DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

July 29, 2016

The Honorable Orrin Hatch
Chair
Committee on Finance
United States Senate
219 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Ron Wyden
Ranking Member
Committee on Finance
United States Senate
221 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Ron Johnson
Chair
Committee on Homeland Security and Governmental Affairs
United States Senate
340 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate
513 Hart Senate Office Building
Washington, D.C. 20510

Re: Cybersecurity Act of 2015, Section 406 – Department of the Treasury
(OIG-CA-16-033B)

Dear Messrs. Chairmen and Ranking Members:

The Cybersecurity Act of 2015 (Public Law 114-113, Division N), Section 406, requires that Inspectors General of agencies operating a "covered system" report on the agencies' information security policies, procedures, and practices for controlling access to such systems. A covered system means a national security

system as defined in 40 U.S.C. §11103, or a Federal computer system that provides access to personally identifiable information (PII).

Cyber threats to all Federal information systems are an ongoing challenge, and as such, we have reported this as the Department of the Treasury's (Treasury) top management and performance challenge for the past two years.[1, 2] We recognize that continued vigilance on the part of Treasury is necessary to safeguard systems critical to the functions of government and the Nation's financial infrastructure. Accordingly, my office has also been attentive in its oversight of this area.

In this regard, I am transmitting the results of my office's review of covered systems hosted by Treasury bureaus and offices and the information systems policies, procedures, and practices related to secure access to such systems. Our review also included whether appropriate standards were followed in operating Treasury's covered systems. It should be noted that the scope of our work did not include covered systems and the related policies, procedures and practices followed by the Internal Revenue Service and its respective Inspector General, the Treasury Inspector General for Tax Administration.

To meet our requirements under Section 406, we reviewed logical access policies and practices used by Treasury's bureaus and offices. We also reviewed logical access controls and multi-factor authentication used to govern access by privileged users. In addition, we reviewed policies and procedures with respect to inventories of software licenses, and capabilities used for data loss prevention, forensics and visibility capabilities, and digital rights management capabilities. Finally, we reviewed policies and procedures to ensure that Treasury's bureaus and offices, including their contractors, implemented security management practices.

In brief, we found that Treasury uses appropriate standards:

- National Institute for Standards and Technology (NIST) special publications (SP),
- Federal Information Processing Standards (FIPS) publications,
- Office of Management and Budget (OMB) policies and guidance,
- Homeland Security Presidential Directive 12 (HSPD 12)
- Committee on National Security Systems Directives (CNSSD) and Committee on National Security Systems Instructions (CNSSI)

---

[1] Management and Performance Challenges Facing the Department of the Treasury (OIG-CA-16-002; issued Oct. 30, 2015) (https://www.treasury.gov/about/organizational-structure/ig/Audit%20Reports%20and%20Testimonies/oigca16002.pdf)

[2] Management and Performance Challenges Facing the Department of the Treasury (OIG-CA-15-001; issued Oct. 23, 2014)) (https://www.treasury.gov/about/organizational-structure/ig/Audit%20Reports%20and%20Testimonies/OIGCA15001.pdf)

- Treasury Directives Publication (TD P): 85-01 Volumes I and II, *Treasury Information Technology Security Program,* and TD P 15-03, *Treasury Directive Publication Intelligence Information Systems Security Policy Manual,* which reference other Federal standards in Treasury's overarching policies and procedures.

In addition, Treasury bureaus and offices reference TD P 85-01, TD P 15-03, and aforementioned Federal standards to establish both bureau-specific and system-specific policies.

The following summarizes the results of our review. Please refer to the enclosure for details of each area of concern.

Description of the logical access policies and procedures to access a covered system

Treasury's policies established in TD P 85-01 and TD P 15-03 are based on guidance from NIST SP, FIPS, OMB, HSPD 12, and CNSSD. Treasury's offices and bureaus established specific bureau or system policies and procedures (e.g., system security plans) to implement Treasury policies.

Description and list of the logical access controls and multi-factor authentication used to access a covered system by privileged users

Treasury directives, TD P 85-01 and TD P 15-03, established policies for the following controls:

Access Controls
AC-1: Access Control Policy and Procedures
AC-2: Account Management
AC-3: Access Enforcement
AC-4: Information Flow Enforcement
AC-5: Separation of Duties
AC-6: Least Privilege
AC-7: Unsuccessful Logon Attempts
AC-10: Concurrent Session Control
AC-11: Session Lock
AC-12: Session Termination
AC-14: Permitted Actions without Identification or Authentication
AC-17: Remote Access
AC-18: Wireless Access
AC-19: Access Control for Mobile Devices
AC-20: Use of External Information Systems
AC-21: Information Sharing

Identification and Authentication
IA-1: Identification and Authentication Policy and Procedures
IA-2: Identification and Authentication (Organizational Users)
IA-3: Device Identification and Authentication
IA-4: Identifier Management
IA-5: Authenticator Management
IA-6: Authenticator Feedback
IA-7: Cryptographic Module Authentication
IA-8: Identification and Authentication (Non-Organizational Users)

Our review of sampled systems indicated that these controls had been implemented for most systems. For those systems that these controls were not fully implemented, there were plans in place to bring both the documentation and the controls into compliance.

Description of the reasons for not using logical access controls and multi-factor authentication

For covered systems that do not have multi-factor authentication due to technological limitations of the software or hardware, either plans are in place to upgrade such systems or the risk has been accepted in cases where the technology cannot be upgraded.

Description of the following information security management practices used regarding covered systems

i. **Policies and procedures followed to conduct inventories of software licensing present on the on covered systems and associated licenses:**

Treasury provides general high-level policy in TD P 85-01 for bureaus to follow based on NIST and OMB standards and guidelines. Bureaus are responsible for creating and maintaining their software licensing and inventory. Each bureau uses their own sets of policies and procedures based on Treasury, NIST, and OMB guidance, and have a central unit responsible for maintaining and tracking software inventory and licenses.

ii. **Capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including data loss prevention (DLP) capabilities, forensics and visibility capabilities, and digital rights management (DRM) capabilities:**

Treasury currently leverages DLP inspection modules in the enterprise Trusted Internet Connection (TIC) mail relays to examine outbound mail. In addition, Treasury is planning a deployment of a DLP tool that would examine other protocols. Treasury maintains layered defensive technologies

used to detect activity, including: intrusion detection systems, EINSTEIN 1 and 2, extensive logging, big data analytics looking for suspicious patterns, and threat-intelligence informed blocking technologies. Furthermore, the TICs retain full packet capture to aid in investigations. In addition, the Treasury Government Security Operations Center (GSOC) maintains a capability to perform network and ad-hoc host-based forensics to support investigations. Treasury currently does not have an enterprise capability to monitor digital rights management.

iii. A description of how the covered agency is using the capabilities described in clause (ii):

This description is provided above in clause (ii).

iv. If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities:

Treasury is not aware of any Federal-wide policy or statute that requires the use of DLP, DRM, or forensic investigation technologies. As such, these technologies generally are not called out in the agency-wide policy. However, Treasury has planned enterprise license solutions with DRM capabilities in the future.

Description of applicable policies and procedures related to ensuring entities, including contractors that provide services to covered systems, implement the practices described above (i – iv)

Treasury requires bureaus to implement tools as needed to achieve desired security outcomes as set forth in TD P 85-01. DLP and DRM are two examples of technological solutions that bureaus may choose to employ to achieve the security objective required in policy. Similarly, Treasury-wide policy does not require the use of forensic tools, but instead requires that bureaus capture and retain system event and incident records at a level sufficient to permit the investigation and cause analysis of security events and incidents. Forensic analysis is one example of a tool that may be employed in such investigation.

Treasury uses standards promulgated by NIST and policies and guidance issued by OMB to establish in TD P 85-01 policies for ensuring that third-party IT service providers handling federal SBU information implement information security management practices equivalent to those required of federal agencies.

We plan to continue work in evaluating Treasury's security over its covered systems specific to adherence to access controls and the multi-factor authentication policies and procedures. We will issue a separate report to Treasury at the end of our review.

This letter is also being provided to the Chairmen and Ranking Members of the House Financial Services Committee and the House Oversight and Government Reform Committee. If you wish to discuss further, please contact me at 202-622-1090, or your staff can contact my Counsel, Rich Delmar, at 202-927-3973 or delmarr@oig.treas.gov.

Sincerely,

Eric M. Thorson
Inspector General

Enclosure

cc: Acting General Counsel
Deputy Under Secretary for Legislative Affairs
Deputy Secretary of the Treasury
Acting Assistant Secretary for Management
Deputy Assistant Secretary for Information Systems and Chief Information Officer

Response to Section 406 of the Cybersecurity Act of 2015

Treasury Directive Publication (TD P) 85-01 is the Department of the Treasury's (Treasury) Department-wide Information Technology (IT) security policy. Procedures for information security management practices are left to, and are maintained at, the bureau or system level. Detailed descriptions of the Office of the Chief Information Officer's (OCIO) Department-wide policies, and bureaus' and offices' policies and procedures for the sampled systems are below:

Description of the logical access policies and procedures to access a covered system

Office of the Chief Information Officer
For non-National Security Systems (NSS), Treasury uses standards promulgated by the National Institute for Standards and Technology (NIST) and policies and guidance issued by the Office of Management and Budget (OMB) to establish policies for logical access. Applicable standards and federal-wide guidance include Homeland Security Presidential Directive 12; Federal Information Processing Standard 201-2; and NIST Special Publications (SP) 800-25, 800-32, 800-53, 800-73-4, 800-76-2, 800-78-4, 800-79-2, 800-87, 800-96, 800-120, 800-156, and 800-157. Overarching agency policies are expressed in Treasury Directives (TD) 71-12 and 85-01 and their associated publications, TD P 71-12 and TD P 85-01.

For collateral NSS, Treasury uses standards promulgated by NIST and the policies and guidance issued by the Committee on NSS (CNSS) to establish policies for logical access in TD P 85-01. Applicable standards and federal-wide guidance include CNSS Directive (CNSSD) No. 504, No. 506, and No. 507; CNSS Instruction (CNSSI) No. 1253 and No. 1300; CNSS Policy (CNSSP) No. 3 and No. 25; National Telecommunications and Information Systems Security Policy No. 200; and NIST SP 800-53. Additional standards and guidance promulgated by the intelligence community apply to intelligence systems, however overarching agency policies are expressed in TD 85-01 and 15-03 and their associated publications, TD P 85-01 and TD P 15-03.

As NSS have additional criteria to consider for logical access, the Office of Intelligence and Analysis (OIA) established additional policy and procedures for logical access.

Office of Intelligence and Analysis:
All personnel requiring access must have a valid clearance, a need-to-know, and sign a nondisclosure statement. The request for access is approved by the Director of the OIA, Special Security Office. The justification must be initiated by the head of the office that made the access request, and sent to the

Information System Security Manager for processing. Request for access is based on Executive Order 12968, *Access to Classified information.* Further, Intelligence Community Policy Guidance Number 704.2 is used to determining eligibility for access.

Bureaus and Offices:
Bureaus' and offices' policies and procedures derive from the Department-level policies, with modifications to suit business needs. Overall, bureaus and offices Information Technology security policies reference TD P 85-01 and NIST SP 800-53. While some bureaus' policies and procedures had not been updated to adhere to NIST SP 800-53 Rev. 4, plans were in place to bring the documentation into compliance.

We determined that Treasury's policies and procedures follow appropriate federal policies and standards. However, we are still reviewing sampled systems to determine if they adhere to Treasury's access controls and multi-factor authentication policies and procedures.

Description and list of the logical access controls and multi-factor authentication used to access a covered system by privileged users

For non-NSS, Treasury-wide policy in TD P 85-01 incorporates the Access Control (AC), Identity and Access Management (IA), and Configuration Management (CM) control families from NIST SP 800-53. TD P 85-01 Volume I, Appendix A, defines parameters for many of these controls and introduces additional, agency-specific controls to further ensure that logical access permissions are appropriately and securely managed.

For collateral NSS, Treasury-wide policy in TD P 85-01 incorporates the AC, CM, and IA control families from CNSSI No. 1253. TD P 85-01 Volume II Appendix A provides an initial set of security controls for NSS and defines parameters for many of these controls. TD P 85-01 Volume II Appendix A also introduces additional, agency-specific controls to further ensure that logical access permissions are appropriately and securely managed.

For Intelligence systems, TD P 15-03 provides high-level requirements for logical access and authentication. Specific controls for privileged users are documented and maintained at the system level.

Please refer to Table 1 at the end of this enclosure for a detailed list of relevant IA and AC logical access controls. As noted above, some parameters and procedures for implementing access controls are maintained at the bureau or system level.

Bureaus and Offices
Bureaus' and offices' policy and procedures are derived from the Department-level policies, with modifications to suit business needs. Overall, Treasury offices and bureaus' Information Technology security policies refer to TD P 85-01 and NIST SP 800-53. While some documentation had not been updated to adhere to NIST SP 800-53 Rev. 4, plans were in place to bring the documentation into compliance.

Description of the reasons for not using logical access controls and multi-factor authentication

Office of the Chief Information Officer
All covered systems are protected by some form of logical access control. In many cases, users seeking to access a covered system must first authenticate to a Treasury network. As of March 15, 2016, multi-factor authentication (i.e. a PIV card) was required for non-remote access to 100 percent of privileged user accounts and 93 percent of general "unprivileged" user accounts.

Once a user has authenticated to the network, some covered systems require additional system-level authentication to enforce logical access control. This authentication may be single-factor for reasons that will vary from system to system. In some cases, the system may rely on legacy technology that is not capable of supporting multi-factor authentication. For these systems, a modernization and technology refresh will be required to enable more robust logical access protections. Other systems may be required to permit access via non-government furnished or mobile equipment because PIV card readers have not been widely adopted outside of the Federal government and apart from traditional servers and desktop/laptop workstations. It is anticipated that the introduction of PIV-derived credentials will permit gradual adoption of multi-factor authentication for these use cases.

Bureaus and Offices
While each bureau and office had policies and procedures in place with respect to multi-factor authentication (derived from TD P 85-01 and NIST 800-53), multi-factor authentication could not be implemented in all cases. Some bureaus reported that some hardware and software was incapable of handling multi-factor authentication. Plans were in place to update the affected hardware or software, or an acceptance of the risk for components that were not feasible to update.

Description of the following information security management practices used regarding covered systems

i. **Policies and procedures followed to conduct inventories of software licensing present on the on covered systems and associated licenses:**

Office of the Chief Information Officer
For non-NSS, Treasury uses standards promulgated by NIST and policies and guidance issued by OMB and the Department of Homeland Security (DHS) to establish policies for software inventory management in TD P 85-01. Applicable standards and federal-wide guidance include NIST SP 800-53 and 800-167. Treasury-wide policy incorporates the CM and SA (System and Services Acquisition) control families from NIST SP 800-53.TD P 85-01 Volume I Appendix A defines parameters for many of these controls and introduces additional agency-specific controls to further ensure that software asset inventories are appropriately and securely managed.

For collateral NSS, Treasury uses standards promulgated by NIST and policies and guidance issued by CNSS to establish policies for software inventory management in TD P 85-01. Applicable standards and federal-wide guidance include CNSSD No. 504, CNSSI No. 1253, and NIST SP 800-53. Additional standards and guidance promulgated by the intelligence community apply to intelligence systems are not included here. Treasury-wide policy incorporates the CM and SA control families from CNSSI No. 1253. TD P 85-01 Volume II Appendix A provides an initial set of security controls for NSS, defines parameters for many of these controls, and introduces additional agency-specific controls to further ensure that software asset inventories are appropriately and securely managed.

Procedures are managed and maintained at the bureau enterprise or system level. Treasury does not have a centralized collection of procedures used to manage software inventories for each covered system, although the Treasury CIO does consolidate some bureau reports of software inventories tied to capital investments for reporting to OMB.

Bureaus and Offices

Bureau of the Fiscal Service (Fiscal Service)
Fiscal Service provided its *Approved IT Products Standard and Automated Mainframe Inventory Process,* which stated that an automated mechanism is used to detect the addition of unauthorized components on bureau desktop IT equipment. End User Support Branch (EUSB) is also the maintainer of IT property inventory, including software licenses.

Office of the Comptroller of the Currency (OCC)
In accordance with OCC's policy, Policies and Procedures Manual (PPM) 4000-3, OCC monitors and tracks the installation or use of non-standard, unapproved hardware and software, including harmful software or malware, and pursues personnel or criminal and civil penalties as established by OCC policy or law. Only appropriately licensed software installed by authorized personnel may operate on OCC-issued electronic equipment used to display, modify, transmit or store OCC information. Information Technology Services maintains and regularly updates its list of standard hardware and software.

Per PPM 4000-3, the OCC CIO is responsible for managing licenses for, maintaining, and disposing of hardware and software, as well as providing sufficient quantities of standard licensed software and hardware. The Director of IT Operations Strategy and Controls establishes and maintains an OCC hardware and software management program. IT Acquisitions (IT ACQS) keeps track of software licenses. When a new software request ticket is assigned, license availability is verified. If a license is available, the request is approved. If the maximum amount has already been reached, the ticket is put on hold and reviewed for a possible new software/license purchase to accommodate the user request. New purchases are reflected in the license counts tracking log. IT ACQS runs System Center Configuration Manager (SCCM) reports quarterly for software that is installed in the OCC environment. The information is saved in spreadsheets and reconciled with the license counts tracking log, and is updated to account for licenses no longer needed by users who have left OCC.

Financial Crimes Enforcement Network (FinCEN)
FinCEN's Information Systems Security Policy (ISSP)-020 refers to TD P 85-01. Specifically, bureaus shall periodically scan their networks to detect and remove any unauthorized software or unlicensed software. FinCEN's ISSP-031 for Acceptable Use, Attachment B – FinCEN Approved Software List, contains the approved software for FinCEN.

Additionally, FinCEN's policies, ISSP 015 Access Control, ISSP 022 Perimeter Security, ISSP 020 Network Security, ISSP 031 Acceptable Use, ISSP 013 Mobile Computing, ISSP 030 Internet Security and ISSP 012 Encryption, established policies for inventories of software and licenses. Normal users do not have rights to install their own software on desktops per USGCB (United States Government Common Baseline). Requests to add software are approved by the supervisor and then routed to the service desk via a Fin029 form. The approved software list is under change control.

FinCEN removes unauthorized software via System Center Configuration Manager (SCCM), and removals are conducted daily.

United States Mint (Mint)
Mint-wide policy memorandums IT-02, *United States Mint Computer Software Policy*, and IT-13, *United States Mint Information Technology Standards Management Policy*, described how inventory will be used to track and account for all IT resources. These memoranda described software licensing and noted unauthorized copies of software will be licensed or destroyed. Furthermore, Mint also has Enterprise Software Distribution Standard Operating Procedures (ESD SOP) that adhere to Treasury policy and standards as specified in TD P 85-01. The ESD SOP provides instructional procedures, guidance, and standardization in the distribution of software entitlements owned and purchased by Mint. The ESD SOP also describes how to disseminate software and licenses for the Mint's OCIO.

Departmental Offices (DO)
DO referred to TD P 85-01 and DO-910 as the applicable policies regarding software inventory and licensing. Software lists are maintained on a per-system basis.

Below are the methods used for the following sampled systems to maintain information on software licensing:

- Enterprise Content Management
  Enterprise Content Management system's components are tracked and inventoried on an internal website. The inventory is reviewed and updated at least monthly or when there is a major change in the system.
- DO LAN
  Inventory of software is an automated process. The tracking of licenses associated with the software is a manual process and is performed as part of the software request process.
- Treasury Government Security Operations Center (GSOC)
  Software is Open Source and does not have standard licenses. Commercial off the shelf software with specific license requirements are tracked specific to the piece of software.

Alcohol Tax and Trade Bureau (TTB)
TTB's policy is established in *Automated Information Systems Security Program Policy,* and related procedures. In addition, system owners provide TTB's OCIO with copies of all software licenses, which are stored in a software library. TTB's OCIO maintains an inventory of software licenses to facilitate compliance with licensing agreements. If a system owner no longer

needs a license due to a change in system status, they notify the TTB OCIO. In addition, a system administrator must have a work order or approval to install approved software.

Bureau of Engraving and Printing (BEP)
BEP utilizes System Center Configuration Manger (SCCM), Tenable Security Center, and manually input licensing information into a secured Excel Spreadsheet. BEP is in the process of revising the BEP Security Policy Manual 10.08-35, and until the Manual is updated, Treasury TD P 85-01 is the authoritative policy for system inventory and licensing requirements.

ii. Capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including data loss prevention (DLP) capabilities, forensics and visibility capabilities, and digital rights management (DRM) capabilities, and a description of how the covered agency is using the capabilities:

Office of the Chief Information Officer
The Department of the Treasury protects sensitive data and has implemented layers of defense to protect against and monitor for data loss. Treasury is not aware of any Federal-wide policy or statute that requires the use of DLP, DRM, or forensic investigation technologies. As such, these technologies generally are not called out in the agency-wide policy. However, Treasury has planned enterprise license solutions DRM capabilities in the future. The Department currently has DLP capabilities to detect the inclusion of sensitive information in all outbound email as well as in outbound web traffic originating from the IRS. In addition, Treasury is actively planning a deployment of a DLP tool (vendor to be determined) for the enterprise TIC(Trusted Internet Connection) that would examine other protocols. In FY 2017, Treasury plans for an upgrade of DLP technology at the Bureau of the Fiscal Service TIC to a more robust solution. The Treasury enterprise wide area network provides encryption to all data in transit across the Treasury network. Through the GSOC, Treasury leverages real-time monitoring capabilities focused on detecting malicious activity. This approach has exposed tactics used by external threat actors, to include common techniques for exfiltration of data.

At the enterprise TIC, Treasury has deployed several capabilities designed to detect and investigate potential threats, including exfiltration. The agency maintains layered defensive technologies used to detect activity to include: intrusion detection systems (IDS), EINSTEIN 1 and 2, extensive logging, big data analytics looking for suspicious patterns, and threat-intelligence informed blocking technologies. Furthermore, the TICs retain 30 days of full packet capture (well above the TIC 2.0 standard of seven days) to aid in investigations. In addition, GSOC maintains a capability to perform network

and ad-hoc host-based forensics to support investigations.

Treasury currently does not have an enterprise capability to monitor DRM. Treasury also does not have a central inventory of DRM tools or capabilities at the bureaus.

Bureaus and Offices

Bureau of the Fiscal Service
A few Fiscal Service systems utilize Web Application Firewalls that only help with injection attacks and not DLP. None of the systems have deployed logging for all actions against the data. However, Fiscal Service is exploring the use of DLP capabilities. Additionally, Fiscal Service is using data loss prevention technologies for email in a passive mode. Emails containing social security numbers, credit card numbers, and user ids and passwords sent to external email domains are logged. Reports are sent to the CSIRC (Computer Security Incident Response Center) where they are reviewed for additional follow-up.

Office of the Comptroller of the Currency
OCC is currently monitoring all outbound HTTP and SMTP unencrypted traffic for target data types. OCC is currently testing DLP capabilities, and piloting the capability to monitor endpoints (laptops/desktops) for the presence of unauthorized sensitive data. OCC is also piloting the capability to specifically monitor and block emails containing sensitive data from leaving the OCC network, including via encrypted email traffic. OCC has the capability to scan server contents for the presence of personally identifiable information (PII) but is still developing the pilot program/process to implement this capability. The *OCC Computer Security Incident Response Center (CIRC) Program and Operations Guide* contains an overview of operational support provided by CIRC, including review process for monitoring/detection of incidents, signs of breach, analysis/investigation phase in regards to information loss, forensics capability, loss/stolen incidents. This guide also contains details regarding CIRC procedures for monitoring activity, including outbound activity, on the IPS, Proxy, and Firewall. The *CIRC Data Breach Action Plan* contains detailed information regarding investigation/forensics review process in event of data breach/data exfiltration.

Currently the OCC does not have an enterprise solution in place to manage digital rights.

Financial Crimes Enforcement Network
For DLP, FinCEN employs a Blue Coat Proxy with SSL (Secure Sockets Layer) intercept and a Cisco-based network IDS system along with host based IDS on desktops. A ForeScout CounterACT appliance is deployed centrally at FinCEN which has visibility into the core network traffic, active directory, and System Center Configuration Manager (SCCM) to ensure only authorized hosts and managed hosts are on the network. All network IDS logs integrate with the FinCEN SIEM (Security Information and Event Management). As a pre-cautionary measure, FinCEN is currently conducting a compromise assessment on all windows platforms to search for advanced persistent threats. This is both agent-based and network-based. Normal users do not have rights to install their own software on desktops per USGCB. FinCEN does not have forensic capabilities, as they rely on Treasury GSOC for assistance when required. FinCEN does not have DRM capabilities.

United States Mint (Mint)
The Mint is using Symantec DLP as a compensating control in support of the Payment Card Industry Data Security Standard (PCI-DSS) requirements. This goal is accomplished through using the Endpoint Discover and Endpoint Prevent offered by Symantec DLP to perform deep content inspection of data at rest or in motion to aid in PCI compliance requirements. This product is also used by the Mint to discover other PCI or PII that may be found on Mint IT systems via ad-hoc scanning throughout the organization. The Mint uses Encase enterprise for forensic and visibility capabilities. The Mint does not have DRM capabilities.

Departmental Offices
The GSOC works with the Fiscal Service TIC to monitor the DLP scanning performed by the TIC for the Bureaus that transit the TIC infrastructure. The GSOC has a significant set of tools in place to monitor the Treasury environment for threats and perform forensics on identified threats. The scope of these capabilities is quite significant and includes, among other things, IDS, Email Scanning, Packet Capture and Analysis, and Splunk analysis of data using current Threat Indicators. Additionally, the DO LAN has implemented EnCase to assist with forensic activity. DO does not have any digital rights management capabilities.

Alcohol Tax and Trade Bureau
TTB utilizes Zix to prevent data loss, the SIEM detects data exfiltration, also GSOC monitors through the TIC and reports on DLP alerts on a daily basis. TTB utilizes FireEye EX, NX and FX to provide visibility into email, web/network and files. Gigamon TAP is utilized to aggregate network traffic and feed into the IBM QRadar SIEM as well as other security tools (enCase) for forensic analysis. Only TTB system administrators shall have software

installation privileges. In addition, the system administrator must have a work order or approval to install approved software.

Bureau of Engraving and Printing
DLP is managed and monitored by the GSOC. Forensics and Visibility capabilities are managed internally by Information Technology Security Division (ITSD). According to BEP, digital rights management is not applicable to BEP.

iii. A description of how the covered agency is using the capabilities described in clause (ii):

This description is provided above in clause (ii).

iv. If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities:

Office of the Chief Information Officer
Treasury's approach to detecting exfiltration and other threats leverages multiple layered technologies aimed at detecting and/or blocking malicious activity at every step of the intrusion lifecycle, or kill chain. Treasury blocks known bad infrastructure, analyzes traffic for known bad and suspicious signatures, and performs anomaly detection to identify unknown threats. Treasury's DLP implementation is initially focused on detecting potential loss of personally identifiable information using signatures to detect any PII leaving the network. The GSOC's big data analytics platform leverages log data mining in order to find unusual traffic patterns common to exfiltration, including spikes in outbound traffic, among other things. These protection mechanisms are routinely updated and tuned leveraging both commercial feeds as well as internally driven analytics informed by all-source threat intelligence.

The primary barrier to deploying additional capabilities is the need for additional resources – both to pay tool licensing costs and to fund additional staff needed to operate, maintain, and utilize the tools.

Newer technologies like digital rights management DRM are critical for securing Treasury's enterprise data. Shared data that is DRM-encrypted can be used by authorized recipients and within an authorized environment, even if downloaded on a device that is not controlled by the enterprise. When available, the Department will evaluate leveraging a DRM shared service capability, as suggested in OMB Memorandum M-16-04, or a DRM tool offering currently planned in the fourth phase of the DHS CDM initiative that could enable a systematic approach to data-level protection across the

Federal government. Treasury has planned enterprise license solutions for Microsoft and Adobe applications with options to include DRM capabilities in the future. Treasury's enterprise license for Adobe was established in June 2016. Treasury would require a DRM solution that includes role-based control at the document level and is planning for future budget funding requests to procure such a solution.

Bureaus and Offices

Bureau of the Fiscal Service
Fiscal Service currently does not have the internal resources to use forensic capabilities. The NIRT (National Incident Response Team) and Treasury GSOC provide forensics capabilities for Fiscal Service.

The Fiscal Service Baseline Security Requirements (BLSR) provides policy regarding incident response. Specifically, IR-7_N_00 INCIDENT RESPONSE ASSISTANCE: The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents. Supplemental Guidance - Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required.

Fiscal Service is not using digital rights management technologies. Fiscal Service has developed categories of information to ensure appropriate safeguards are utilized in transit of that information; however, the bureau has not yet put technical controls in place to enforce digital rights management.

Office of the Comptroller of the Currency
OCC did not provide a reason for not having DRM capability.

Financial Crimes Enforcement Network
FinCEN did not provide a reason for not having forensic and DRM capabilities. FinCEN relies on Treasury GSOC for assistance when required.

United States Mint
Mint did not provide a reason for not having DRM capability.

Departmental Offices
DO relied on Treasury for DLP, forensics, and DRM capabilities.

Alcohol Tax and Trade Bureau

TTB is not utilizing DRM and did not provide a reason.

Description of applicable policies and procedures related to ensuring entities, including contractors that provide services to covered systems, implement the practices described above (i – iv)

Office of the Chief Information Officer
For non-NSS, Treasury uses standards promulgated by NIST and policies and guidance issued by OMB to establish in TD P 85-01 policies for ensuring that third-party IT service providers handling federal Sensitive But Unclassified (SBU) information implement information security management practices equivalent to those required of federal agencies. Applicable standards and federal-wide guidance include the Federal Acquisition Regulation (FAR) and NIST SP 800-53. Treasury-wide policy applies to contractor systems and incorporates the SA control family from NIST SP 800-53. TD P 85-01 Volume I Appendix A defines parameters for many of these controls and introduces additional, agency-specific controls further requiring the application of Treasury cybersecurity controls to service providers.

For collateral NSS, Treasury uses standards promulgated by NIST and policies and guidance issued by CNSS to establish in TD P 85-01 policies for ensuring that third-party IT service providers handling federal national security information implement information security management practices equivalent to those required of federal agencies. Applicable standards and federal-wide guidance include CNSSD No. 504, CNSSI No. 1253, and NIST SP 800-53. Additional standards and guidance promulgated by the intelligence community apply to intelligence systems are not included here. Treasury-wide policy applies to contractor systems and incorporates the SA control family from CNSSI No. 1253. TD P 85-01 Volume II Appendix A provides an initial set of security controls for NSS, defines parameters for many of these controls, and introduces additional, agency-specific controls further requiring the application of Treasury cybersecurity controls to service providers.

Procedures are managed and maintained at the bureau enterprise or system level. Treasury does not have a centralized collection of bureau procedures used to ensure that third-party IT service providers handling federal information implement appropriate information security management practices equivalent to those required of federal agencies.

Bureaus and Offices

Bureau of the Fiscal Service
Fiscal Service's security policies apply to all systems and services processing Fiscal Service information. Fiscal Service includes these security requirements in contracts that process sensitive information. Its agent relationships, Fiscal and Financial, contain similar provisions. In general, Fiscal Service policies and SOPs apply to contractors and third party operated systems unless otherwise noted. Fiscal Service BLSRs established security policies that require approval prior to removal of SBU information. Removal of SBU information from Fiscal Service, by any means, such as but not limited to, emailing to a non-Fiscal Service address, mailing digital or non-digital media, or physical transport outside Fiscal Service facilities, shall be documented and approved on a Form 7005 that has been signed by the CPO (Chief Privacy Officer) or CISO (Chief Information Security Officer). Digital information (excluding SBU or PII) stored on encrypted GFE (Government Furnished Equipment) may be transported outside controlled facilities without a Form 7005. This control excludes interconnections that fall within the boundary of a FISMA (Federal Information Security Modernization Act) system.

Fiscal Service does not have policies in place that address digital rights management.

Fiscal Service's security policies apply to all systems and services processing Fiscal Service information. Fiscal Service includes security requirements in contracts that process sensitive information. Its agent relationships, Fiscal and Financial, also contain similar provisions in their respective agreements. In general, Fiscal Service policies and SOPs (Standard Operating Procedures) apply to contractors and third party operated systems unless otherwise noted in the policy and/or SOP. The scope of the requirement's applicability is documented within the policy or SOP.

Office of the Comptroller of the Currency
OCC complies with policy set in TD P 85-01 in requiring that its vendors that operate information systems on its behalf meet FedRAMP or NIST 800-53 moderate baseline requirements commensurate with the risk and magnitude of harm that could result from the loss or misuse of, or unauthorized access to these resources, including software management. OCC also requires vendors operating systems on its behalf to implement NIST 800-53 moderate baseline and/or FedRAMP incident response controls to address cybersecurity threats.

United States Mint
Mint's Memorandum IT-13 requires that all IT investments, programs, projects, and task orders must comply with IT standards and that all requests for the acquisition, maintenance, and/or enhancement of IT assets must be compliant with IT standards
.

Departmental Offices
DO requires external entities who provide dedicated resources to DO systems, to implement security controls that comply with applicable federal laws, directives, policies, regulations, standards, guidance, and established service-level agreements. Agreements between the offices and the external entities shall be documented in interconnection service agreements (ISAs) and/or MOU/MOAs. External entities shall undergo a cloud/FedRAMP determination process, where applicable.

Alcohol Tax and Trade Bureau
TTB does not have individual policies governing IT resource use/security for external entities. All TTB contractors use TTB provided hardware and software, which are maintained by TTB OCIO. TTB follows NIST SP 800-53 Rev. 4 guidance, TD P 85-01, and TTB *Automated Information Systems Security Program Policy.*

Bureau of Engraving and Printing
BEP has two external entities that provide services to BEP. Both of these entities are FedRAMP certified as required by TD P 85-01.

Financial Crimes Enforcement Network
FinCEN does not have policies and procedures or capabilities specifically addressing forensic and DRM. DLP is covered in FinCEN's Information Systems Security Policy (ISSP)-022, which references TD P 85-01.

Table 1

TD P 85-01 Appendix A established policies for access control, identity and access management, and configuration management security controls for unclassified systems as below. Treasury's policies for collateral and intelligence NSS are similar but contain additional requirements.

NIST CONTROL#	TD P 85-01 REFERENCE #	REQUIREMENT:	Baseline		
			L	M	H
AC-1	AC-1_N.00	ACCESS CONTROL POLICY AND PROCEDURES The organization: a. Develops, documents, and disseminates to [Bureau-defined personnel or roles]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	X	X	X
	AC-1_N.01	2. Procedures to facilitate the implementation of the access control policy and associated access controls; and	X	X	X
	AC-1_N.02	b. Reviews and updates the current: 1. Access control policy [at least every three years or if there is a significant change]; and	X	X	X
	AC-1_N.03	2. Access control procedures [at least every three years or if there is a significant change].	X	X	X
AC-2	AC-2_N.00	ACCOUNT MANAGEMENT Control: The organization: a. Identifies and selects the following types of information system accounts to support organizational	X	X	X

		missions/business functions: [Bureau-defined information system account types]; (see b-e in 800-53 rev 4)			
	AC-2_N.01	b. Assigns account managers for information system accounts;	X	X	X
	AC-2_N.02	c. Establishes conditions for group and role membership;	X	X	X
	AC-2_N.03	d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;	X	X	X
	AC-2_N.04	e. Requires approvals by [Bureau-defined personnel or roles] for requests to create information system accounts;	X	X	X
	AC-2_N.05	f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Bureau-defined procedures or conditions]; (see g, h, I in 800-53 rev 4)	X	X	X
	AC-2_N.06	g. Monitors the use of information system accounts;	X	X	X
	AC-2_N.07	h. Notifies account managers: 1. When accounts are no longer required;	X	X	X
	AC-2_N.08	2. When users are terminated or transferred; and	X	X	X
	AC-2_N.09	3. When individual information system usage or need-to-know changes;	X	X	X

	AC-2_N.10	i. Authorizes access to the information system based on: 1. A valid access authorization;	X	X	X
	AC-2_N.11	2. Intended system usage; and	X	X	X
	AC-2_N.12	3. Other attributes as required by the organization or associated missions/business functions;	X	X	X
	AC-2_N.13	j. Reviews accounts for compliance with account management requirements [of users annually; privileged users semi-annually]; and	X	X	X
	AC-2_N.14	k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	X	X	X
AC-2(2)	AC-2(2)_N.00	ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS The information system automatically [Selection: removes; disables] temporary and emergency accounts after [no longer than two business days].		X	X
AC-2(3)	AC-2(3)_N.00	ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS The information system automatically disables inactive accounts after [120 days (Public users can be determined by the Bureau)].		X	X
AC-2(4)	AC-2(4)_N.00	ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Bureau-defined personnel or roles].		X	X

AC-2(5)	AC-2(5)_N.00	ACCOUNT MANAGEMENT | INACTIVITY LOGOUT The organization requires that users log out when [Bureau-defined time period of expected inactivity or description of when to log out]			X
AC-2(11)	AC-2(11)_N.00	ACCOUNT MANAGEMENT | USAGE CONDITIONS The information system enforces [Bureau-defined circumstances and/or usage conditions] for [Bureau-defined information system accounts].			X
AC-2(12)	AC-2(12)_N.00	ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE The organization: (a) Monitors information system accounts for [Bureau-defined atypical use]; and			X
	AC-2(12)_N.01	(b) Reports atypical usage of information system accounts to [Bureau-defined personnel or roles].			X
AC-2(13)	AC-2(13)_N.00	ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS The organization disables accounts of users posing a significant risk within [Bureau-defined, but not greater than one business day time period] of discovery of the risk.			X
AC-3	AC-3_N.00	ACCESS ENFORCEMENT Control: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	X	X	X

	AC-3_T.002	Users having accounts with administrator access privileges on Treasury systems may access those accounts only from Treasury government or authorized government contractor systems. *INFORMATIVE: In other words, a key intent is to prohibit personally-owned or public kiosk (e.g., library) systems from being used for remote Administrator access.* *INFORMATIVE: If individuals with administrator rights require e-mail or Internet access beyond local boundaries, one alternative would be to issue separate, non-privileged accounts (one per affected individual) for that purpose. For the considerations of this section, administrator accounts/rights are those that allow for the installation or configuration of software on any Treasury asset.*	X	X	X
AC-4	AC-4_N.00	INFORMATION FLOW ENFORCEMENT Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [applicable policies, agreements, contracts and/or procedures].		X	X
AC-5	AC-5_N.00	SEPARATION OF DUTIES Control: The organization: a. Separates [Bureau-defined duties of individuals];		X	X

AC-6	AC-6_N.00	LEAST PRIVILEGE Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.		X	X
	AC-6_T.003	Accounts with administrative privileges (including local administrator rights) shall be prohibited from web browsing and other Internet connections outside of the local protected boundary (usually Treasury) unless such risk is accepted in writing by the Bureau CIO. *INFORMATIVE: If individuals with administrator rights require e-mail or Internet access beyond local boundaries, one alternative would be to issue separate, non-privileged accounts (one per affected individual) for that purpose. For the considerations of this section, administrator accounts/rights are those that allow for the installation or configuration of software on any Treasury asset.*		X	X
	AC-6_T.004	Accounts with administrative privileges (including local administrator rights) shall be blocked from access to e-mail unless such risk is accepted in writing by the Bureau CIO. *INFORMATIVE: If individuals with*		X	X

		administrator rights require e-mail or Internet access beyond local boundaries, one alternative would be to issue separate, non-privileged accounts (one per affected individual) for that purpose. For the considerations of this section, administrator accounts/rights are those that allow for the installation or configuration of software on any Treasury asset.			
AC-6(1)	AC-6(1)_N.00	LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS The organization explicitly authorizes access to [Bureau-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].		X	X
AC-6(2)	AC-6(2)_N.00	LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS The organization requires that users of information system accounts, or roles, with access to [security functions including but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters], use non-privileged accounts or roles, when accessing non-security functions.		X	X
AC-6(3)	AC-6(3)_N.00	LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS The organization authorizes network access to [Bureau-defined privileged commands] only for [Bureau-defined			X

		compelling operational needs] and documents the rationale for such access in the security plan for the information system.			
AC-6(5)	AC-6(5)_N.00	LEAST PRIVILEGE | PRIVILEGED ACCOUNTS The organization restricts privileged accounts on the information system to [Bureau-defined personnel or roles].		X	X
AC-7	AC-7_N.00	UNSUCCESSFUL LOGON ATTEMPTS Control: The information system: a. Enforces a limit of [three] consecutive invalid logon attempts by a user during a [120 minute period; and	X	X	X
	AC-7_N.01	b. (LOW, MODERATE) Automatically [locks the account/node for 15 minutes or until released by an administrator] when the maximum number of unsuccessful attempts is exceeded.	X	X	
	AC-7_N.01	b. (HIGH) Automatically [locks the account/node until released by an administrator] when the maximum number of unsuccessful attempts is exceeded.			X
AC-10	AC-10_N.00	CONCURRENT SESSION CONTROL Control: The information system limits the number of concurrent sessions for each [Bureau-defined account and/or account type] to [one for non-privileged users and three for privileged users].			X
AC-11	AC-11_N.00	SESSION LOCK Control: The information system: a. Prevents further access to the		X	X

		system by initiating a session lock after [30 minutes or less] of inactivity or upon receiving a request from a user; and			
AC-12	AC-12_N.00	SESSION TERMINATION Control: The information system automatically terminates a user session after [Bureau-defined conditions or trigger events requiring session disconnect].		X	X
AC-14	AC-14_N.00	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION Control: The organization: a. Identifies [Bureau-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and	X	X	X
AC-17	AC-17_N.00	REMOTE ACCESS Control: The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and	X	X	X
	AC-17_N.01	b. Authorizes remote access to the information system prior to allowing such connections.	X	X	X
	AC-17_T.006	Two-factor authentication shall be implemented for all remote access back to a Departmental system. *INFORMATIVE: "Remote access" is defined as LAN-like access to a Treasury system from a location or facility not controlled by a Treasury*	X	X	X

		organization. Access to websites and other systems available to the public, as well as access to non-Treasury or publicly available information, is not considered "remote access." *Examples: If a Treasury employee works at home on a personally-owned computer using public or non-Treasury information, that would not entail "remote access." If a State of Rhode Island employee has been granted access to a Treasury system and that employee accesses the Treasury system from a State of Rhode Island facility, it would be considered "remote access." A Treasury employee using a Treasury laptop without connectivity back to a Treasury system for an audit at a firm in a commercial office building would not be considered "remote access."*			
AC-17(2)	AC-17(2)_N.00	REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.		X	X
	AC-17(2)_T.206	Remote Access Security. Remote access sessions to Treasury IT assets (e.g., networks, systems) shall only be provided through an encryption mechanism such as a virtual private network (VPN) connection that meets FIPS 140 validation requirements.	X	X	X

		INFORMATIVE: This control does not apply to sessions used for the dissemination of non-sensitive information to the public.			
AC-17(3)	AC-17(3)_N.00	REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS The information system routes all remote accesses through [Bureau-defined number] managed network access control points.		X	X
AC-17(4)	AC-17(4)_N.00	REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS The organization: (a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Bureau-defined needs]; and		X	X
AC-18	AC-18_N.00	WIRELESS ACCESS Control: The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and	X	X	X
	AC-18_N.01	b. Authorizes wireless access to the information system prior to allowing such connections.	X	X	X
	AC-18_T.246	Treasury bureaus shall coordinate with the Treasury Office of Intelligence and Analysis to establish a wireless program to protect National Security Systems (NSS) when unclassified wireless technologies are used to transmit, receive, process, or store unclassified data in the proximity of Treasury NSS or National Security Information (NSI).	X	X	X

		INFORMATIVE: This control also applies to any/all guest wireless networks.			
	AC-18_T.247	Guest wireless networks operated by or on behalf of Treasury in Treasury facilities shall be completely logically separate from all Treasury networks.	X	X	X
	AC-18_T.008	Bureaus shall ensure that unapproved wireless networking capabilities of desktops, laptops, printers, copiers, fax machines, SCADA systems, and other devices are disabled (through automated means, where technically possible) and monitored through automated means for unauthorized changes. *INFORMATIVE: One alternative yet acceptable approach to "monitoring through automated means" is regularly pushing out settings that restrict unapproved wireless connections.*	X	X	X
	AC-18_T.009	Bureaus shall monitor for unauthorized wireless access to the information system and enforce requirements for wireless connections to the information system.	X	X	X
	AC-18_T.010	Implementation and use of wireless networks must be approved by the Authorizing Official in accordance with organizational risk tolerance and commensurate with the security categorization of the data to be carries by the system, which may be	X	X	X

		no higher than the security categorization of the system			
	AC-18_T.011	Bureaus shall employ security mechanisms for wireless networks consistent with the sensitivity of the information to be transmitted. For transmissions of FIPS 199 MODERATE or HIGH confidentiality information, FIPS 140-2 validated encryption must be employed.		X	X
	AC-18_T.012	Bureaus shall scan for rogue wireless access points and other wireless activity that are not in compliance with Departmental policy.	X	X	X
AC-18(1)	AC-18(1)_N.00	WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.		X	X
AC-19	AC-19_N.00	ACCESS CONTROL FOR MOBILE DEVICES Control: The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and	X	X	X
	AC-19_N.01	b. Authorizes and monitors the connection of mobile devices to organizational information systems.	X	X	X
	AC-19_T.016	Bureaus shall ensure that all Treasury information on all mobile devices is encrypted using FIPS 140-2 (or	X	X	X

		succeeding guidance) validated encryption technology, except when no such encryption technology solutions are available to address a specific device.			
	AC-19_T.018	The bureau CISO or designee must give written approval before an individual within the office may take a government-owned laptop computer and/or other mobile devices overseas.	P	P	P
	AC-19_T.019	Bureau deployment of government-owned mobile devices to process, store, or transmit Treasury information must be approved by the Authorizing Official in accordance with organizational risk tolerance and commensurate with the security categorization of the data to be processed, stored, or transmitted, which may be no higher than the security categorization of the devices.	X	X	X
	AC-19_T.020	Mobile devices taken outside the U.S. (whether for official or personal travel) may not connect wirelessly to a Treasury system unless sanitized. *INFORMATIVE: Excluded is this situation of transiting another country provided the device remains under the immediate control of the user.* *INFORMATIVE: It is permissible simply to prohibit non-wireless mobile device connections entirely.*	X	X	X

	AC-19_T.021	This control addresses laptop computers that are temporarily taken overseas. All laptops temporarily taken overseas must be protected by: 1) full disk FIPS validated encryption; 2) disabling any wireless capability; and 3) either disabling all USB ports(s) or use of tamper-evident bags/seals/containers each time the laptop is left unattended (i.e., not under the direct and immediate control of a U.S. Government employee or authorized government contractor). If any laptop is not protected as described above, it may not be reconnected to a Treasury system or network until sanitized.	X	X	X
	AC-19_T.022	Laptops and other devices containing Treasury information categorized as High or Moderate (confidentiality) under FIPS 199 shall not be connected to networks while outside the U.S., unless employing a separate hard drive or a secure partition (physical or virtual) with a separate operating system instance that contains no High or Moderate Treasury information.		X	X
	AC-19_T.023	Hard drives or partitions that connect to networks while outside the U.S. shall not be connected to Treasury networks at any time.	X	X	X
	AC-19_T.024	During overseas travel, batteries shall be removed from battery-powered mobile devices and stored separate from the device when the device is left unattended. The battery also shall be removed if the device is within auditable range of sensitive	X	X	X

		conversations while overseas. *INFORMATIVE: This control applies to any mobile device where removable of the battery is possible*			
	AC-19_T.025	During overseas travel, SIM cards shall be removed and stored separate from devices that employ them when going through non-U.S. customs. *INFORMATIVE: This control applies to any mobile device where removal of the battery is possible*	X	X	X
	AC-19_T.026	Bureaus shall provide users with procedures to follow during foreign travel when a device is taken out of their possession and view for other than routine airport security scans.	p	p	p
AC-19(5)	AC-19(5)_N.00	ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Bureau-defined mobile devices].		X	X
AC-20(1)	AC-20(1)_N.00	USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: (a) Verifies the implementation of		X	X

		required security controls on the external system as specified in the organization's information security policy and security plan; or			
	AC-20(1)_N.01	(b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.		X	X
AC-20(2)	AC-20(2)_N.00	USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES The organization [Selection: restricts; prohibits] the use of organization-controlled portable storage devices by authorized individuals on external information systems.		X	X
AC-21	AC-21_N.00	INFORMATION SHARING Control: The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Bureau-defined information sharing circumstances where user discretion is required]; and		X	X
	AC-21_N.01	b. Employs [Bureau-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.		X	X
IA-1	IA-1_N.00	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and	X	X	X

		disseminates to [Bureau-defined personnel or roles]: 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and			
	IA-1_N.01	2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and	X	X	X
	IA-1_N.02	b. Reviews and updates the current: 1. Identification and authentication policy [every three years or if there is a significant change]; and	X	X	X
	IA-1_N.03	2. Identification and authentication procedures [every three years or if there is a significant change].	X	X	X
IA-2	IA-2_N.00	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	X	X	X
	IA-2_T.091	Bureaus shall require authentication with HSPD-12 credentials for access to all systems. In the event that an individual's HSPD-12 credential is rendered inoperable or otherwise temporarily unavailable, Bureaus may temporarily rely on other two-factor (or stronger) credentials for administrator (privileged) accounts	X	X	X

		and any of the approaches in NIST 800-63-1 for end users. Such reliance shall not exceed two weeks or the standard length of time to issue a new/replacement HSPD-12 credential, whichever is shorter. *INFORMATIVE: It is understood that this transition cannot begin until HSPD-12 credentials are deployed for logical access controls. However, in order to demonstrate the requirement for resource planning and lifecycle management purposes, the implementation date of was set for January 1, 2009 with the understanding and expectation that bureaus will meet the implementation date by establishment of a POA&M which includes bureau milestones for deployment and transition to use of HSPD-12 credentials for logical access controls.* *This control does not apply to Windows-based local administrator accounts.*			
	IA-2_T.093	Bureaus shall specifically require all contractors with recurring physical or logical access requirements to Treasury facilities or systems to be issued credentials that comply with HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors (See also FIPS Publication 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors).	X	X	X

IA-2(11)	IA-2(11)_N.00	IDENTIFICATION AND AUTHENTICATION | REMOTE ACCESS - SEPARATE DEVICE The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Bureau-defined strength of mechanism requirements].		X	X
IA-3	IA-3_N.00	DEVICE IDENTIFICATION AND AUTHENTICATION Control: The information system uniquely identifies and authenticates [Bureau-defined specific and/or types of devices] before establishing a [local; remote; network] connection.		X	X
IA-4	IA-4_N.00	IDENTIFIER MANAGEMENT Control: The organization manages information system identifiers by: a. Receiving authorization from [Bureau-defined personnel or roles] to assign an individual, group, role, or device identifier;	X	X	X
	IA-4_N.01	b. Selecting an identifier that identifies an individual, group, role, or device;	X	X	X
	IA-4_N.02	c. Assigning the identifier to the intended individual, group, role, or device;	X	X	X
	IA-4_N.03	d. Preventing reuse of identifiers for [Bureau-defined time period]; and	X	X	X
	IA-4_N.04	e. Disabling the identifier after [120 days].	X	X	X

	IA-4_T.057	Bureaus shall change all default vendor-set or factory-set administrator accounts and passwords prior to implementation (e.g., during installation or immediately after installation).	X	X	X
IA-5	IA-5_N.00	AUTHENTICATOR MANAGEMENT Control: The organization manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; *(see b-f and h-j in SP 800-53 rev 4)*	X	X	X
	IA-5_N.06	g. Changing/refreshing authenticators [Bureau-defined time period by authenticator type];	X	X	X
IA-5(1)	IA-5(1)_N.00	AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION The information system, for password-based authentication: (a) Enforces minimum password complexity of [a minimum of (12) characters for those systems subject to USGCB, a minimum of (8) characters for other systems (where USGCB does not apply), and must contain a combination of letters, numbers, and special characters];	X	X	X
	IA-5(1)_N.01	(b) Enforces at least the following number of changed characters when new passwords are created: [one changed character or as determined by the system];	X	X	X

	IA-5(1)_N.02	c. Stores and transmits only cryptographically-protected passwords;	X	X	X
	IA-5(1)_N.03	(d) Enforces password minimum and maximum lifetime restrictions of [USGCB - 1 Day minimum 60 Day maximum, all Others bureau-defined];	X	X	X
	IA-5(1)_N.04	(e) Prohibits password reuse for [USGCB - 24 Passwords Remembered; all Others - 10 passwords remembered] generations; and	X	X	X
	IA-5(1)_N.05	(f) Allows the use of temporary password for a system logons with an immediate change to a permanent password;	X	X	X
IA-5(2)	IA-5(2)_N.00	AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION The information system, for PKI-based authentication: (a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;		X	X
	IA-5(2)_N.01	(b) Enforces authorized access to the corresponding private key;		X	X
	IA-5(2)_N.02	(c) Maps the authenticated identity to the account of the individual or group; and		X	X
	IA-5(2)_N.03	(d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.		X	X

	IA-5(2)_T.096	Certification Authority (CA) systems used to support Treasury Public Key Infrastructure (PKI) certificates shall be subordinate to the Treasury root CA. *INFORMATIVE: This control applies when certificates are used to authenticate systems or provide public cryptographic keys to fulfill requests originating outside local networks.*	X	X	X
IA-5(3)	IA-5(3)_N.00	AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION The organization requires that the registration process to receive [HSPD-12 SmartCards] be conducted [Selection: in person; by a trusted third party] before [Bureau-defined registration authority] with authorization by [Bureau-defined personnel or roles].		X	X
IA-5(11)	IA-5(11)_N.00	AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION The information system, for hardware token-based authentication, employs mechanisms that satisfy [Bureau-defined token quality requirements].	X	X	X
IA-8	IA-8_N.00	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) Control: The information system uniquely identifies and authenticates non-organizational users (or	X	X	X

		processes acting on behalf of non-organizational users).			
	IA-8_T.090	Bureaus shall deploy identification and authentication technology consonant with the results of the e-authentication risk analysis.	X	X	X
IA-8(3)	IA-8(3)_N.00	IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-APPROVED PRODUCTS The organization employs only FICAM-approved information system components in [Bureau-defined information systems] to accept third-party credentials.	X	X	X