carryover balances, reimbursables, and transfers.

D – Appropriations Language and Explanation of Changes

Appropriations Language	Explanation of Changes
DEPARTMENT OF THE TREASURY DEPARTMENTAL OFFICES 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] *2023*: Provided, That such funds shall supplement and not supplant any other amounts made available to the Treasury offices and bureaus for cybersecurity: Provided further, That of the total amount made available under this heading $1,000,000 shall be available for administrative expenses for the Treasury Chief Information Officer to provide oversight of the investments made under this heading: Provided further, That such funds shall supplement and not supplant any other amounts made available to the Treasury Chief Information Officer. *(Department of the Treasury Appropriations Act, 2020.)*	*None*

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 2015 Actuals	FY 2016 Actuals	FY 2017 Actuals	FY 2018 Actuals	FY 2019 Actuals	FY 2020 Enacted	FY 2021 Request
Appropriated Resources	0	0	$47,743	$24,000	$25,208	$18,000	$18,000
Budget Activity Total	**0**	**0**	**$47,743**	**$24,000**	**$25,208**	**$18,000**	**$18,000**
Full-time Equivalents (FTE)	**0**	**0**	**1**	**8**	**12**	**11**	**6**

Note: The FY 2015 – 2019 appropriated resources represents the approved operating plan. FY 2015 - FY 2019 FTE are actuals.

2.1.2 Cybersecurity Enhancement Account Resources and Measures

Performance Measure	FY 2015 Actual	FY 2016 Actual	FY 2017 Actual	FY 2018 Actual	FY 2019 Actual	FY 2019 Target	FY 2020 Target	FY 2021 Target
Number of Major Incidents	N/A	N/A	N/A	0	0	2	2	0
Number of Reported Incidents	N/A	N/A	N/A	225	152	280	280	150
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	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	N/A	N/A	N/A	57%	55%	65%	75%
Risk Management Assessment Overall Rating	N/A	N/A	N/A	68%	68%	60%	70%	DISC
% of Cross-Agency Priority (CAP) Cybersecurity Key Performance Indicators (KPIs) that Treasury meets/exceeds OMB performance targets	N/A	N/A	N/A	60%	60%	B	B	80%

Key: DISC – Discontinued; B – Baseline

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 volume 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: 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. If the number of reported incidents rises while the number of major incidents remains steady or declines, it indicates 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 measure. As reflected in the *Actual* value column, there was a reduction in incidents to 159 for FY 2019 in comparison to those projected by Treasury. The target goal of 280 for FY 2019 was chosen as an increase in recognized incidents of up to 25 percent from FY 2018 actuals, applying the same criteria, within the FY 2019 timeframe was expected. In order to allow time to increase preventative measures effectiveness, it was decided that the FY 2020 target should remain flat from FY 2019 numbers.

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. In the past three years, Treasury's CEA performance targets were based upon the percentage of HVA system assessments/reviews that were conducted in a timely manner. Treasury has consistently recorded a 100 percent completion rate, even though it faced increasing challenges over the mid- and long-term period. Treasury will now focus on steps to address findings resulting from these assessments. This focus will assure that the proper Plans of Action and Milestones (POAMs) are both in place for all reviewed systems and that the POAMs have been 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.

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. The Cybersecurity KPIs for FY 2018-2020 focus on capabilities that the Office of Management and Budget (OMB) has determined will, when implemented appropriately, provide the most effective improvements to cybersecurity across the federal enterprise. OMB established the initial Cybersecurity CAP KPIs for FY 2018-2020 in April 2018. In December 2018, OMB revised the CAP KPIs, eliminating several component measures that had been factored into the performance goals in FY 2018. As a result of these changes, Treasury met the same number of KPI targets at the end of FY 2019 as it had met in FY 2018. Improvement is anticipated in FY 2021 due to maturing cybersecurity enhancement investments made in prior years. The FY 2021 target Risk Management Rating of 80 percent will be met through mitigation of known vulnerabilities and deployment of additional cyber capabilities.

C – Changes in Performance Measures

The following are proposed changes in performance measures from the previous year President's Budget.

Performance Measure or Indicator	Proposed Change and Justification
1. Replace "*Risk Management Assessment (RMA) Overall Rating*" with CAP KPI targets met (substitution)	While RMA was a focus of senior leadership in FY 2018, it has since been supplanted by the Cross-Agency Priority (CAP) Cybersecurity Key Performance Indicators (KPIs). The Cyber CAP KPIs leverage the CIO FISMA reporting metrics much as the RMA does, focusing on a smaller number of high-priority capabilities.
2. Replace "*% of Tier I HVAs where RVAs or SARs are completed on time*" with "*% of High and/or Critical Findings from RVAs or SARs on Tier I HVAs that are closed by the end of the FY*" (substitution)	The percentage of RVAs and SARs completed on a timely basis for Treasury's HVAs had consistently reached a level of 100 percent based on previous investment. This percentage left no room for continued improvement. The HVA investment will now evolve and refocus on making systemic improvements based on remediation and corrective actions taken to address assessment findings and vulnerabilities once they are identified.

D – Evidence-Building Activity

CEA initiatives result from the ongoing analysis and review of current risk posture (threat, configuration, and operational data). This is accomplished through proactive RVAs and SARs, which generate data to inform leadership where critical remediation is required and to identify opportunities to leverage shared services to solve common problems across the Department. Metrics surrounding detection, attack vectors, depth into our defenses, and containment inform

operational decisions on capabilities and configurations for the defensive and analytical capabilities in the Department's cybersecurity infrastructure. The CEA is also critical to systematize and automate the collection of cybersecurity operational data, increasing its accuracy and accelerating its availability so that resources and organizational capacity can be directed in a timely and efficient manner. Improvements in these foundational capabilities will improve Treasury's ability to use data to refine the operational decision-making process.

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:
https://www.treasury.gov/about/budget-performance/Pages/summary-of-capital-investments.aspx.
The website also contains a digital copy of this document.