NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: IRS 1075
Focal Document URL: https://www.irs.gov/pub/irs-pdf/p1075.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-irs-1075-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1.0	FEDERAL TAX INFORMATION, REVIEWS and OTHER REQUIREMENTS	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.2	Authorized Use of FTI	Any agency that receives FTI for an authorized use may not use that information in any manner or for any purpose not consistent with that authorized use. If an agency needs FTI for a different authorized use under a different provision of IRC § 6103, a separate request must be sent to IRS Disclosure. An unauthorized secondary use of FTI is specifically prohibited and may result in discontinuation of disclosures to the agency and imposition of civil or criminal penalties on the responsible officials. The Office of Safeguards validates that an agency's "need and use" of FTI conforms with the governing provisions allowing the disclosure of FTI. The agency's SSR must describe the purpose(s) for which FTI is collected, used, maintained and shared.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.3	Secure Data Transfer	The IRS established a Secure Data Transfer (SDT) program to provide encrypted electronic transmission of FTI between the IRS and trading partners. For support with establishing an IRS SDT account, please submit an SDT Customer Support Request. Complete information on establishing an SDT account is available in the SDT Handbook. The SDT Handbook is available from a local IRS governmental liaison or a request to the Safeguards mailbox. Only the following types of documents will be accepted via SDT: Contact the SafeguardReports@irs.gov mailbox for specific details on how to submit information via SDT.	Functional	No Relationship	N/A	N/A	N/A	0	1.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.3-1	Secure Data Transfer	Control File (.txt)	Functional	No Relationship	N/A	N/A	N/A	0	1.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.3-2	Secure Data Transfer	Adobe (.pdf)	Functional	No Relationship	N/A	N/A	N/A	0	1.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.3-3	Secure Data Transfer	Word Document (.doc or .docx)	Functional	No Relationship	N/A	N/A	N/A	0	1.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.3-4	Secure Data Transfer	Excel Document (.xls or.xlsx)	Functional	No Relationship	N/A	N/A	N/A	0	1.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.3-5	Secure Data Transfer	Zipped File (.zip)	Functional	No Relationship	N/A	N/A	N/A	0	1.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.4	State Tax Agency Limitations	FTI may be obtained per IRC § 6103(d) by state tax agencies only to the extent the information is needed for and is reasonably expected to be used for state tax administration. An agency's records must include some account of the result of its use of FTI (e.g., disposition of closed cases and summary of revenues generated) or include reasons why the information was not used. If any agency continually receives FTI that it is unable to use for any reason, it must contact the IRS official liaison and discuss the need to stop the receipt of this FTI. State tax agencies using FTI to conduct statistical analysis, tax modeling or revenue projections must notify the IRS by submitting a signed Need and Use Justification Statement for Use of Federal Tax Information form and follow the established guidelines (available through the assigned Governmental Liaison). Annually, the agency must provide updated information in the SSR regarding its modeling activities that include FTI. In the SSR, the agency must describe: • Any use of FTI that is in addition to what was described in the original Need and Use Justification Form • Any new, previously unreported internal tax administration compilations that include FTI • Changes to the listing of authorized employees (Attachment B to the Need and Use Justification Form) If the agency intends to use a contractor or sub-contractor for conducting statistical analysis, tax modeling or revenue projections, it must submit a 45-day notification (see Section 1.9.4, Disclosing FTI to Contractors or Sub-Contractors) prior to contractor or sub-contractor access to the FTI. The agency's SSR must detail the use of FTI for this purpose. In addition, the agency must submit a separate statement detailing the methodology used and data to be used by the contractor or sub-contractor. The Office of Safeguards and Statistics of Income functions will review the information provided to confirm that adequate safeguarding protocols are in place and that the modeling methodology to be used to remove taxpayer identifying information is appropriate.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.5	Coordinating Safeguards within an Agency	Because of the diverse purposes that authorized disclosures may be made to an agency and the division of responsibilities among different components of an agency, FTI may be received and used by several quasi-independent units within the agency's organizational structure. Where there is such a dispersal of FTI, the agency must centralize safeguarding responsibilities to the greatest extent practical and establish and maintain uniform safeguard standards consistent with IRS guidelines. The official(s) assigned these responsibilities must hold a position high enough in the agency's organizational structure to ensure compliance with the agency safeguard standards and procedures. The selected official(s), or point(s) of contact (POC(s)) must also be responsible for ensuring that internal inspections are conducted, submission of required safeguard reports to the IRS, properly reporting any data breach incidents, disclosure awareness training and for any necessary liaison with the IRS.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.6	Safeguard Reviews	A safeguard review is an on-site, remote, or a combination of both (hybrid) evaluation of the use of FTI and the measures employed by the receiving agency and its agents (where authorized) to protect the data. This review includes all FTI received whether from the IRS or a secondary source such as SSA, Bureau of the Fiscal Service or another agency (see Federal Tax Information). Safeguard reviews are conducted to determine the adequacy of safeguards as opposed to evaluating an agency's programs. Several factors will be considered when determining the need for a review, the type of review, and the frequency of which a review will be conducted.	Functional	No Relationship	N/A	N/A	N/A	0	1.6 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.6-1	Safeguard Reviews	On-site reviews: Disclosure Enforcement Specialists (DES), Cybersecurity Reviewers (CSR), and Management Officials will conduct an on-site evaluation of the security and privacy controls implemented by the agency and all supporting parties. Assessment techniques include, but are not limited to visual inspections, observations, interviews, document exchange, and automated scanning.	Functional	No Relationship	N/A	N/A	N/A	0	1.6 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.6-2	Safeguard Reviews	Remote reviews: Disclosure Enforcement Specialists, Cybersecurity Reviewers, and Management Officials will conduct a remote evaluation of the security and privacy controls implemented by the agency and all supporting parties using secured collaborative technologies (e.g., screen-sharing capabilities, teleconferences, video enabled software, etc.). Assessment techniques include, but are not limited to visual inspections, observations, interviews, document exchange, and automated scanning.	Functional	No Relationship	N/A	N/A	N/A	0	1.6 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.6.1	Before the Review	The IRS initiates the review by communication with an agency point of contact (POC) as reported by the agency in the SSR. The preliminary discussion will be followed by a formal engagement letter to the agency head, which provides official notification of the planned safeguard review. This engagement letter outlines what the review will encompass. Additional requests for specific information will be provided to the agency POC. These requests may include a list of records to be reviewed (e.g., training manuals, flowcharts, policies, awareness program documentation and organizational charts relating to the processing of FTI). Prior to the review, the agency POC will receive information regarding the manner in which the review will be conducted (e.g., on-site and/or remote), the scope and purpose of the review, a list of the specific areas to be reviewed and agency personnel to be interviewed. A Preliminary Security Evaluation (PSE) call will be held to determine the scope of the review (see NIST Control PM-5 C.1, Inventory of PII). The electronic flow of FTI will be discussed to provide the review team with a thorough understanding of the location and use of FTI throughout the agency's infrastructure. During the call primary POCs will be introduced, the scope of the review will be defined, assessment logistics will be discussed, and any questions will be answered. Participants should include agency IT staff knowledgeable about the location and flow of FTI throughout the agency as well as staff or contractors from other locations such as consolidated data centers. Additionally, mini-PSE calls for contractors, sub-contractors, off-site locations, etc. may be needed to obtain additional information in determining the review scope. Requests for additional information and clarification to include automated scanning procedures will be discussed after the PSE call(s) and a proposed scope will be provided.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1.6.2	During the Review	The review process validates the accuracy of the SSR and conformance with the current version of Publication 1075 requirements and National Institute of Standards and Technology (NIST) Special Publication 800-53. At the opening conference, review procedures will be communicated, followed by a data flow discussion, and confirming the flow of FTI (see NIST Control PM-5 CE-1, Inventory of PII). Observing actual operations is a required step in the review process. Sites to be reviewed will be based on the flow of the FTI, which may include, but are not limited to, field offices, consolidated data centers, off-site storage facilities, disaster recovery sites, contractor and sub-contractor sites. Review methods may include but are not limited to: Agencies must facilitate execution of the review methods utilized by Safeguards staff. Agency management approval must be obtained prior to review, if agency policies and procedures contradict any of these methods. The agency POC will be advised the of critical issues and findings as the review progresses. A briefing will be held with the POC to go over the Preliminary Findings Report (PFR) before the closing conference. The closing conference is held upon completion of the agency's review, where the PFR is issued to provide the agency an overview of the findings identified during the review.	Functional	No Relationship	N/A	N/A	N/A	0	1.6.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.6.2-1	During the Review	Spot check agency records for FTI	Functional	No Relationship	N/A	N/A	N/A	0	1.6.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.6.2-2	During the Review	Employee interviews	Functional	No Relationship	N/A	N/A	N/A	0	1.6.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.6.2-3	During the Review	Facility tours	Functional	No Relationship	N/A	N/A	N/A	0	1.6.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.6.2-4	During the Review	Document review	Functional	No Relationship	N/A	N/A	N/A	0	1.6.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.6.2-5	During the Review	Automated/manual testing (See Safeguards website for tools used for automated testing)	Functional	No Relationship	N/A	N/A	N/A	0	1.6.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.6.2-6	During the Review	Remote assessment tools	Functional	No Relationship	N/A	N/A	N/A	0	1.6.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.6.3	After the Review	An SRR and CAP will be issued within 45 days of the closing conference to document the review findings. Requests for corrections to the SRR must be emailed to the SafeguardReports@irs.gov mailbox. The Office of Safeguards will respond with an acknowledgement and a determination. Each finding will be identified with a criticality level that identifies potential risk to loss, breach or disclosure of FTI. See Safeguards Finding Criticality Definitions for more details. All findings must be addressed in a timely fashion. The Office of Safeguards will identify deadlines for resolution based upon the risk associated with each finding. Outstanding issues must be resolved and addressed in the next reporting cycle of the CAP. If the Agency has any critical findings, the agency must submit a mitigation plan to Safeguards within 7 days from the closing conference date. Safeguards will report the critical findings along with your agency plan to the Treasury Inspector General for Tax Administration (TIGTA). The CAP must be updated and submitted semi-annually using the last CAP issued by the Office of Safeguards (see Section 2.E.5, Corrective Action Plan) until all review findings are accepted as closed. If an agency has a CAP due within 60 days of the review, that CAP is not required because the remaining open findings will be handled as part of the upcoming on-site or remote Safeguard Review Each CAP submission must include an explanation and/or evidence of actions already taken or planned to resolve all outstanding findings. The agency must submit an actual or planned implementation date for each outstanding finding.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.7	Termination of FTI	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.7.1	Agency Request	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.7.1.1	Termination Documentation	When an agency no longer requires FTI, notify Safeguards at SafeguardReports@irs.gov by providing the following: Once documentation is reviewed, the Office of Safeguards will send an acknowledgement of the agency's termination, instructions on Safeguard reporting and on-site review obligations. Instructions for reinstatement will be included in the acknowledgement letter.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.7.1.1.1	Termination Documentation	Copies of notifications to all agencies from which FTI is received, that FTI will no longer be requested, and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.7.1.1.2	Termination Documentation	Letter from the Head of Agency certifying that all residual FTI has been destroyed. (See Section 2.F Disposal of FTI – IRC § 6103(p)(4)(F))	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.7.1.2	Archiving FTI Procedure	This section is for agencies terminating receipt of FTI but required by statute to retain FTI for designated periods. If residual FTI is required to be retained by statute for a designated period (e.g., 5 or 10 years), then agencies must: • Ensure that a currently authorized agency, contractors, or sub-contractor retain FTI in accordance with Publication 1075 security standards • Provide copies of notifications as shown in Section 1.7.1.1, Termination Documentation • Submit an annual SSR each year while the agency has possession or oversight of the data • Continue to be subject to periodic Safeguard Reviews • Submit a letter from Head of Agency certifying that all residual FTI has been destroyed when the retention period has ended	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.7.2	FTI Suspension, Termination and Administrative Review	The IRS may terminate or suspend disclosure of return and return information to any authorized recipient under 6103(p)(4), if the IRS determines that: Prior to terminating FTI, the IRS will notify the authorized recipient in writing and may suspend further disclosures if it is deemed that federal tax administration would be seriously impaired. Agencies in receipt of the termination or suspension letter may appeal the determination as outlined in Exhibit 3, USC Title 26, CFR § 301.6103(p)(7)-1.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.7.2.1	FTI Suspension, Termination and Administrative Review	The authorized recipient (or agency) has allowed an unauthorized inspection or disclosure of FTI and has not taken adequate corrective action to prevent the recurrence of an unauthorized inspection or disclosure; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.7.2.2	FTI Suspension, Termination and Administrative Review	The authorized recipient does not satisfactorily maintain the safeguards prescribed by Section 6103(p)(4) and Publication 1075 and has made no adequate plan to improve its system to maintain the safeguards satisfactorily.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.8	Reporting Improper Inspections or Disclosures	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.8.1	Terms	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.8.2	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.8.3	Office of Safeguards Notification Process	Concurrent to notifying TIGTA, the agency must notify the Office of Safeguards by email to Safeguards mailbox, safeguardreports@irs.gov. To notify the Office of Safeguards, the agency must document the specifics of the incident or breach known at that time into a data incident report, including but not limited to: Reports must be sent electronically and encrypted via IRS-approved encryption techniques as outlined in Section 2.E.3, Encryption Requirements. Use the term "data incident report" in the subject line of the email. Do not include any FTI in the data incident report. Even if all information is not available, immediate notification is the most important factor, not the completeness of the data incident report. Additional information must be provided to the Office of Safeguards as soon as it is available. The agency will cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident.	Functional	No Relationship	N/A	N/A	N/A	0	1.8.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.8.3-1	Office of Safeguards Notification Process	Name of agency and agency POC for resolving data incident with contact information	Functional	No Relationship	N/A	N/A	N/A	0	1.8.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.8.3-2	Office of Safeguards Notification Process	Date and time the incident/breach occurred	Functional	No Relationship	N/A	N/A	N/A	0	1.8.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.8.3-3	Office of Safeguards Notification Process	Date and time the incident/breach was discovered	Functional	No Relationship	N/A	N/A	N/A	0	1.8.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.8.3-4	Office of Safeguards Notification Process	How the incident/breach was discovered	Functional	No Relationship	N/A	N/A	N/A	0	1.8.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1.8.3-5	Office of Safeguards Notification Process	Description of the incident/breach and the data involved, including specific data elements, if known	Functional	No Relationship	N/A	N/A	N/A	0	1.8.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.8.3-6	Office of Safeguards Notification Process	Potential number of FTI records involved; if unknown, provide a range if possible	Functional	No Relationship	N/A	N/A	N/A	0	1.8.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.8.3-7	Office of Safeguards Notification Process	Address where the incident/breach occurred	Functional	No Relationship	N/A	N/A	N/A	0	1.8.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.8.3-8	Office of Safeguards Notification Process	IT involved (e.g., laptop, server, mainframe)	Functional	No Relationship	N/A	N/A	N/A	0	1.8.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.8.3-9	Office of Safeguards Notification Process	Does the incident involve an unauthorized access or	Functional	No Relationship	N/A	N/A	N/A	0	1.8.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.8.3-10	Office of Safeguards Notification Process	disclosure by an agency employee? (Y/N) If a criminal indictment is not pursued, will a disciplinary or adverse action be proposed against the agency employee involved in this unauthorized access or disclosure? (Y/N)	Functional	No Relationship	N/A	N/A	N/A	0	1.8.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.8.4	Incident Response Procedures	In the event of an unauthorized disclosure or data breach, the agency must contact TIGTA and the IRS immediately. Both TIGTA and the IRS must be contacted within 24 hours of the discovery of the disclosure or breach. The agency must not wait to conduct an internal investigation to determine if FTI was involved. Any internal investigation conducted by the agency should not delay the timely reporting of the disclosure or breach. Incident response policies and procedures required in NIST Control IR-1, Incident Response Policy and Procedure, must be used when responding to an identified unauthorized disclosure or data breach incident. The Office of Safeguards will coordinate with the agency regarding appropriate follow-up actions required to be taken by the agency to ensure continued protection of FTI. Once the incident has been addressed, the agency will conduct a post-incident review to ensure the incident response policies and procedures provide adequate guidance. Any identified deficiencies in the incident response policies and procedures must be resolved as soon as reasonably possible. Additional training on any changes to the incident response policies and procedures must be provided to all employees, including contractors, sub contractors and consolidated data center employees, immediately. See - NIST Control IR-4, Incident Handling for additional information. The agency must test the incident response capability annually using tabletop exercises to determine the incident response effectiveness and document the results. See NIST Control IR-3, Incident Response Testing. The agency must track and document system security and privacy incidents. See NIST Control IR-5, Incident Monitoring.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
1.8.5	Incident Response Notification to Impacted Individuals	The agency must provide written notification to a taxpayer whose FTI was subject to unauthorized access or disclosure when a disciplinary or adverse action is proposed against the agency employee responsible. The required written notification to the taxpayer must include the date of the unauthorized inspection or disclosure and the rights of the taxpayer under IRC § 7431. The agency must confirm to the Office of Safeguards when the required written notification to the taxpayer is completed. In addition, the agency must inform the Office of Safeguards of any pending media releases, including sharing a draft of the release, prior to distribution.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.9	Disclosure to Other Persons	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.9.1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.9.2	Authorized Disclosure Precautions	When disclosure of FTI is authorized, the agency must take certain precautions prior to redisclosure to a contractor or sub-contractor, namely: • Has the IRS been given sufficient notice prior to releasing FTI to a contractor or sub-contractor? • Has the agency been given reasonable assurance through a visitation or received a report certifying that all security standards (physical and IT systems) have been addressed? • Does the contract authorizing the disclosure of FTI have the appropriate safeguard language? See the model language of Exhibit 7, Safeguarding Contract Language. Agencies must fully report to the IRS in their SSRs all disclosures of FTI to contractors and subcontractors. Any additional disclosures to contractors and sub-contractors must be reported using the Notification process and reported on the next annual SSR. An agency may not contract for the disclosure of FTI that is not authorized by IRC § 6103. Only contracts for services that require access to FTI to perform their duties under the contract are required to comply with these standards.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.9.3	External Personnel Security	An external provider refers to organizations other than the agency operating or acquiring the system. External providers include, for example, contractors or sub-contractors and other organizations providing system development, information technology services, outsourced applications, testing/assessment services and network and security management. Agencies must include personnel security requirements in contracts. External providers may have personnel working at agency facilities with credentials, badges or system privileges. Notifications of external personnel changes ensure appropriate termination of privileges and credentials. See NIST Control PS-7, External Personnel Security.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
1.9.4	Disclosing FTI to Contractors or Sub-Contractors	The agency must notify the Office of Safeguards prior to re-disclosing FTI to contractors or subcontractors. The agency must notify and obtain written approval from the Office of Safeguards prior to redisclosing FTI to sub-contractors (when the agency's contractor uses or desires to re-disclose FTI to another contractor). See Section 2.E, Reporting Requirements - 6103(p)(4)(E) and Section 2.E.6, Notification Reporting Requirements, for additional information. In addition to the notification, the agency must: • Establish privacy roles and responsibilities for contractors or sub-contractors and service providers to safeguard the confidentiality and integrity of FTI. • Include privacy requirements in contracts and other acquisition-related documents. • Share FTI externally only for the purposes statutorily authorized. • Where appropriate, enter into a contract, an SLA, memoranda of understanding, memoranda of agreement, letters of intent, computer matching agreement or similar agreement, with third parties that specifically describe the FTI covered and specifically enumerate the purposes for which the FTI may be used. • Monitor, audit and train its staff on the authorized uses and sharing of FTI with third parties and on the consequences of unauthorized use or sharing of FTI. • Require agency notification of contractor or sub-contractor personnel changes to ensure appropriate termination of privileges and credentials. See NIST Control PS-7, External Personnel Security. • Evaluate any proposed new instances of sharing FTI with third parties to assess whether they are authorized. • Require contractor or sub-contractor employ a formal sanction process for contractor employees and, when permitted by statute, sub-contractor employees failing to comply with established information security policies and procedures for FTI. Notification of designated agency personnel is required within 72 hours. If the agency requires the use of a contractor to conduct tax modeling, revenue estimation or other statistical activities, 45-day notification requirements apply (see Section 1.9.4, Disclosing FTI to Contractors). The Taxpayer First Act § 2004, which added IRC § 6103(p)(9), formalizes in statute the following agency requirements effective December 31, 2022: • Agencies must require that contractors, sub-contractors, or other agents have requirements in effect to provide safeguards required under IRC § 6103(p)(4) to protect FTI. • The Taxpayer First Act also codifies agency responsibilities to conduct on-site reviews of contractors, sub-contractors, and other agents and provide the findings of these reviews to Safeguards as part of the report required	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.9.5	Re-Disclosure Agreements	When required regulatory prerequisite steps are satisfied and where appropriate, under the authority of IRC § 6103(p)(2)(B), the IRS may execute an agreement with an agency that authorizes the re-disclosure of FTI to another entity. These agreements are negotiated and approved by IRS Disclosure with concurrence of the Office of Safeguards. Agreements must include language to enforce the requirements for: Federal agencies authorized by statute to enter into re-disclosure agreements are required to provide a list of all executed agreements annually in the SSR. When requested by the Office of Safeguards, agencies must provide a copy of all re-disclosure agreements within 30 days. An electronic copy must be sent to the Office of Safeguards via SDT. If SDT is not available, the agreements may be emailed to the SafeguardReports@irs.gov mailbox.	Functional	No Relationship	N/A	N/A	N/A	0	1.9.5 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.9.5-1	Re-Disclosure Agreements	Incident reporting related to FTI	Functional	No Relationship	N/A	N/A	N/A	0	1.9.5 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.9.5-2	Re-Disclosure Agreements	Implementing personnel sanctions for failure to comply with established information security policy and procedures related to FTI	Functional	No Relationship	N/A	N/A	N/A	0	1.9.5 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.9.5-3	Re-Disclosure Agreements	Confirmation to the agency any proposals of disciplinary and adverse action concerning unauthorized accesses and disclosures involving FTI	Functional	No Relationship	N/A	N/A	N/A	0	1.9.5 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.9.5-4	Re-Disclosure Agreements	Notification of individuals whose FTI was subject to unauthorized access or disclosure including the date the unauthorized access or disclosure of FTI occurred.	Functional	No Relationship	N/A	N/A	N/A	0	1.9.5 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
1.10	Return Information in Statistical Reports	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.10.1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1.10.2	Making a Request under IRC § 6103(j)	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.10.3	State Tax Agency Statistical Analysis	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2	PHYSICAL SECURITY REQUIREMENTS	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.A	Recordkeeping Requirement – IRC § 6103(p)(4)(A)	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.A.1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.A.2	Logs of FTI (Electronic and Non-Electronic Receipts)	The agency must establish a tracking system to identify and track the location of electronic and nonelectronic FTI from receipt until it is destroyed. The FTI log may include the following tracking elements: *To the extent possible, do not include FTI in the log. If FTI is used, the log must be secured in accordance with all other safeguarding requirements. If the authority to make further disclosures is present (e.g., agents/contractors/sub-contractors), information disclosed outside the agency must be recorded on a separate list or log. The log must: Agencies transmitting FTI from one mainframe computer to another, as in the case of the SSA sending FTI to state human services agencies, need only identify the bulk records transmitted. This identification will contain the approximate number of taxpayer records, the date of the transmissions, the best possible description of the records and the name of the individual making/receiving the transmission. See Figure 1 - Sample FTI Logs	Functional	Intersects With	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive/regulated data is stored, transmitted or processed.	5	2.A.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.A.2-1.1	Logs of FTI (Electronic and Non-Electronic Receipts)	Taxpayer Identifier*	Functional	No Relationship	N/A	N/A	N/A	0	2.A.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.A.2-1.2	Logs of FTI (Electronic and Non-Electronic Receipts)	Tax year(s)	Functional	No Relationship	N/A	N/A	N/A	0	2.A.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.A.2-1.3	Logs of FTI (Electronic and Non-Electronic Receipts)	Type of information (e.g., revenue agent reports, Form 1040, work papers)	Functional	No Relationship	N/A	N/A	N/A	0	2.A.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.A.2-1.4	Logs of FTI (Electronic and Non-Electronic Receipts)	The reason for the request	Functional	No Relationship	N/A	N/A	N/A	0	2.A.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.A.2-1.5	Logs of FTI (Electronic and Non-Electronic Receipts)	Date requested	Functional	No Relationship	N/A	N/A	N/A	0	2.A.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.A.2-1.6	Logs of FTI (Electronic and Non-Electronic Receipts)	Date received	Functional	No Relationship	N/A	N/A	N/A	0	2.A.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.A.2-1.7	Logs of FTI (Electronic and Non-Electronic Receipts)	Exact location of the FTI	Functional	No Relationship	N/A	N/A	N/A	0	2.A.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.A.2-1.8	Logs of FTI (Electronic and Non-Electronic Receipts)	Who has had access to the data	Functional	No Relationship	N/A	N/A	N/A	0	2.A.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.A.2-1.9	Logs of FTI (Electronic and Non-Electronic Receipts)	If disposed of, the date and method of disposition	Functional	No Relationship	N/A	N/A	N/A	0	2.A.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.A.2-2.1	Logs of FTI (Electronic and Non-Electronic Receipts)	Reflect to whom the disclosure was made	Functional	No Relationship	N/A	N/A	N/A	0	2.A.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.A.2-2.2	Logs of FTI (Electronic and Non-Electronic Receipts)	What was disclosed	Functional	No Relationship	N/A	N/A	N/A	0	2.A.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.A.2-2.3	Logs of FTI (Electronic and Non-Electronic Receipts)	Why it was disclosed	Functional	No Relationship	N/A	N/A	N/A	0	2.A.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.A.2-2.4	Logs of FTI (Electronic and Non-Electronic Receipts)	When it was disclosed	Functional	No Relationship	N/A	N/A	N/A	0	2.A.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.A.3	Converted Media	Conversion of FTI from paper to electronic media (scanning) or from electronic media to paper (print screens or printed reports) also requires tracking from creation to destruction of the converted FTI. All converted FTI must be tracked on logs containing the fields detailed in Section 2.A.2, Logs of FTI, (Electronic and Non-Electronic Receipts) depending upon the current form of the FTI, electronic or nonelectronic.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.A.4	Recordkeeping of Disclosures to State Auditors	When disclosures are made by a state tax agency to state auditors, recordkeeping requirements pertain only in instances where the auditors use FTI for further scrutiny and inclusion in their work papers. In instances where auditors read large volumes of records containing FTI, whether in paper or electronic format, the state tax agency need only identify bulk records examined. This identification will contain the approximate number of taxpayer records, the date of inspection, a description of the records and the name of the individual(s) making the inspection. Recordkeeping log samples are provided in Section 2.A.2, Logs of FTI, (Electronic and Non-Electronic Receipts). Disclosure of FTI to auditors external to child support enforcement, human services or labor benefit agencies is not authorized by statute. FTI in case files must be removed prior to access by the auditors.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.B	Secure Storage – IRC § 6103(p)(4)(B)	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.B.1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.B.2	Minimum Protection Standards	MPS establishes a uniform method of physically protecting data and systems as well as non-electronic forms of FTI. This method contains minimum standards that will be applied on a case-by-case basis. Because local factors may require additional security measures, management must analyze local circumstances to determine location, container, and other physical security needs at individual facilities. MPS have been designed to provide management with a basic framework of minimum-security requirements. The objective of these standards is to prevent unauthorized access to FTI. MPS thus requires two barriers. Example barriers under the concept of MPS are outlined in the following table. Each topic represents one barrier and must be used as a starting point to identify two barriers of MPS to protect FTI. See Table 1 - Minimum Protection Standards for details. The MPS or "two-barrier" rule applies to FTI, beginning at the FTI itself and extending outward to individuals without a need-to-know. MPS provides the capability to deter, delay or detect surreptitious entry. Protected information must be containerized in areas where unauthorized employees may have access after-hours. As an example, an agency often desires or requires that security personnel, custodial service workers, or landlords for non-government-owned facilities have access to locked buildings and rooms. This may be permitted if there is a second barrier to prevent access to FTI. A security guard, custodial services worker or landlord may have access to a locked building or a locked room if FTI is in a locked security container. If FTI is in a locked room but not in a locked security container, the guard, janitor, or landlord may have a key to the building but not the room. Additional controls have been integrated into this document that map to NIST Special Publication (SP) 800-53 Revision 5. These are identified in Section 4.0, NIST 800-53 Security and Privacy Controls. Per NIST guidelines, policies and procedures must be developed, documented and disseminated, as necessary, to facilitate implementing physical and environmental protection controls. Multifunction Devices (MFDs) or High-Volume Printers must be locked with a mechanism to prevent physical access to the hard disk or meet MPS. For additional guidance, see NIST Control PE-3, Physical Access Control.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2.B.2	Minimum Protection Standards	MPS establishes a uniform method of physically protecting data and systems as well as non-electronic forms of FTI. This method contains minimum standards that will be applied on a case-by-case basis. Because local factors may require additional security measures, management must analyze local circumstances to determine location, container, and other physical security needs at individual facilities. MPS have been designed to provide management with a basic framework of minimum-security requirements. The objective of these standards is to prevent unauthorized access to FTI. MPS thus requires two barriers. Example barriers under the concept of MPS are outlined in the following table. Each topic represents one barrier and must be used as a starting point to identify two barriers of MPS to protect FTI. See Table 1 – Minimum Protection Standards for details. The MPS or "two-barrier" rule applies to FTI, beginning at the FTI itself and extending outward to individuals without a need-to-know. MPS provides the capability to deter, delay or detect surreptitious entry. Protected information must be containerized in areas where unauthorized employees may have access after-hours. As an example, an agency often desires or requires that security personnel, custodial service workers, or landlords for non-government-owned facilities have access to locked buildings and rooms. This may be permitted if there is a second barrier to prevent access to FTI. A security guard, custodial services worker or landlord may have access to a locked building or a locked room if FTI is in a locked security container. If FTI is in a locked room but not in a locked security container, the guard, janitor, or landlord may have a key to the building but not the room. Additional controls have been integrated into this document that map to NIST Special Publication (SP) 800-53 Revision 5. These are identified in Section 4.0, NIST 800-53 Security and Privacy Controls. Per NIST guidelines, policies and procedures must be developed, documented and disseminated, as necessary, to facilitate implementing physical and environmental protection controls. Multifunction Devices (MFDs) or High-Volume Printers must be locked with a mechanism to prevent physical access to the hard disk or meet MPS. For additional guidance, see NIST Control PE-3, Physical Access Control.	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	8	
2.B.3	Restricted Area Access	Care must be taken to deny unauthorized access to areas containing FTI during duty and non-duty hours. This can be accomplished by creating restricted areas, security rooms or locked rooms. Additionally, FTI in any form (computer printout, photocopies, tapes, notes) must be protected during non-duty hours. This can be done through a combination of methods, including secured or locked perimeter, secured area or containerization. A restricted area is an area where entry is limited to authorized personnel (individuals assigned to the area). All restricted areas must either meet secured area criteria or provisions must be made to store FTI in appropriate containers during non-duty hours. Using restricted areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized access, disclosure, or theft of FTI. All the following procedures must be implemented to qualify as a restricted area. Restricted areas will be prominently posted and separated from non-restricted areas by physical barriers that control access. The number of entrances must be kept to a minimum and must have controlled access (e.g., electronic access control, key access, door monitor) to prevent unauthorized entry. The main entrance must be controlled by locating the desk of a responsible employee at the entrance to ensure that only authorized personnel with an official need may enter.	Functional	Intersects With				5	
2.B.3.1	Visitor Access Logs	A visitor access log must be maintained at a designated entrance to a restricted area and all visitors (persons not assigned to the area) entering the area shall be directed to the designated entrance. Prior to accessing areas that contain FTI, a visitor must sign a visitor access log. The security personnel must validate the person's identity by examining government-issued identification (e.g., state driver's license or passport). The security personnel must compare the name and signature entered in the access log with the name and signature of the government-issued identification. When leaving the area, the security personnel or escort must enter the visitor's time of departure. The visitor access log must require the visitor to provide the following information: Each restricted area access log must be closed out at the end of each month and reviewed by management. Visitor access logs must be retained for five (5) years, see Exhibit 9, Table 9. See Figure 2 – Visitor Access Log for details.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	2.B.3.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.3.1	Visitor Access Logs	A visitor access log must be maintained at a designated entrance to a restricted area and all visitors (persons not assigned to the area) entering the area shall be directed to the designated entrance. Prior to accessing areas that contain FTI, a visitor must sign a visitor access log. The security personnel must validate the person's identity by examining government-issued identification (e.g., state driver's license or passport). The security personnel must compare the name and signature entered in the access log with the name and signature of the government-issued identification. When leaving the area, the security personnel or escort must enter the visitor's time of departure. The visitor access log must require the visitor to provide the following information: Each restricted area access log must be closed out at the end of each month and reviewed by management. Visitor access logs must be retained for five (5) years, see Exhibit 9, Table 9. See Figure 2 – Visitor Access Log for details.	Functional	Intersects With	Identification Requirement	PES-06.2	Physical access control mechanisms exist to requires at least one(1) form of government-issued or organization-issued photo identification to authenticate individuals before they can gain access to the facility.	5	2.B.3.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.3.1-1	Visitor Access Logs	Name and organization of the visitor	Functional	Subset Of	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	10	2.B.3.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.3.1-2	Visitor Access Logs	Signature of the visitor	Functional	Subset Of	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	10	2.B.3.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.3.1-3	Visitor Access Logs	Form of identification	Functional	Subset Of	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	10	2.B.3.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.3.1-4	Visitor Access Logs	Date of access	Functional	Subset Of	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	10	2.B.3.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.3.1-5	Visitor Access Logs	Time of entry and departure	Functional	Subset Of	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	10	2.B.3.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.3.1-6	Visitor Access Logs	Purpose of visit	Functional	Subset Of	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	10	2.B.3.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.3.1-7	Visitor Access Logs	Name and organization of person visited	Functional	Subset Of	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	10	2.B.3.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.3.2	Authorized Access List	To facilitate the entry of employees/vendor/contractor/non-agency personnel who have a frequent and continuing need to enter a restricted area, but who are not assigned to the area, an Authorized Access List (AAL) can be maintained so long as MPS are enforced. See Section 2.B.2, Minimum Protection Standards. The AAL must contain the following: AAL must be reviewed monthly or upon occurrence or potential indication of an event such as a possible security breach or personnel change. If there is any doubt of the identity of the individual, the security monitor must verify the identity of the individual against the AAL prior to allowing entry into the restricted area. For additional guidance, see NIST Control PE-2, Physical Access Authorizations. Also, see NIST Control PE-16, Delivery and Removal, for guidance on controlling information system components entering and exiting the restricted area.	Functional	Subset Of	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	10	2.B.3.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.3.2-1	Authorized Access List	Name of employee/vendor/contractor/non-agency personnel	Functional	Subset Of	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	10	2.B.3.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.3.2-2	Authorized Access List	Agency or department name	Functional	Subset Of	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	10	2.B.3.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.3.2-3	Authorized Access List	Name and phone number of the agency POC authorizing access	Functional	Subset Of	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	10	2.B.3.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.3.2-4	Authorized Access List	Address of agency/vendor/contractor	Functional	Subset Of	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	10	2.B.3.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.3.2-5	Authorized Access List	Purpose and level of access	Functional	Subset Of	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	10	2.B.3.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2.B.3.3	Controlling Access to Areas Containing FTI	Management or a designee must maintain an authorized list of all personnel who have access to information system areas, where these systems contain FTI. This does not apply to those areas within the facility officially designated as publicly accessible. The agency must maintain a policy addressing issuance of appropriate authorization credentials, including badges, identification cards or smart cards. This policy must include proper use and accountability requirements. In addition, a list must be maintained that identifies those individuals who have authorized access to any systems where FTI is housed. Access authorizations and records maintained in electronic form are acceptable. Each agency must control physical access to the information system devices that display FTI information or where FTI is processed to prevent unauthorized individuals from observing the display output. For additional information, see NIST Control PE-5, Access Control for Output Devices. The agency or designee must monitor physical access to the information system where FTI is stored to detect and respond to physical security incidents. For additional information, see NIST Control PE-6, Monitoring Physical Access. For all areas that process FTI, the agency must position information system components within the facility to minimize the opportunity for unauthorized access. When cleaning and facility maintenance personnel work in restricted areas containing unsecured FTI, those activities must be performed in the presence of an authorized employee. The agency must establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel. The agency must verify that non-escorted personnel performing maintenance on the system possess the required access authorizations and if not, then the agency must designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities. See NIST MA-5, Maintenance Personnel. Allowing an individual to “piggyback” or “tailgate” into restricted locations must be prohibited and documented in agency policy. The agency must ensure that all individuals entering an area containing FTI do not bypass access controls or allow unauthorized entry of other individuals. Unauthorized access must be challenged by authorized individuals (e.g., those with access to FTI). Security personnel must	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	
2.B.3.4	Control and Safeguarding Keys and Combinations	All containers, rooms, buildings, and facilities containing FTI must be locked when not in actual use. Access to a locked area, room or container can be controlled only when the key or combination is controlled. Compromising a combination or losing a key negates the security provided by that lock. Combinations to locks must be changed annually or when an employee who knows the combination retires, terminates employment or transfers to another position. Combinations must be given only to those who have a need to have access to the area, room or container and must never be written on a sticky-note, calendar pad or any other item (even though it is carried on one’s person or hidden from view). An envelope containing the combination must be secured using the same security measures for the envelope as the locked material. Access control measures (keys, proximity cards, combinations) must be issued only to individuals having a need to access an area, room, or container. Inventory records must be maintained and must account for the total number of keys, proximity cards, combinations, etc. that are available and issued. The inventory must account for master keys and key duplicates. An annual reconciliation must be done on all key records. The number of keys or persons with knowledge of the combination to a secured area must be kept to a minimum. Keys and combinations will be given only to those individuals who have a frequent need to access the area.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
2.B.3.5	Locking Systems for Secured Areas	Access control systems (e.g., badge readers, smart cards, and biometrics) that provide the capability to audit access control attempts must maintain access control logs with successful and failed access attempts to secure areas containing FTI or systems that process FTI. Agency personnel must review access control logs on a monthly basis. The access control log must contain the following elements:	Functional	Intersects With	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	5	2.B.3.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.3.5-1	Locking Systems for Secured Areas	Owner of the access control device requesting access	Functional	Subset Of	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	10	2.B.3.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.3.5-2	Locking Systems for Secured Areas	Success/failure of the request	Functional	Subset Of	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	10	2.B.3.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.3.5-3	Locking Systems for Secured Areas	Date and time of the request	Functional	Subset Of	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	10	2.B.3.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.4	FTI in Transit	Handling FTI must be such that the FTI does not become misplaced or available to unauthorized personnel. Any time FTI is transported from one location to another, care must be taken to provide appropriate safeguards. When FTI is hand-carried by an individual in connection with a trip or in the course of daily activities, it must be kept with that individual and protected from unauthorized disclosures. All shipments of paper or electronic FTI (including compact disk [CD], digital video disk [DVD], thumb drives, hard drives, tapes and microform) must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. All FTI transported through the mail or courier/messenger service must be double-sealed; that is, one envelope within another envelope. The inner envelope must be marked confidential with some indication that only the designated official or delegate is authorized to open it. The outermost envelope must not be labeled as FTI or provide any indication that the contents contain FTI, since that may actually increase risk to the contents.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
2.B.4	FTI in Transit	Handling FTI must be such that the FTI does not become misplaced or available to unauthorized personnel. Any time FTI is transported from one location to another, care must be taken to provide appropriate safeguards. When FTI is hand-carried by an individual in connection with a trip or in the course of daily activities, it must be kept with that individual and protected from unauthorized disclosures. All shipments of paper or electronic FTI (including compact disk [CD], digital video disk [DVD], thumb drives, hard drives, tapes and microform) must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. All FTI transported through the mail or courier/messenger service must be double-sealed; that is, one envelope within another envelope. The inner envelope must be marked confidential with some indication that only the designated official or delegate is authorized to open it. The outermost envelope must not be labeled as FTI or provide any indication that the contents contain FTI, since that may actually increase risk to the contents.	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	5	
2.B.4	FTI in Transit	Handling FTI must be such that the FTI does not become misplaced or available to unauthorized personnel. Any time FTI is transported from one location to another, care must be taken to provide appropriate safeguards. When FTI is hand-carried by an individual in connection with a trip or in the course of daily activities, it must be kept with that individual and protected from unauthorized disclosures. All shipments of paper or electronic FTI (including compact disk [CD], digital video disk [DVD], thumb drives, hard drives, tapes and microform) must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. All FTI transported through the mail or courier/messenger service must be double-sealed; that is, one envelope within another envelope. The inner envelope must be marked confidential with some indication that only the designated official or delegate is authorized to open it. The outermost envelope must not be labeled as FTI or provide any indication that the contents contain FTI, since that may actually increase risk to the contents.	Functional	Intersects With	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	5	
2.B.4.1	Security During Office Moves	When it is necessary for an office to move to another location, plans must be made to protect and account for all FTI properly. FTI must be in locked cabinets or sealed packing cartons while in transit. Using sealed boxes serves the same purpose as double-sealing and prevents anyone from viewing the contents. FTI must remain in the custody of an agency employee and accountability must be maintained to ensure that cabinets or cartons do not become misplaced or lost during the move.	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	5	
2.B.5	Physical Security of Computers, Electronic and Removable Media	Computers and electronic media (including telephones using Voice Over Internet Protocol [VOIP]) that receive, process, store, access, protect and/or transmit FTI must be in a secure area with restricted access. In situations when requirements of a secure area with restricted access cannot be maintained, such as home work sites, remote terminals or other office work sites, the equipment must receive the highest level of protection practical, including full disk encryption. All computers and mobile devices that contain FTI and reside at an alternate work site must employ encryption mechanisms to ensure that FTI may not be accessed if the computer is lost or stolen. Basic security requirements must be met, such as keeping FTI locked up when not in use. When removable media contains FTI, it must be labeled as FTI. All computers, electronic media and removable media containing FTI must be kept in a secured area under the immediate protection and control of an authorized employee or locked up. When not in use, the media must be promptly returned to a proper storage area/container. Inventory records of computers, electronic and removable media must be maintained and reviewed semiannually for control and accountability. Section 2.A, Recordkeeping Requirement, contains additional information. For additional guidance on log retention requirements, see Exhibit 9, Record Retention Schedules. For physical security protections of transmission medium (e.g., cabling), see NIST Control PE-4, Access Control for Transmission.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2.B.5	Physical Security of Computers, Electronic and Removable Media	Computers and electronic media (including telephones using Voice Over Internet Protocol [VOIP]) that receive, process, store, access, protect and/or transmit FTI must be in a secure area with restricted access. In situations when requirements of a secure area with restricted access cannot be maintained, such as home work sites, remote terminals or other office work sites, the equipment must receive the highest level of protection practical, including full disk encryption. All computers and mobile devices that contain FTI and reside at an alternate work site must employ encryption mechanisms to ensure that FTI may not be accessed if the computer is lost or stolen. Basic security requirements must be met, such as keeping FTI locked up when not in use. When removable media contains FTI, it must be labeled as FTI. All computers, electronic media and removable media containing FTI must be kept in a secured area under the immediate protection and control of an authorized employee or locked up. When not in use, the media must be promptly returned to a proper storage area/container. Inventory records of computers, electronic and removable media must be maintained and reviewed semiannually for control and accountability. Section 2.A, Recordkeeping Requirement, contains additional information. For additional guidance on log retention requirements, see Exhibit 9, Record Retention Schedules. For physical security protections of transmission medium (e.g., cabling), see NIST Control PE-4, Access Control for Transmission.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	3	
2.B.6	Media Off-Site Storage Requirements	Media containing FTI that is sent to an off-site storage facility must be properly secured, labeled, and always protected from access by unauthorized individuals. The media may not be stored on open shelving, unless the shelving is in a restricted area (see Section 2.B.3, Restricted Area Access) accessible only to individuals with authorized access to FTI. The agency must ensure that contractoroperated off-site storage facilities maintaining FTI on open shelving comply with all safeguarding requirements (e.g., visitor access logs, internal inspections, contractor access restrictions, and employee training) and the contract must include Exhibit 7 safeguarding language. These facilities are subject to IRS safeguard reviews. Agencies that do not have the statutory authority to contract for services that involve the disclosure of FTI (e.g. state Human Services and certain workforce agencies not receiving data under 6103(d)), may not allow the release of media containing FTI to a contractor-operated off-site storage facility unless the following conditions are met:	Functional	Subset Of	Physically Secure All Media	DCH-06.1	Mechanisms exist to physically secure all media that contains sensitive information.	10	2.B.6 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.6-1	Media Off-Site Storage Requirements	The media is encrypted and labeled as containing "federal tax information"	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	2.B.6 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.6-1	Media Off-Site Storage Requirements	The media is encrypted and labeled as containing "federal tax information"	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	2.B.6 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.6-2	Media Off-Site Storage Requirements	The media is locked in a turtle case or security container	Functional	Intersects With	Physically Secure All Media	DCH-06.1	Mechanisms exist to physically secure all media that contains sensitive information.	5	2.B.6 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.6-3	Media Off-Site Storage Requirements	The agency retains the key to the turtle case	Functional	Intersects With	Physically Secure All Media	DCH-06.1	Mechanisms exist to physically secure all media that contains sensitive information.	5	2.B.6 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.B.7	Alternate Work Site	If the confidentiality of FTI can be adequately protected, telework sites such as employee's homes or other non-traditional work sites can be used. FTI remains subject to the same safeguard requirements and the highest level of attainable security. All the requirements of Section 2.B.5, Physical Security of Computers, Electronic and Removable Media, apply to alternate work sites.	Functional	Intersects With	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	5	
2.B.7.1	Equipment	The agency must retain ownership and control for all hardware, software and end-point equipment connecting to public communication networks, where these are present at alternate work sites. The use of virtual desktop infrastructure with non-agency-owned devices (including personally owned devices) is an acceptable alternative, where all requirements in Section 3.3.7 Virtual Desktop Infrastructure are met. Employees must have a specific room or area in a room that has the appropriate space and facilities for the type of work done. Employees also must have a way to communicate with their managers or other members of the agency if security problems arise. The agency must ensure employees have access to locking file cabinets or desk drawers so that documents, disks, and tax returns may be properly secured when not in use. If agency furniture is not furnished to the employee, the agency must ensure that an adequate means of storage exists at the alternate work site. The agency must provide "locking hardware" to secure automated data processing equipment to large objects, such as desks or tables. Smaller, agency-owned equipment must be locked in a filing cabinet or desk drawer when not in use.	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
2.B.7.2	Storing Data	FTI may be stored on hard disks only if agency-approved security access control devices (hardware/software) have been installed, are receiving regularly scheduled maintenance including upgrades and are being used. Access controls must include password security, an audit trail, encryption, virus detection and data overwriting capabilities.	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
2.B.7.3	Other Safeguards	Only agency-approved security access control devices and agency-approved software will be used. Use of illegal and/or non-approved software is prohibited. Electronic media that is to be reused must follow media sanitization requirements. The agency must maintain a policy for the security of alternative work sites. The agency must coordinate with the managing host system(s) and any networks and maintain documentation on the test. Before implementation, the agency must certify that the security controls are adequate for security needs. Additionally, the agency must develop and disseminate rules and procedures to ensure that employees do not leave computers unprotected at any time. These rules must address brief absences while employees are away from the computer. The agency must provide specialized training in security, disclosure awareness and ethics for all participating employees and managers. This training must cover situations that could occur as the result of an interruption of work by family, friends, or other sources.	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
2.C	Restricting Access – IRC § 6103(p)(4)(C)	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.C.1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.C.2	Policies and Procedures	Agencies must maintain the following policies and procedures relating to the safeguarding of FTI. For policies and procedures to be current, they need to have been updated or revalidated within the last three (3) years.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.2-1	Alternate Work Site – See Section 2.B.7 Alternate Work Sites	If permitted, a policy/procedure must address the security of FTI at alternate work sites. A policy is required even if alternate work sites are prohibited.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.2-2	Email – See Section 3.3.2 Email Communications	A policy/procedure must address the proper protection of FTI when transmitted by email, or if emailing of FTI is not allowed, a policy must state that it is prohibited.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.2-3	Facsimile - See Section 3.3.3 Facsimile and Facsimile Devices	A policy/procedure must address the proper protection of FTI when transmitted by facsimile, or if facsimile transmission of FTI is not allowed, a policy must state that it is prohibited.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.2-4	Employee Badge – See Section 2.B.2 and Table 1 Minimum Protection Standards	The policy/procedures must address when employees serve as secondary barriers for safeguarding FTI, picture identification badges or credentials must be visible and worn above the waist.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.2-5	FTI Disposal/Destruction – See Sections 2.A.2 FTI Logs, (Electronic and Non-Electronic Receipts), 2.F.3 Destruction and Disposal, 2.F.4 Other Precautions and 2.F.3.1 Media Sanitization	The policy/procedures must address the proper safeguarding of FTI including the tracking and the schedule/method of disposal or destruction.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.2-6	Incident Response – See NIST Control IR-1 and Sections 1.8.4 Incident Response Procedures	The policy/procedures must include the proper response to identified unauthorized disclosure or data breach incidents.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.2-7	Internal Inspections – See Sections 2.D.3 Internal Inspections and 2.D.9 Plan of Action and Milestones	The policy/procedures must include a documented schedule to ensure that all internal inspections are conducted timely. Additionally, a POA&M must be developed and monitored, including tracking the corrective actions identified during the internal inspections and identified actions planned to resolve the findings.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.2-8	Restricting Use of Personally Owned Computers – See Section 2.B.7.1 Equipment	The policy/procedures must include only agency-owned computers, media and software used to process, access and store FTI.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2.C.2-9	Disclosure Awareness, Security and Privacy, Role-Based and Contingency Training – See Sections 2.D.2 Training Requirements, 2.D.2.1 Disclosure Awareness Training, NIST Controls AT-2 Awareness Training, AT-3 Role-Based Training and CP-3 Contingency Training	These policies/procedures must contain a signed certification by the employee or contractor stating they understand the security policy and procedures for safeguarding FTI, prior to access to FTI.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.2-10	Transcript Delivery System (TDS) Audit Log Review (if applicable) – See Section 4.1, Access Control	The policy/procedures must address the development, documentation, and dissemination of audit/accountability security controls.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.2-11	Background Investigation – See Section 2.C.3 Background Investigation Minimum Requirements	The policy/procedure requires that employees, contractors, and sub-contractors (if authorized) with access to FTI must have a background investigation completed and favorably adjudicated.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.2-12	Access Control – See Section 2.B.3.3 Controlling Access to Areas Containing FTI and NIST Control AC-1, Access Control Policy and Procedures.	The policy/procedures must address the issuance of appropriate authorization credentials, including badges, identification cards or smart cards and include proper use and accountability requirements. The policy/procedures must also include the prohibition of allowing individuals to "piggyback" or "tailgate" into any location containing FTI.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.2-13	Audit and Accountability – see NIST Control AU-1, Audit and Accountability Policies and Procedures	The policy/procedures must address purpose, scope, roles, responsibilities, compliance, management commitment and coordination among organizational entities. Agencies must develop, document, and implement remediation actions for violations of the audit and accountability policy.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.2-14	Media Protection – see NIST Control MP-1, Media Protection Policies and Procedures	The policy/procedures must cover the protection of media to include access, marking, storage, transport, use and sanitization. See NIST Controls MP-1 through MP 7.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.2-15	Physical and Environmental – See NIST Control PE-1	The policy/procedures must include a clean desk policy for the protection of FTI; designate restricted IT areas that house IT assets such as, but not limited to, mainframes, servers, controlled interface equipment, associated peripherals, and communications equipment; and address specific building access systems, as needed.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.2-16	Personnel Security – See NIST PS-1, Personnel Security Policy and Procedures	The policy/procedures must address position risk designation, personnel screening, personnel termination, personnel transfer, access agreements and personnel sanctions.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.2-17	Insider Threat Program– See NIST Control PM-12, Insider Threat Program	The policy/procedures must address an insider threat program that includes a cross-discipline insider threat incident handling team and designate a senior official as the responsible individual to implement and provide oversight for the program.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.2-18	Privacy Program Plan3 – See NIST Control PM-18, Privacy Program Plan	A privacy program plan is a formal document that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program and the program management and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	2.C.2 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.3	Background Investigation Minimum Requirements	Determining the suitability of individuals who require access to U.S. government SBU information, including FTI, is a key factor in ensuring adequate information security. Prior to granting access to FTI and periodically thereafter, the Agency must complete a suitability background investigation that is favorably adjudicated by the Agency and to include, at a minimum, the following requirements: Federal agencies must conduct a suitability or security background investigation based on the position sensitivity of the individual's assigned position and risk designation associated with the investigative Tier established by the FIS. Granting access to FTI requires, at a minimum, a Tier 2 level investigation. A FIS Tier 2 standard background investigation meets the suitability investigative requirement for non sensitive positions designated as moderate risk public trust (requested using Standard Form 85P). Investigations conducted at Tiers 2-5 meet the minimum standard for an employee, contractor, and sub contractor with access to FTI. Federal agencies may be asked to provide evidence that the required background investigation was conducted for each individual granted access to FTI. FIS standards require reinvestigation, at a minimum, every five (5) years. State and local agencies that are not required to implement the federal background investigation standards must establish a personnel security program that ensures a background investigation is completed at the appropriate level for any individual who will have access to FTI using the guidance above as the minimum standard, with a reinvestigation conducted within five (5) years from the previous investigation.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	2.C.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.3-1	Background Investigation Minimum Requirements	Agencies must develop a written policy requiring that employees, contractors, and subcontractors (if authorized), with access to FTI must complete a background investigation that is favorably adjudicated. The policy will identify the process, steps, timeframes, and favorability standards that the agency has adopted. The agency may adopt the favorability standards set by the Federal Investigative Standards (FIS) or one that is currently used by another state agency, or the Agency may develop its own standards specific to FTI access.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	2.C.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.3-2	Background Investigation Minimum Requirements	The written background investigation policy must establish a result criterion for each required element that defines what would result in preventing or removing an employee's, contractor's and sub-contractor's access to FTI.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	2.C.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.3-3	Background Investigation Minimum Requirements	Agencies must initiate a background investigation for all employees, contractors, and subcontractors prior to permitting access to FTI.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	2.C.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.3-4	Background Investigation Minimum Requirements	State agencies must ensure a reinvestigation is conducted within five (5) years from the date of the previous background investigation for each employee, contractor, and sub-contractor requiring access to FTI.	Functional	Intersects With	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5	2.C.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.3-5	Background Investigation Minimum Requirements	Agencies must make written background investigation policies and procedures as well as a sample of completed employee, contractor, and sub-contractor background investigations available for inspection upon request.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	2.C.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.3-6	Background Investigation Minimum Requirements	Background investigations for any individual granted access to FTI must include, at a minimum:	Functional	Subset Of	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	2.C.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.3-6.1	Background Investigation Minimum Requirements	FBI fingerprinting (FD-258) - review of Federal Bureau of Investigation (FBI) fingerprint results conducted to identify possible suitability issues. Contact the appropriate state identification bureau for the correct procedures to follow. A listing of state identification bureaus can be found at: https://www.fbi.gov/about-us/cjis/identity-history-summary-checks/state-identification-bureau-listing. This national agency check is the key to evaluating the history of a prospective candidate for access to FTI. It allows the Agency to check the applicant's criminal history in all 50 states, not only current or known past residences.	Functional	Subset Of	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	2.C.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.3-6.2	Background Investigation Minimum Requirements	Check of local law enforcement agencies where the subject has lived, worked, and/or attended school within the last five (5) years and if applicable, of the appropriate agency for any identified arrests. The local law enforcement check will assist agencies in identifying trends of misbehavior that may not rise to the criteria for reporting to the FBI database but is a good source of information regarding an applicant.	Functional	Subset Of	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	2.C.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.3-6.3	Background Investigation Minimum Requirements	Citizenship/residency – Validate the subject's eligibility to legally work in the United States (e.g., a United States citizen or foreign citizen with the necessary authorization). Employers must complete USCIS Form I-9 to document verification of the identity and employment authorization of each new employee hired after November 16, 1986, to work in the United States. Within three (3) days of completion, any new employee must also be processed through E-Verify to assist with verification of their status and the documents provided with the Form I-9. The E-Verify system is free of charge and can be located at www.uscis.gov/e-verify. This verification process may only be completed on new employees. Any employee with expiring employment eligibility must be documented and monitored for continued compliance.	Functional	Subset Of	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	2.C.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.4	Personnel Actions	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.C.4.1	Personnel Transfer	When reassignments or transfers of individuals are permanent or of such extended durations certain actions are warranted. Agencies must define actions appropriate for these types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example, returning old and issuing new keys, identification cards and building passes; closing system accounts and establishing new accounts; changing system access authorizations (i.e., privileges); and access to official records to which individuals had access at previous work locations and in previous system accounts. See NIST Control PS-5, Personnel Transfer.	Functional	Intersects With	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2.C.4.2	Personnel Sanctions	Agencies must document in policy and procedure a formal sanctions process for individuals failing to comply with established information security policies and procedures. Agencies must notify designated agency personnel within 72 hours when a formal employee sanction process is initiated, identifying the individual sanctioned and any required administrative actions. See NIST Control PS-8, Personnel Sanctions. When the formal sanction is a proposed disciplinary or adverse action involving an unauthorized access or disclosure of FTI, the agency must provide written notification to the taxpayer whose FTI was subject to unauthorized access or disclosure. The required written notification must include the date the unauthorized access or disclosure of FTI occurred and the rights of the taxpayer under IRC § 7431 (see Section 1.8.5, Incident Response Notification to Impacted Individuals).	Functional	Intersects With	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
2.C.4.3	Personnel Termination	In personnel termination situations, certain actions are required. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, agencies must consider disabling the system accounts of individuals that are being terminated prior to the individuals being notified. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. System-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards and building passes. See NIST Control PS-4, Personnel Termination.	Functional	Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
2.C.5	Commingling of FTI	Commingling of FTI refers to having FTI and non-FTI data stored together, regardless of format. For example, commingling occurs when FTI is included in a sentence of text in a paper notice or letter; a row or column containing FTI in a database table; files stored on electronic media where some contain FTI and some do not; or at a shared data center where some systems contain FTI that require access restrictions, and some do not. Any kind of commingling creates the need for additional controls, since the introduction of FTI requires the entire letter, data table, removable media, etc. be handled and protected as FTI. It is recommended that FTI be kept physically and logically separate from other information to the maximum extent possible to avoid inadvertent disclosures and need for additional controls. Agencies should attempt to avoid maintaining FTI as part of their case files including any recordation or transcription in case notes or activity logs, whether paper or electronic. In situations where physical separation is impractical, the file must be clearly labeled to indicate that FTI is included and the file must be safeguarded. If a new address is received from IRS records and entered into a computer database, the address must be identified as FTI and safeguarded. If the taxpayer or third party subsequently provides the address independently, the address will not be considered FTI as long as the address is overwritten using individual or third-party knowledge or records as the source of information to replace the IRS source address. All FTI must be removed prior to releasing files to an individual or agency without authorized access to FTI.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	3	
2.C.5	Commingling of FTI	Commingling of FTI refers to having FTI and non-FTI data stored together, regardless of format. For example, commingling occurs when FTI is included in a sentence of text in a paper notice or letter; a row or column containing FTI in a database table; files stored on electronic media where some contain FTI and some do not; or at a shared data center where some systems contain FTI that require access restrictions, and some do not. Any kind of commingling creates the need for additional controls, since the introduction of FTI requires the entire letter, data table, removable media, etc. be handled and protected as FTI. It is recommended that FTI be kept physically and logically separate from other information to the maximum extent possible to avoid inadvertent disclosures and need for additional controls. Agencies should attempt to avoid maintaining FTI as part of their case files including any recordation or transcription in case notes or activity logs, whether paper or electronic. In situations where physical separation is impractical, the file must be clearly labeled to indicate that FTI is included and the file must be safeguarded. If a new address is received from IRS records and entered into a computer database, the address must be identified as FTI and safeguarded. If the taxpayer or third party subsequently provides the address independently, the address will not be considered FTI as long as the address is overwritten using individual or third-party knowledge or records as the source of information to replace the IRS source address. All FTI must be removed prior to releasing files to an individual or agency without authorized access to FTI.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	3	
2.C.5.1	Commingling of Electronic Media	If FTI is recorded on electronic media (e.g., tapes) with other data, it must be protected as if it were entirely FTI. Such commingling of data on electronic media should be avoided. When data processing equipment is used to process or store FTI and the information is mixed with agency data, access must be controlled by: Commingled data at multi-purpose facilities results in security and privacy risks that must be addressed. If the agency shares physical or computer facilities with other agencies, departments or individuals not authorized to have FTI, strict physical and systemic controls must be maintained to prevent unauthorized disclosure of this information.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	2.C.5.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.5.1-1	Commingling of Electronic Media	Restricting computer access only to authorized personnel	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	2.C.5.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.5.1-2	Commingling of Electronic Media	Systemic means, including labeling; for additional information, see NIST Control MP-3, Media Marking	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	2.C.5.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.5.1-3	Commingling of Electronic Media	When technically possible, data files, data sets and shares must be overwritten after each use	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	2.C.5.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.6	Access to FTI via State Tax Files or Through Other Agencies	Some state disclosure statutes and administrative procedures permit access to state tax files by other agencies, organizations or employees not involved in tax matters. As a general rule, IRC § 6103(d) does not permit access to FTI by such employees, agencies, or other organizations. The IRC clearly provides that FTI will be furnished to state tax agencies only for tax administration purposes and made available only to designated state tax personnel and legal representatives or to the state audit agency for an audit of the tax agency. Questions about whether particular state employees are entitled to access FTI must be forwarded to the Disclosure Manager at the IRS Office that serves your location4. Generally, the IRC does not permit state tax agencies to furnish FTI to other state agencies or to political subdivisions, such as cities or counties. State tax agencies may not furnish FTI to any other state or local agency, even where agreements have been made, informally or formally, for the reciprocal exchange of state tax information unless formally approved by the IRS. Also, non-government organizations, such as universities or public interest organizations performing research, cannot have access to FTI. Although state tax agencies are specifically addressed previously in this section, the restrictions on data access and non-disclosure to another agency or third party applies to all agencies authorized to receive FTI. Generally, statutes that authorize disclosure of FTI do not authorize further disclosures by the recipient agency. Unless IRC § 6103 provides for further disclosures by the agency, the agency cannot make such disclosures or otherwise grant access to FTI to either employees of another component of the agency not involved with administering the program for which the FTI was specifically received or to another state agency for any purpose. Agencies and subdivisions within an agency may be authorized to obtain the same FTI for different purposes, such as a state tax agency administering tax programs (IRC § 6103(d)) and a component human services agency administering benefit eligibility verification programs (IRC § 6103(l)(7)) or child support enforcement programs (IRC § 6103(l)(6)).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.C.7	Offshore Operations	FTI cannot be accessed by agency employees, agents, representatives, contractors, or sub-contractors located outside of the legal jurisdictional boundary of the United States (outside of the United States, its territories, embassies, or military installations). FTI must not be received, processed, stored, accessed, or transmitted to (IT) systems located offshore nor may FTI be sent offshore for disposal. Systems containing FTI must be located, operated and maintained by personnel physically located within the United States (this prohibits foreign remote maintenance, foreign call centers, help desks and the like) and should follow Publication 1075 requirements including the Background Investigation Requirements in Section 2.C.3. Some agencies may have a need for their employees to travel internationally for business purposes. As such, agencies must develop procedures to follow during foreign travel. When agency employees travel abroad, they must not: During international travel, batteries of agency-managed or Bring Your Own Device (BYOD) mobile devices and laptops must be removed from battery-powered mobile devices and stored separate from the device when left unattended. SIM cards must be removed and stored separate from devices that employ them when entering non-U.S. customs. Once agency employees return from abroad, it is important for agencies to ensure the continued security of networks where FTI resides. Agencies must sanitize all devices taken abroad prior to allowing them to connect to their trusted network. Additionally, agencies must disable wireless connectivity options until devices have been sanitized and may wish to provide additional security training for employees travelling abroad.	Functional	Subset Of	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	10	2.C.7 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2.C.7-1	Offshore Operations	Bring IT equipment containing stored FTI (e.g., laptop computers, tablets, phones, removable media); or	Functional	Subset Of	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	10	2.C.7 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.7-2	Offshore Operations	Access agency systems that receive, process, store, protect and/or transmit FTI.	Functional	Subset Of	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	10	2.C.7 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.C.8	Controls Over Processing	The agency must establish adequate controls to prevent disclosing FTI to other state agencies, tax or non-tax, or to political subdivisions, such as cities or counties, for any purpose, including tax administration, absent explicit written IRS authority granted under IRC § 6103(p)(2)(B). Processing of FTI in an electronic media format including removable media, microfilms, photo impressions or the conversion to other formats (including tape reformatting or duplication, reproduction or conversion to digital images or hard copy printout) will be performed as indicated in the environments listed in 2.C.8.1 and 2.C.8.2.	Functional	Subset Of	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	10	
2.C.8.1	Agency-owned and Operated Facility	Processing under this method will take place in a manner that will protect the confidentiality of the information on the electronic media. All safeguards outlined in this publication also must be followed and will be subject to IRS safeguard reviews.	Functional	Subset Of	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	10	
2.C.8.2	Agency, Contractor or Sub-Contractor Shared Facilities	Recipients of FTI are permitted to use a shared facility but only in a manner that does not allow access to FTI by employees, agents, representatives, or contractors of other agencies using the shared facility. For purposes of applying sections 6103(l), (m) and (n), the term "agent" includes contractors and subcontractors. Access restrictions pursuant to the IRC authority by which the FTI is received continue to apply; for example, human services agencies administering benefit eligibility programs may not allow contractors or sub-contractors, including consolidated data center contractors, access to any FTI. The agency must include, as appropriate, the requirements specified in Exhibit 7, Safeguarding Contract Language. The agency, as well as its contractor, sub-contractor and shared sites that receive, process, store, access, protect and/or transmit FTI, are subject to Safeguard reviews. These requirements also apply to releasing electronic media to a private contractor, sub-contractor or other agency office, even if the purpose is merely to erase the old media for reuse.	Functional	Subset Of	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	10	
2.C.9	Service Level Agreements (SLA)	Agencies using support functions, including, but not limited to, consolidated data centers, shared print facilities, and disaster recovery sites, must implement appropriate controls to ensure the protection of FTI. This includes a service level agreement (SLA) between the agency authorized to receive FTI and support functions. The SLA must cover the following: Generally, consolidated data centers are operated either by a separate state agency (e.g., Department of Information Services) or by a private contractor or sub-contractor. If an agency is considering transitioning to either a state-owned or private vendor consolidated data center, the Office of Safeguards strongly suggests the agency submit a request for discussions with Safeguards as early as possible in the decision making or implementation planning process. The purpose of these discussions is to ensure the agency remains compliant with safeguarding requirements during the transition to the consolidated data center.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
2.C.9-1	Service Level Agreements (SLA)	The agency with authority to receive FTI is responsible for ensuring the protection of all FTI received. The state support function shares responsibility for safeguarding FTI.	Functional	Subset Of	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	10	
2.C.9-2	Service Level Agreements (SLA)	The Exhibit 7 language must be included in the SLA between the recipient agency and support functions and in all contracts involving contractors or sub-contractors hired by the state support function.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
2.C.9-3	Service Level Agreements (SLA)	The SLA provides written notification to the state support function's management that they are bound by the provisions of Publication 1075, relative to protecting all FTI within their possession or control.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
2.C.9-4	Service Level Agreements (SLA)	The SLA shall detail the IRS's right to inspect state support function facilities and operations receiving, processing, storing, accessing, protecting and/or transmitting FTI under this agreement to assess compliance with requirements defined in IRS Publication 1075. The SLA shall specify that IRS's right of inspection includes the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
2.C.9-5	Service Level Agreements (SLA)	The SLA shall detail the state support function's responsibilities to address corrective action recommendations to resolve findings of noncompliance identified by IRS inspections.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
2.C.9-6	Service Level Agreements (SLA)	The agency will conduct an internal inspection of the state support function every 18 months, as described in Section 2.D.3, Internal Inspections. Multiple agencies sharing a state support function such as a consolidated data center may partner together to conduct a single, comprehensive internal inspection. However, care must be taken to ensure agency representatives do not gain unauthorized access to other agencies' FTI during the internal inspection.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
2.C.9-7	Service Level Agreements (SLA)	The employees from the state support function with access to or use of FTI, including system administrators and programmers, must:	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
2.C.9-7.1	Service Level Agreements (SLA)	Meet the background check requirements defined in Background Investigation Minimum Requirements and	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
2.C.9-7.2	Service Level Agreements (SLA)	Receive disclosure awareness training and sign a confidentiality statement, prior to initial access to or use of FTI, as well as annually thereafter. These provisions also extend to any contractors or sub-contractors hired by the state support function that have authorized access to or use of FTI.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
2.C.9-8	Service Level Agreements (SLA)	The specific data breach incident reporting procedures for all state support function employees, contractors and sub-contractors must be covered. The required disclosure awareness training must include a review of these procedures.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
2.C.9-9	Service Level Agreements (SLA)	Responsibilities must be identified for coordination of the 45-day notification of the use of contractors or sub-contractors with access to FTI.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
2.C.9-10	Service Level Agreements (SLA)	Require a formal sanction process for individuals covered by the SLA for failing to comply with established FTI security policies and procedures. Notification of designated agency personnel is required within 72 hours when the formal sanction is a proposed disciplinary or adverse action involving an unauthorized access or disclosure of FTI and must include the date the unauthorized access or disclosure of FTI occurred.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
2.C.10	Review Availability of Contractor and Sub-Contractor Facilities	As part of the agency review process, all affiliated contractors and sub-contractors who receive, transmit, process and store FTI on behalf of the agency are subject to review and testing. The agency must include Exhibit 7, Safeguarding Contract Language for all contracts. These requirements also apply to releasing electronic media to a private contractor, sub-contractor or other agency office, even if the purpose is merely to erase the old media for reuse.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
2.C.11	Restricting Access – Other Disclosures	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.C.11.1	Child Support Agencies—IRC §§ 6103(l)(6), (l)(8) and (l)(10)	In general, no officer or employee of any state or local child support enforcement agency can make further disclosures of FTI. However, limited information may be disclosed to agents, contractors or sub-contractors of the agency for the purpose of, and to the extent necessary in, establishing and collecting child support obligations from and locating individuals owing such obligations. The information that may be disclosed for this purpose to an agent, contractor, or a sub-contractor is limited to: • The address • Social Security Number of an individual with respect to whom child support obligations are sought to be established or enforced • The amount of any reduction under IRC § 6402(c) in any overpayment otherwise payable to such individual Tax refund offset payment information may not be disclosed by any federal, state or local child support enforcement agency employee, representative, agent, contractor, or sub-contractor into any court proceeding. To satisfy the re-disclosure prohibition, submit only payment date and payment amount for all payment sources (not just tax refund offset payments) into court proceedings. Additional information regarding the use of FTI for child support enforcement purposes can be found at: https://www.irs.gov/privacy-disclosure/use-of-federal-tax-information-fti-for-child-support-enforcementpurposes-matrix Forms 1099 and W-2 information are not authorized by statute to be disclosed to contractors or subcontractors under the child support enforcement program (IRC § 6103(l)(6)).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.C.11.2	Human Services Agencies—IRC § 6103(l)(7)	No officer or employee of any federal, state, or local agency administering certain programs under the Social Security Act, the Food Stamp Act of 1977, or Title 38, United States Code, or certain housing assistance programs is permitted to make further disclosures of FTI for any purpose. Human services agencies may not contract for services that involve the disclosure of FTI to contractors or sub-contractors.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.C.11.3	Deficit Reduction Agencies —IRC § 6103(l)(10)	Agencies receiving FTI from Bureau of Fiscal Service (BFS) related to tax refund offsets are prohibited from making further disclosures of the FTI received unless authorized.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.C.11.4	Centers for Medicare and Medicaid Services—IRC § 6103(l)(12)(C)	The Administrator of the Centers for Medicare and Medicaid Services (CMS) is authorized under IRC § 6103(l)(12)(C) to disclose FTI it receives from SSA to its agents for the purpose of, and to the extent necessary in, determining the extent that any Medicare beneficiary is covered under any group health plan. A contractual relationship must exist between CMS and the agent. The agent, however, is not authorized to make further disclosures of FTI for any purpose.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.C.11.5	Disclosures under IRC § 6103(l)(20)	Disclosures to officers, employees, contractors, and sub-contractors of SSA and other specified agencies are authorized to receive specific tax information for the purpose of carrying out the Medicare Part B premium subsidy adjustment and Part D Base Beneficiary Premium Increase. These disclosures and any redisclosures authorized by this provision are subject to safeguards requirements.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2.C.11.6	Disclosures under IRC § 6103(l)(21)	Disclosures to officers, employees, contractors, and sub-contractors of the U.S. Department of Health and Human Services (HHS) are at the request of a taxpayer seeking financial assistance for health insurance affordability programs. HHS may release FTI to an Exchange established under the Affordable Care Act or a state agency administering eligibility determinations for Medicaid or Children's Health Insurance Programs for the purpose of establishing eligibility for participation in the Exchange, verifying the appropriate amount of any credits and determining eligibility for participation in the state program. These disclosures are subject to safeguards requirements. Any agent contractor, or sub-contractor is also subject to IRS safeguard requirements and review. IRC § 6103(l)(21)(C) may allow HHS Office of Inspector General to have access to FTI maintained in the eligibility records of an Exchange or state entity administering these programs, under certain limited circumstances. This authority does not extend to independent state audit agencies that may not have access to FTI in eligibility records unless a contractual relationship is established that conforms to the disclosure requirements of IRC § 6103.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.C.11.7	Disclosures under IRC § 6103(l)	Federal law enforcement agencies receiving FTI pursuant to court orders or by specific request under section 6103(i) for purposes of investigation and prosecution of non-tax federal crimes, or to apprise of or investigate terrorist incidents, are subject to safeguards requirements and review. The Department of Justice (DOJ) must report in its SSR the number of FTI records provided and to which federal law enforcement agency the data was shared for the calendar year processing period.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.C.11.8	Disclosures under IRC § 6103(m)(2)	Disclosures to agents of a federal agency under IRC § 6103(m)(2) are authorized for the purposes of locating individuals in collecting or compromising a federal claim against the taxpayer in accordance with Sections 3711, 3717 and 3718 of Title 31. If the FTI is shared with agents, contractors, or sub contractors, the agency and agents, contractors, or sub-contractors are all subject to IRS safeguarding requirements and reviews.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.D	Other Safeguards - IRC § 6103(p)(4)(D)	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.D.1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.D.2	Training Requirements	Education and awareness are necessary to provide employees, contractors, sub-contractors, and other persons with the information to protect FTI. There are multiple components to a successful training program. In this section, training requirements are consolidated to ensure agencies understand the requirements to comply with this publication. Disclosure awareness training is described in detail within Section 2.D.2.1, Disclosure Awareness Training. Additional training requirements are located in various sections of the document and identified in the following table. See Table 2 - Training Requirements for details.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
2.D.2.1	Disclosure Awareness Training	Prior to granting an authorized agency employee, state support employee, contractor, or sub-contractor access to FTI, or to systems containing FTI, each employee, contractor, or sub-contractor must certify their understanding of the agency's security and privacy policy and procedures for safeguarding FTI through the agency's disclosure awareness training. The use of FTI in any training environment, including Disclosure Awareness training or material, is prohibited. Disclosure awareness training (including role-based training) must provide personnel who have access to FTI with initial and annual training on: Employees, contractors, and sub-contractors must be advised of the penalty provisions of IRC §§ 7431, 7213, and 7213A (see Exhibit 4, Sanctions for Unauthorized Disclosure, and Exhibit 5, Civil Damages for Unauthorized Disclosure). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches (see Section 1.8, Reporting Improper Inspections or Disclosures). During this training, agencies must make employees, contractors, or sub-contractors aware that disclosure restrictions and penalties apply even after employment or contract with the agency has ended. For the initial certification, and each annual recertification thereafter, the employee, contractor or sub contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of penalty provisions and the security requirements. It must also contain a statement that the employee understands they must report possible improper inspection or disclosure of FTI, including breaches and security incidents to both TIGTA and Safeguards within 24 hours. Example: I understand the penalty provisions of IRC §§ 7431, 7213 and 7213A. Example: I understand upon discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents, I must follow the proper incident reporting requirements to ensure the Office of Safeguards and the Treasury Inspector General for Tax Administration are notified of a possible issue involving FTI. The initial certification and recertification must be documented and placed in the agency's files for review and retained for at least five (5) years. The agency must include practical exercises in awareness training that simulate	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	2.D.2.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.D.2.1	Disclosure Awareness Training	Prior to granting an authorized agency employee, state support employee, contractor, or sub-contractor access to FTI, or to systems containing FTI, each employee, contractor, or sub-contractor must certify their understanding of the agency's security and privacy policy and procedures for safeguarding FTI through the agency's disclosure awareness training. The use of FTI in any training environment, including Disclosure Awareness training or material, is prohibited. Disclosure awareness training (including role-based training) must provide personnel who have access to FTI with initial and annual training on: Employees, contractors, and sub-contractors must be advised of the penalty provisions of IRC §§ 7431, 7213, and 7213A (see Exhibit 4, Sanctions for Unauthorized Disclosure, and Exhibit 5, Civil Damages for Unauthorized Disclosure). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches (see Section 1.8, Reporting Improper Inspections or Disclosures). During this training, agencies must make employees, contractors, or sub-contractors aware that disclosure restrictions and penalties apply even after employment or contract with the agency has ended. For the initial certification, and each annual recertification thereafter, the employee, contractor or sub contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of penalty provisions and the security requirements. It must also contain a statement that the employee understands they must report possible improper inspection or disclosure of FTI, including breaches and security incidents to both TIGTA and Safeguards within 24 hours. Example: I understand the penalty provisions of IRC §§ 7431, 7213 and 7213A. Example: I understand upon discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents, I must follow the proper incident reporting requirements to ensure the Office of Safeguards and the Treasury Inspector General for Tax Administration are notified of a possible issue involving FTI. The initial certification and recertification must be documented and placed in the agency's files for review and retained for at least five (5) years. The agency must include practical exercises in awareness training that simulate	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	5	2.D.2.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.D.2.1-1.1	Disclosure Awareness Training	Organizational authority for receiving FTI	Functional	Subset Of	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	10	2.D.2.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.D.2.1-1.2	Disclosure Awareness Training	Authorized uses of FTI	Functional	Subset Of	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	10	2.D.2.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.D.2.1-1.3	Disclosure Awareness Training	Disclosure of FTI with external parties only when authorized	Functional	Subset Of	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	10	2.D.2.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.D.2.1-1.4	Disclosure Awareness Training	Consequences of unauthorized access, use or disclosure of FTI	Functional	Subset Of	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	10	2.D.2.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.D.2.1-2.1	Disclosure Awareness Training	Email and other electronic messages to inform users	Functional	Subset Of	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	10	2.D.2.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.D.2.1-2.2	Disclosure Awareness Training	Discussion at group and managerial meetings	Functional	Subset Of	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	10	2.D.2.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.D.2.1-2.3	Disclosure Awareness Training	Security bulletin boards throughout the secure work areas	Functional	Subset Of	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	10	2.D.2.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.D.2.1-2.4	Disclosure Awareness Training	Security articles in employee newsletters	Functional	Subset Of	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	10	2.D.2.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.D.2.1-2.5	Disclosure Awareness Training	Pertinent articles that appear in the technical or popular press to share with members of the management staff	Functional	Subset Of	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	10	2.D.2.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.D.2.1-2.6	Disclosure Awareness Training	Posters to display with short, simple educational messages (e.g., instructions on reporting unauthorized access "UNAX" violations)	Functional	Subset Of	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	10	2.D.2.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.D.2.1-2.7	Disclosure Awareness Training	Additional formal and informal training	Functional	Subset Of	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	10	2.D.2.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.D.2.2	Disclosure Awareness Training Products	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2.D.3	Internal Inspections and On-Site Reviews	Another measure IRS requires for the safeguarding of FTI is internal inspections by the recipient agency. The purpose is to ensure that the security and privacy policies and procedures established by the agency to protect FTI are functioning, maintained, and enforced. The agency must submit copies of these inspection reports (see Internal Inspection Template on the Office of Safeguards website) to the IRS with the SSR (see Section 2.E.4, Safeguard Security Report). To provide an objective assessment, the inspection should be conducted by agency personnel outside the FTI using function being inspected. To provide reasonable assurance that FTI is adequately safeguarded, the inspection must address the safeguard requirements the IRC and IRS impose. The agency must monitor and audit privacy controls and internal privacy policy to ensure effective implementation. In a situation where it is unwieldy or otherwise not feasible for agency leadership to personally conduct the inspection, it is permissible for off-site locations with access to FTI to self-certify the internal inspection. If possible, the agency should make an initial visit to the off-site location prior to disclosing FTI and conduct an initial inspection. The agency must ensure the self-certified inspection is signed by an agency employee, received timely, reviewed thoroughly, have in-depth discussions with the person conducting the self-certification and submit the self-certified inspections with the agency SSR. Contractors and sub-contractors may not conduct self-certification internal inspections. Agencies must establish a review cycle as follows: • Field offices receiving FTI at least every three (3) years • Headquarters office facilities housing FTI and the agency computer facility at least every 18 months • All contractors and sub-contractors with access to FTI, including a consolidated data center or offsite storage facility: at least every 18 months The agency must complete a documented schedule (internal inspection plan), detailing the timing of all internal inspections in the current year and next two years (three-year cycle). The plan must be included as part of the SSR, as described in Section 2.E.4. Inspection reports, including a record of corrective actions, must be retained by the agency for a minimum of five years from the date the inspection was completed. IRS personnel may review these reports during a safeguard review. A summary of the agency's findings and the actions taken to correct any	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
2.D.4	Recordkeeping	Each agency and function within that agency shall maintain a log of all requests for FTI, including receipt and disposal of returns or return information. This includes any medium containing FTI, such as computer tapes, cartridges, CDs, or data received electronically.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.D.5	Secure Storage	FTI (including tapes, cartridges, or other removable media) must be stored in a secure location, safe from unauthorized access.	Functional	Subset Of	Media Storage	DCH-06	Mechanisms exist to:(1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and(2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	10	
2.D.6	Limited Access	Access to returns and return information (including tapes, cartridges, or other removable media) must be limited to only those employees, officers, contractors, and sub-contractors who are authorized access by law or regulation and whose official duties require such access. The physical and systemic barriers to unauthorized access must be reviewed and reported. An assessment of facility security features must be included in the report.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	8	
2.D.7	Disposal	Upon completion of use, agencies must ensure that the FTI is destroyed or returned to the IRS or the SSA according to the guidelines contained in Section 2.F, Disposing of FTI - IRC § 6103(p)(4)(F).	Functional	Intersects With	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	5	
2.D.8	Computer Systems Security	The agency's review of the adequacy of its cybersecurity provisions must provide reasonable assurance that access to FTI is limited to personnel who have a need-to-know. This need-to-know must be enforced electronically as well as physically (see Internal Inspection Template on the Office of Safeguards website and Section 4.1, Access Control, and other portions of Section 3.0, Cyber security Requirements, as applicable). The review of the computer facility must include the evaluation of cybersecurity and physical security controls.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
2.D.9	Plan of Action and Milestones (POA&M)	The agency must implement a process for ensuring that corrective actions are developed and monitored. The process must include the findings identified during the internal inspections and the remediation plans and dates to resolve these findings. Although similar, the IRS CAP covers findings identified by the Office of Safeguards during the safeguard review and would not include or track agency findings from the internal inspection process.	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
2.E	Reporting Requirements – IRC § 6103(p)(4)€	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.E.1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.E.2	Report Submission Instructions	Correspondence, reports, and attachments must be sent electronically to the Office of Safeguards using one of the following two methods: • SDT, if the agency participates in the SDT program. • Email to Safeguards mailbox at SafeguardReports@irs.gov. Email transmissions must be sent by an IRS-approved encrypted method as outlined in Section 2.E.3, Encryption Requirements. Agencies must follow the requirements below when submitting correspondence, reports, and attachments to the Office of Safeguards: • Submissions must include a signed certification letter from the Head of Agency or a designee. In the event the agency submits a report signed by a designee, there must be a delegation of authority signed by the Head of Agency (HOA). • All correspondence requiring HOA signature must be in the form of a handwritten (aka. Wet) signature or a digital certificate signature. The HOA can delegate individuals to sign these documents on their behalf. To do so, the HOA must provide a delegation of authority for individual they will assign as their designee. The delegation of authority must be kept current by the agency and retained for at least three years and will be reviewed by IRS personnel during Safeguard reviews. • Submissions must be made using official templates provided by the Office of Safeguards. • Reports referencing file attachments must clearly identify the filename and section contained within the attachment being referenced. • Attachments must be named clearly and identify the associated section in the SSR, CAP or 45- day notification. • Attachment filenames must follow a standardized naming convention, either by a logical order (e.g., CAPATT1, CAPATT2) or by finding number (e.g., D.1, H.1.3, H.13.4). • Attachments must not be embedded into the SSR, CAP or 45-day notification.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	8	
2.E.2	Report Submission Instructions	Correspondence, reports, and attachments must be sent electronically to the Office of Safeguards using one of the following two methods: • SDT, if the agency participates in the SDT program. • Email to Safeguards mailbox at SafeguardReports@irs.gov. Email transmissions must be sent by an IRS-approved encrypted method as outlined in Section 2.E.3, Encryption Requirements. Agencies must follow the requirements below when submitting correspondence, reports, and attachments to the Office of Safeguards: • Submissions must include a signed certification letter from the Head of Agency or a designee. In the event the agency submits a report signed by a designee, there must be a delegation of authority signed by the Head of Agency (HOA). • All correspondence requiring HOA signature must be in the form of a handwritten (aka. Wet) signature or a digital certificate signature. The HOA can delegate individuals to sign these documents on their behalf. To do so, the HOA must provide a delegation of authority for individual they will assign as their designee. The delegation of authority must be kept current by the agency and retained for at least three years and will be reviewed by IRS personnel during Safeguard reviews. • Submissions must be made using official templates provided by the Office of Safeguards. • Reports referencing file attachments must clearly identify the filename and section contained within the attachment being referenced. • Attachments must be named clearly and identify the associated section in the SSR, CAP or 45- day notification. • Attachment filenames must follow a standardized naming convention, either by a logical order (e.g., CAPATT1, CAPATT2) or by finding number (e.g., D.1, H.1.3, H.13.4). • Attachments must not be embedded into the SSR, CAP or 45-day notification.	Functional	Intersects With	Ad-Hoc Transfers	DCH-17	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	5	
2.E.3	Encryption Requirements	The Office of Safeguards requires that all reports, when sent to the Office of Safeguards via email, be transmitted using IRS-approved encryption methods to protect sensitive information. Agencies are requested to adhere to the following guidelines to use encryption: Refer to your specific file compression software user guide for instructions on how to compress and encrypt files. Known compatible products with IRS include but are not limited to WinZip and Secure Zip. Please remember, while the attachment is encrypted, the subject line and content of the email message will not be encrypted, so it is important that any sensitive information be contained in the attachment (encrypted document).	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	2.E.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.3-1	Encryption Requirements	Compress files in .zip or .zipx formats	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	2.E.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.3-2	Encryption Requirements	Encrypt the compressed file using Advanced Encryption Standard	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	2.E.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.3-3	Encryption Requirements	Use a minimum of 128-bit encryption key string	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	2.E.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.3-4	Encryption Requirements	Ensure a strong password or passphrase is generated to encrypt the file	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	2.E.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.3-5	Encryption Requirements	Communicate the password or passphrase with the Office of Safeguards through a separate email or via a telephone call to your IRS contact person. Do not provide the password or passphrase in the same email containing the encrypted attachment.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	2.E.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2.E.4	Safeguards Security Reports (SSR)	The SSR is the primary method for agencies to report to the IRS Office of Safeguards processes, procedures, and security and privacy controls in place to protect FTI in compliance with IRC § 6103(p)(4). Agencies have an annual requirement to submit SSRs after their initial receipt of FTI. There are enhanced requirements for agencies that are applying to receive FTI for the first time and for existing agencies requesting new FTI data streams.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.E.4.1	Initial SSR Submission Instructions – New Agency Responsibilities	Agencies executing data exchange agreements involving access to FTI will be subject to safeguarding requirements and must provide evidence that adequate safeguard protections and controls are in place before IRS will authorize the release of FTI. The agency must submit an initial SSR for approval at least 90 days prior to the agency's planned FTI receipt date. In order to obtain initial IRS approval to receive FTI, an agency must have an approved SSR. To facilitate IRS approval, the agency is expected to: • Designate an agency Safeguards POC, see Section 1.5 Coordinating Safeguards Within an Agency • Make program officials, contractors, and/or sub-contractors available to discuss access and use of FTI, as needed The agency is required to submit evidentiary documentation for the controls shown in Table 3 in conjunction with the first submission of the agency's SSR See Table 3 – SSR Evidentiary Documentation for details. If the agency does not submit all required evidentiary documentation as described above, the IRS reserves the right to conduct a safeguard review to assess the effectiveness of the controls established in order to approve the SSR prior to initial release of FTI. Subsequently, Safeguards will conduct a riskbased assessment to determine when to schedule an agency's first safeguard review after initial receipt of FTI. Refer to the Office of Safeguards website for additional guidance and instructions for completing the document.	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection:(1) Interface characteristics;(2) Security, compliance and resilience requirements; and;(3) The nature of the information communicated.	5	
2.E.4.2	Agencies Requesting New FTI Data Streams	Agencies currently receiving FTI with an approved SSR and seeking additional FTI data streams (i.e., FTI to be received under newly assigned program authority or expanded statutory authority under IRC § 6103), must submit the following documentation along with the request to receive the new data stream(s): • Approved SSR for the most recent reporting period • Current CAP with approved mitigation strategies for critical and significant findings • Documentation of security testing for the system(s) where the new data stream will be processed. Any findings deemed "critical" must be mitigated • A signed Authority to Operate (ATO) for the system(s) that will be receiving, processing, storing, accessing, protecting and/or transmitting the new FTI data stream that is not covered in the agency's SSR already on file After the agency receives its new data stream, the subsequent SSR submission must reference the receipt of the new data stream and must describe all systems that receive, process, store, access, protect and/or transmit FTI. This SSR submission must also describe all security and privacy control implementations for the FTI environment(s).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.E.4.3	Annual SSR Update Submission Instructions	The agency must update and submit the SSR annually. The purpose of the SSR is for agencies to document the implementation of security and privacy controls that impact the protection of FTI. Agencies must document significant changes to the environment, as applicable. Examples of changes include, but are not limited to: The following information must be updated in each SSR submission to reflect routine updates or changes to the implementation of security and privacy controls and/or the agency's safeguarding program: The annual SSR update must be submitted on the prior year's SSR analysis that was returned to the agency. This will allow for a version control of the document, assurance that the agency addressed all outstanding items previously noted and reduces the need for recreating the entire document.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes.	5	2.E.4.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.4.3-1.1	Annual SSR Update Submission Instructions	New data exchange agreements	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes.	10	2.E.4.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.4.3-1.2	Annual SSR Update Submission Instructions	New computer equipment, systems or applications (hardware or software) (e.g., moving FTI systems to a FedRAMP authorized cloud environment, re-engineering legacy case management systems)	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes.	10	2.E.4.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.4.3-1.3	Annual SSR Update Submission Instructions	New facilities including, office moves, new contractor or sub-contractor locations (e.g., print vendor, call center)	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes.	10	2.E.4.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.4.3-1.4	Annual SSR Update Submission Instructions	Organizational changes, such as moving IT operations to a consolidated data center from an embedded IT operation	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes.	10	2.E.4.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.4.3-1.5	Annual SSR Update Submission Instructions	Development of new business processes or procedures for handling FTI	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes.	10	2.E.4.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.4.3-2.1	Annual SSR Update Submission Instructions	Changes to information or procedures previously reported	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes.	10	2.E.4.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.4.3-2.2	Annual SSR Update Submission Instructions	Current annual period safeguard activities (e.g., performing internal inspections, performing ongoing security and privacy control testing, providing security and privacy awareness training to employees)	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes.	10	2.E.4.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.4.3-2.3	Annual SSR Update Submission Instructions	Planned actions affecting safeguard procedures (e.g., system upgrades, development of new policy framework, use of a new audit log monitoring solution)	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes.	10	2.E.4.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.4.3-2.4	Annual SSR Update Submission Instructions	Agency use of contractors or sub-contractors (non-agency employees)	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes.	10	2.E.4.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.4.4	SSR Submission Dates	The SSR must be submitted annually with all applicable attachments. Each submission of the SSR must include a description of updates or changes that have occurred during the reporting period. Submission due dates are defined below: See Table 4 – SSR Submission Dates *The Postal abbreviation for Commonwealth of the Northern Mariana Islands was updated to MP. Educational institutions receiving IRS addresses to locate debtors under IRC § 6103(m)(4)(B) must send compliance reports to the Department of Education as the federal oversight agency for this program. When extenuating circumstances exist, agencies may request an SSR extension, in 30-day increments, with a maximum of 60 days. Extension requests must be submitted not later than 30 days prior to the scheduled SSR due date. Request for extensions will not be considered after the scheduled SSR due date. A request for a second extension must be accompanied by a draft SSR. Extension requests must be sent to the Office of Safeguards via SDT or sent via email to SafeguardReports@irs.gov, with the subject "SSR Extension Request". The body of the email must address the reasons for the request. All extension requests will be evaluated on a case by case basis. Safeguards will provide an email response, approving or disapproving the request, within five (5) business days after receipt of the request.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.E.5	Corrective Action Plan	The Corrective Action Plan (CAP) is a report containing the findings, the recommended corrective actions, and targeted implementation dates for each weakness identified during an on-site, remote, or hybrid review. The CAP and SRR documents are the same in content, however, the CAP document has functionality to allow agencies to report their progress on corrective actions. The IRS will provide each agency an SRR along with a CAP upon completion of an on-site, remote or hybrid review. The agency must complete the CAP by providing an updated status to each unresolved finding, including the projected or actual date to close the finding, as well as provide status updates to any remaining planned actions. All findings must be addressed in a timely fashion or an out of cycle CAP review may be done to further address an agency's open critical and significant findings. Safeguards will initiate communication with the agency's POC, and a formal engagement letter will be sent. At that time, the agency will be required to update their CAP and provide documentation for closure consideration of the remaining critical and significant findings. The out of cycle CAP review process will include: The agency may be required to submit a mitigation plan if any critical findings remain open and escalation of the p7 process maybe initiated per Exhibit 3, USC Title 26, CFR § 301.6103(p)(7)-1. The agency will receive an updated CAP to resolve outstanding issues in the next reporting cycle.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable;(7) Point of Contact (POC) (e.g., asset/process owner);(8) Resources required to conduct remediation actions;(9) Planned remedial actions to the deficiency(ies);(10) Proposed remediation timeline; and(11) Disposition statement (e.g., closeout summary).	5	2.E.5 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2.E.5-1	Corrective Action Plan	A preliminary discussion held prior to the review of the findings.	Functional	Subset Of	Capabilities Deficiency Tracking	IAO-05	minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner);(8) Resources required to conduct remediation actions;(9) Planned remedial actions to the	10	2.E.5 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.5-2	Corrective Action Plan	During the review, the agency's CAP responses and supporting documentation will be addressed. Requests for additional information and clarification, including automated scanning reports, will be made by Safeguards.	Functional	Subset Of	Capabilities Deficiency Tracking	IAO-05	minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner);(8) Resources required to conduct remediation actions;(9) Planned remedial actions to the	10	2.E.5 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.5-3	Corrective Action Plan	A closing conference will be held upon the completion of the agency's CAP review and a Preliminary Assessment Report (PAR) will be issued to provide the agency an overview of the findings addressed during the review.	Functional	Subset Of	Capabilities Deficiency Tracking	IAO-05	minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner);(8) Resources required to conduct remediation actions;(9) Planned remedial actions to the	10	2.E.5 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.5.1	CAP Submission Instructions	The agency must update and submit the CAP semi-annually to document all corrective actions, taken or planned, in response to the findings enumerated in the SRR. To complete the CAP document, agencies must:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.E.5.1-1	CAP Submission Instructions	Use the version sent by the Office of Safeguards with the SRR and must not alter the format	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.E.5.1-2	CAP Submission Instructions	Provide a written narrative in response to each finding	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.E.5.1-3	CAP Submission Instructions	Provide a planned implementation date or actual completion date in MM/DD/YYYY format for each finding response	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.E.5.1-4	CAP Submission Instructions	Provide evidentiary documentation to validate the closure of any findings identified as Critical or Significant	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.E.5.1-5	CAP Submission Instructions	Provide a signed certification from the Chief Information Security Officer (CISO) or Head of Agency to document and close findings that are no longer applicable to the agency's handling of FTI. Often, this occurs when agencies decommission systems that once transmitted FTI, replace applications or systems with newer technologies, or perform major upgrades to versions of systems that continue to receive, process, store, access, protect and/or transmit FTI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.E.5.2	CAP Submission Dates	CAP Submission due dates are defined below. See Table 5 - CAP Submission Dates for details. *The Postal abbreviation for Commonwealth of the Northern Mariana Islands was updated to MP. If the SRR was issued within 60 days from the upcoming CAP due date in the preceding chart, the agency's first CAP will be due on the subsequent reporting date to allow the agency adequate time to document all corrective actions proposed and taken. Agency CAP submissions provided to the Office of Safeguards within 60 days of an upcoming review will be responded to as part of the review process. When extenuating circumstances exist, agencies may request an extension for no more than 30 days. Extension requests must be submitted not later than 30 days prior to the scheduled CAP due date. Request for extensions will not be considered after the scheduled CAP due date. Extension requests must be sent to the Office of Safeguards via SDT or sent via email to SafeguardReports@irs.gov, with the subject "CAP Extension Request". The body of the email must address the reasons for the request. All extension requests will be evaluated on a case by case basis. Safeguards will provide an email response approving or disapproving the request within five (5) business days after receipt of the request.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.E.6	Notification Reporting Requirements	IRC § 6103 limits the usage of FTI to only those purposes explicitly stated. Due to the security and privacy implications, higher risk of unauthorized disclosure and potential for unauthorized use of FTI based on specific activities conducted, the Office of Safeguards requires advanced notification of at least 45 days prior to implementing certain operations or technology capabilities that require additional uses of the FTI. In addition to the initial receipt of FTI (see Section 1.1), the following circumstances or technology implementations require the agency to submit notification to the Office of Safeguards via the SafeguardReports@irs.gov, mailbox, a minimum of 45 days ahead of the planned implementation: See Table 6 – Notification Reporting for details. See additional details pertaining to each notification topic in the following sections. Contact the Office of Safeguards mailbox with any questions pertaining to notification requirements.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.E.6.1	Cloud Computing	Receiving, processing, storing, accessing, protecting, and/or transmitting FTI in a cloud environment requires prior notification to the Office of Safeguards. The intent of the notification is to require agencies to: If the agency cannot demonstrate it prevents the cloud service provider from having logical access to the data, the agency must submit a notification for disclosure to a contractor or sub-contractor. Refer to Section 3.3.1, Cloud Computing and the Safeguards website for more information related to cloud computing requirements.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	2.E.6.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.6.1-1	Cloud Computing	Document the physical locations where FTI will be processed to ensure FTI remains onshore	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes	10	2.E.6.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.6.1-2	Cloud Computing	Document the cloud service provider's FedRAMP authorization such that Safeguards does not have the responsibility to assess the physical security of cloud service provider facilities	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes	10	2.E.6.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.6.1-3	Cloud Computing	Explain how encryption will be used to prevent unauthorized disclosures to cloud service provider employees	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes	10	2.E.6.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.6.1-4	Cloud Computing	Document all agency-managed security and privacy controls	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes	10	2.E.6.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.E.6.2	Contractor or Sub-Contractor Access	Redisclosure of FTI to contractors or sub-contractors by authorized agencies requires notification to IRS at least 45 days prior to the planned re-disclosure. Contractors or sub-contractors consist of but are not limited to cloud computing providers, consolidated data centers, off-site storage facilities, shred companies, IT support or tax modeling/revenue forecasting providers. The contractor notification requirement also applies in the circumstance where the contractor hires additional sub-contractor services. Approval is required if the (prime) contractor hires additional sub contractor services in accordance with Exhibit 6, Contractor 45-Day Notification Procedures. Notification is also required for contractors or sub-contractors to perform statistical analysis, tax modeling or revenue projections (see Section 1.4, State Tax Agency Limitations).	Functional	Intersects With	Transfer Authorizations	DCH-14.2	Mechanisms exist to verify that individuals or Technology Assets, Applications and/or Services (TAAS) transferring data between interconnecting TAAS have the requisite authorizations (e.g., write permissions or privileges) prior to transferring said data.	5	
2.E.6.3	Tax Modeling	The agency must notify the Office of Safeguards if planning to include FTI in statistical analysis, tax modeling or revenue projections. The Office of Safeguards will forward the notification to the IRS Statistics of Income and Disclosure for approval of the modeling methodology (see Section 1.4, State Tax Agency Limitations). Tax modeling approvals are valid up to three years. If the agency needs to continue the use of FTI in tax modeling past the approved timeframe, a new request must be submitted to the Office of Safeguards.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.E.6.4	Live Data Testing	Agencies must submit a Data Testing Request (DTR) form to request approval to use live FTI in a testing environment. The intent of the notification is to ensure agencies do not process FTI in environments that do not have the same security and privacy controls as the production environment. Safeguards must review the security posture of the development or test environment as described in the agency's notification document submission to determine whether the agency has reduced the risk to an acceptable level. The IRS defines live data as primarily unmodified, non-sanitized data extracted from taxpayer files that identifies specific individual or corporate taxpayers and includes taxpayer information or tax return information. State taxing agencies must ensure their Need and Use Justification statements include the use of FTI in a test environment. Testing request approvals are valid up to three years from the date of the approval. If testing FTI data is no longer required before the approval expires, FTI must be removed from the test environment. If the agency needs to continue the use of FTI in pre-production testing activities past the approved timeframe, a new request for live data must be submitted to the Office of Safeguards. Please see the Office of Safeguards website for additional information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.F	Disposing of FTI – IRC § 6103(p)(4)(F)	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.F.1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.F.2	Returning IRS Information to the Source	Agencies electing to return IRS information must use a receipt process and ensure that the confidentiality is protected at all times during transport (see Section 2.B.4, FTI in Transit).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2.F.3	Destruction and Disposal	FTI furnished to the user and any paper material generated from it, such as copies, photo impressions, computer printouts, notes and work papers, must be destroyed by burning or shredding. If a method other than burning or shredding is used, that method must make the FTI unreadable or unusable. The following guidelines must be observed when destroying paper FTI: See Table 7 - FTI Destruction Methods for details. FTI furnished or stored in electronic format must be destroyed in the following manner: Whenever physical media leaves the physical or systemic control of the agency for maintenance, exchange or other servicing, any FTI on it must be destroyed by sanitizing according to guidance in NIST Control MP-6, Media Sanitization and Section 2.F.3.1, Media Sanitization. FTI must be purged from the media prior to allowing release. When using either method for destruction, every third piece of physical electronic media must be checked to ensure appropriate destruction of FTI. Hand tearing, recycling, or burying information in a landfill are unacceptable methods of disposal.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control 2.F.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.F.3-1	Destruction and Disposal	Electronic media (e.g., hard drives, tapes, CDs and flash media) must be destroyed according to guidance in NIST Control MP-6, Media Sanitization. Electronic media containing FTI must not be made available for reuse by other offices or released for destruction without first being subjected to electromagnetic erasing. If reuse is not intended, the tape must be destroyed by burning or shredding in accordance with applicable standards (see Section 2.F.3.1, Media Sanitation).	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	8	2.F.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.F.3-2	Destruction and Disposal	Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by burning.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	8	2.F.3 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.F.3.1	Media Sanitization	The type of sanitization performed depends on whether or not the media will be reused by the agency or leaving agency control. If the media will be reused by the agency for the same purpose of storing FTI and will not be leaving organization control, then clearing is a sufficient method of sanitization. If the media will be reused and repurposed for a non-FTI function or will be leaving organization control (i.e., media being exchanged for warranty, cost rebate or other purposes and where the specific media will not be returned to the agency), then purging must be selected as the sanitization method. If the media will not be reused at all, then destruction is the method for media sanitization. The requirements are applicable for media used in "preproduction" or "test" environments. The technique for clearing, purging, and destroying media depends on the type of media being sanitized. The following media sanitization requirements are required: See also MP-6. Media Sanitization. Additional media sanitization requirements are available on the Office of Safeguards website.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	8	2.F.3.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.F.3.1-1	Media Sanitization	Every third piece of media must be tested after sanitization has been completed.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	3	2.F.3.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.F.3.1-2	Media Sanitization	Media sanitization must be witnessed or verified by an agency employee.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	3	2.F.3.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.F.3.1-3	Media Sanitization	Media sanitization requirements are the same, regardless of where the information system media is located. However, the party responsible for each step of the sanitization process may differ.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	2.F.3.1 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.F.4	Other Precautions	FTI must never be disclosed to an agency's agents, contractors, or sub-contractors during disposal without legal authorization and destruction must be witnessed by an agency employee. The Department of Justice, state tax agencies, and SSA may be exempted from the requirement of having agency personnel witness destruction by a contractor or sub-contractor. If a contractor or sub-contractor is used: If the agency has legal authority to disclose FTI to a disposal contractor or sub-contractor and chooses one that is National Association for Information Destruction (NAID) certified, the agency will not be required to complete an internal inspection every 18 months of that facility. However, the agency must annually validate and maintain the most recent copy of the NAID certification.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control 2.F.4 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.F.4-1	Other Precautions	The contract must contain safeguard language in Exhibit 7a and 7b, Safeguarding Contract Language as appropriate to the contract to ensure the protection of FTI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control 2.F.4 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.F.4-2	Other Precautions	Destruction of FTI must be certified by the contractor or sub-contractor when not witnessed by an agency employee.	Functional	Intersects With	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	5	2.F.4 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
2.F.4-3	Other Precautions	It is recommended that the agency periodically observe the process to ensure compliance with security of FTI until it reaches a non-disclosable state and that an approved destruction method is utilized.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control 2.F.4 subpoints were listed as bullet points in focal document, so we separated them and assigned numbers to improve mappability.
3.0	CYBERSECURITY REQUIREMENTS	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.2	Assessment Process	The Office of Safeguards will assess agency compliance with the security and privacy requirements identified in this publication as part of the annual reporting and review processes. The IT assessment will include a review of the agency's FTI inventory. All IT systems and supporting components receiving, accessing, storing, processing, protecting, or transmitting FTI must be included in the agency's FTI inventory. This includes, for example: end user and administrator workstations, host operating system(s), contractor systems or laptops, web servers, database management systems, hypervisors, storage arrays and cloud environments. The FTI inventory must also include networking components used to protect or transmit FTI and access an FTI environment. This includes, for example: border/perimeter firewall, virtual private network (VPN), core routers, wireless networks, voice over IP systems and site to site endpoints established with external networks when FTI is shared and/or accessed outside of the LAN. The scope of assessments includes any technology used to receive, process, store, access, protect and/or transmit FTI that is owned and managed by 1) the agency, 2) a state's consolidated IT organization, 3) the agency's contractors and sub-contractors (e.g., print vendors, collections agencies, application development contractors, network engineers at a state consolidated IT office, etc.) and 4) the agency's constituent counties included in an assessment. Requirements are assessed using manual and automated assessment procedures as they relate to NIST SP 800-53 security and privacy controls as outlined in this publication. To ensure a standardized cybersecurity review process, Cybersecurity Reviewers will conduct assessments using Safeguards Computer Security Evaluation Matrices (SCSEM) to evaluate agency policies, procedures and IT systems that receive, process, store, access, protect and/or transmit FTI. The following techniques will be used to collect evidence required to complete SCSEM assessments: See Table 8 – Assessment Methodologies for details. Please see Section 1.6.2, During the Review for information on the review process.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.3	Technology-Specific Requirements	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.3.1	Cloud Computing	To use a cloud computing model to receive, process, store, access, protect and/or transmit FTI, the agency must comply with all requirements in this publication. The following mandatory requirements are in effect for using cloud services to receive, process, store, access, protect and/or transmit FTI: Supplemental Guidance: If the agency or system has the ability to automatically provision or deprovision resources based on need, then it is considered a cloud environment. The service and deployment model used in a cloud computing environment will determine the responsibility for security and privacy controls implementation between the agency and the cloud provider for the protection of FTI that is stored or processed in the cloud environment. The Office of Safeguards tailors its assessment of an agency's cloud solution based on the cloud vendor's FedRAMP authorization boundary. For systems where cloud service providers maintain complete control over and have documented the security and privacy controls of those systems in its FedRAMP authorization framework, the Office of Safeguards will assess those controls using the Cloud SCSEM. For agency-managed systems that reside logically in the cloud environment, but remain outside of the FedRAMP authorization boundary, the Office of Safeguards will leverage its SCSEMs to assess the security posture of those systems. All testing will be performed using the methods described in Section 3.2, Table 8, Assessment Methodologies. Additional cloud computing guidance is available on the Office of Safeguards website. To determine if your agency is utilizing a cloud please use the following Cloud Decision Tree Note: https://www.irs.gov/pub/irs-utl/cloud-decision-tree.pdf	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.3.1.a	FedRAMP Authorization	FTI may only be introduced to cloud environments that have been provided an authorization by the Joint Advisory Board (JAB) or a Federal Agency.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.3.1.b	Onshore Access	Agencies must leverage vendors and services where (i) all FTI physically resides in systems located within the United States; and (ii) all accesses, and support of the systems and services are performed from the United States, its possessions and territories.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
3.3.1.c	Physical Description	Agencies and their cloud providers must provide a complete listing of all data center addresses where FTI will be received, processed, stored, accessed, protected and/or transmitted in their 45-Day notification form.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.3.1.d	Data Encryption in Transit	FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140 certified and operate utilizing the latest FIPS 140 compliant module(s). This requirement must be included in the SLA.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	
3.3.1.e	Data Encryption at Rest	FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryption mechanism. This requirement must be included in the SLA. Supplemental Guidance: If the agency is able to encrypt data in transit and at rest using the latest FIPS 140 certified solutions and maintain sole ownership of encryption keys, preventing logical access from the cloud service providers, Safeguards will consider this a logical barrier and will allow data types with restrictions (e.g., IRC § 6103 (l)(7) data) to move to a cloud environment. Using FIPS 140 certified encryption at rest exempts third-party contractors from some protection requirements such as training and background investigation requirements.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	8	
3.3.1.f	45-Day Notification	The agency must notify the IRS Office of Safeguards at least 45 days prior to transmitting FTI into a cloud environment, per Section 2.E.6, Notification Reporting Requirements.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.3.1.g	Service Level Agreements and Contracts	The agency must establish security and privacy controls, based on IRS Publication 1075, for how FTI is received, processed, stored, accessed, protected and/or transmitted inside the cloud environment. Agencies must provide the requirements through a legally binding contract or SLA with their third-party cloud provider.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
3.3.1.h	Data Isolation	Software and/or services that receive, transmit, process or store FTI must be isolated within the cloud environment so that other cloud customers sharing physical or virtual space cannot access other customer data or applications.	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	5	
3.3.1.i	Risk Assessment	The agency must conduct an annual assessment of the security and privacy controls in place on all information systems used for receiving, processing, storing, accessing, protecting and/or transmitting FTI.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	8	
3.3.1.j	Persistence of Data in Relieved Assets	Storage devices where FTI has resided must be securely sanitized and/or destroyed using methods acceptable by NIST. This requirement must be included in the SLA.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	8	
3.3.1.k	Multifactor Authentication	Agencies must implement sufficient multifactor authentication when their cloud solutions are available from the internet (i.e., there is access to the cloud solution from outside of the agency's trusted network). If the cloud can only be accessed from an agency's internal network, multifactor authentication must be implemented by agency solution(s) when establishing a remote connection.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:(1) Remote network access;(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or(3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	8	
3.3.1.l	Security Control Implementation	Customer defined security and privacy controls must be identified, documented and implemented, and must comply with Publication 1075 requirements.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
3.3.1.l	Security Control Implementation	Customer defined security and privacy controls must be identified, documented and implemented, and must comply with Publication 1075 requirements.	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
3.3.2	Email Communications	If the agency determines FTI is not permitted to be included in email, a written policy must be established and distributed to: If the agency determines FTI is permitted to be included in email, a written policy must be established and distributed to: Additionally, the agency must ensure FTI is properly protected and secured when being transmitted via email. At a minimum:	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.2 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.2.a-1	Email Communications	Prohibit FTI in email transmissions; and	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.2 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.2.b-1	Email Communications	Clearly state the actions that will be taken if FTI is inadvertently sent in email.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.2 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.2.a-2	Email Communications	Prohibit FTI in email transmissions outside of the agency's internal network;	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.2 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.2.b-2	Email Communications	Ensure transmissions are sent only to authorized recipients; and	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.2 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.2.c-2	Email Communications	Require adequate labeling (e.g., email subject contains "FTI") and protection.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.2 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.2.a-3	Email Communications	Mail servers and clients must be securely configured. Underlying operating systems of onpremises mail servers must be hardened and included in the agency's FTI inventory. A 45-day cloud notification must be submitted for cloud-hosted mail solutions.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.2 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.2.b-3	Email Communications	The network infrastructure must be securely configured to block unauthorized traffic, limit security vulnerabilities, and provide an additional security layer to an agency's mail servers and clients.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.2 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.2.c-3	Email Communications	Audit logging must be implemented to track all sent and received emails containing FTI.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.2 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.2.d-3	Email Communications	Email transmissions containing FTI must be encrypted using the latest FIPS 140 validated mechanism.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.2 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.2.e-3	Email Communications	Malware protection must be implemented at one or more points within the email delivery process to protect against viruses, worms and other forms of malware.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.2 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.3	Facsimile and Facsimile Devices	If the agency determines FTI is not permitted to be included in fax communications, a written policy must be established and distributed to: If the agency determines FTI is permitted to be included in fax communications, a written policy must be established and distributed to ensure fax communications are transmitted to an authorized recipient and must adhere to the following requirements: Additionally, the agency must ensure facsimile devices used to transmit FTI are properly protected and secured. At a minimum: If digital fax servers are used, they should be hardened like other servers containing FTI.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.3 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.3.a-1	Facsimile and Facsimile Devices	Prohibit FTI in fax communications; and	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.3 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.3.b-1	Facsimile and Facsimile Devices	Clearly state the actions that will be taken if FTI is inadvertently faxed.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.3 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.3.a-2	Facsimile and Facsimile Devices	Have a trusted staff member at both the sending and receiving fax machines	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.3 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.3.b-2	Facsimile and Facsimile Devices	Accurately maintain broadcast lists and other preset numbers of frequent recipients of FTI	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.3 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.3.c-2	Facsimile and Facsimile Devices	Place fax machines in a secured area	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.3 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.3.d-2	Facsimile and Facsimile Devices	Include a cover sheet on fax transmissions that explicitly provides guidance to the recipient, that includes:	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.3 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.3.d.1-2	Facsimile and Facsimile Devices	A notification of the sensitivity of the data and the need for protection	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.3 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.3.d.2-2	Facsimile and Facsimile Devices	A notice to unintended recipients to telephone the sender via collect call, if necessary, to report the disclosure and confirm destruction of the information	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.3 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.3.a-3	Facsimile and Facsimile Devices	When applicable, encrypt information or be connected to a secure network	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.3 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
3.3.3.b-3	Facsimile and Facsimile Devices	Securely configure multifunction devices (MFD) used to receive or transmit fax communications	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	3.3.3 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.4	Mobile Devices	To use FTI in a mobile device environment, the agency must implement a centralized mobile device management (MDM) solution to authenticate and manage the configuration of agency-owned and personally owned mobile devices prior to allowing access to the internal network. Further guidance of the configuration of mobile device solutions can be found on the Office of Safeguards website. See also AC-19: Access Control for Mobile Device	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	8	
3.3.5	Multifunction Devices (MFDs) and High-Volume Printers (HVPs)	If the agency determines FTI is not permitted to be printed, a written policy must be established and distributed to: If the agency determines FTI is permitted to be printed, a written policy must be established and distributed to: Additionally, the agency must ensure MFDs and HVPs are configured securely and included in the agency's FTI inventory.	Functional	Intersects With	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	8	3.3.5 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.5.a-1	Multifunction Devices (MFDs) and High-Volume Printers (HVPs)	Prohibit FTI from being printed	Functional	Intersects With	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	8	3.3.5 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.5.b-1	Multifunction Devices (MFDs) and High-Volume Printers (HVPs)	Clearly state the actions that will be taken if FTI is inadvertently printed	Functional	Intersects With	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	8	3.3.5 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.5.a-2	Multifunction Devices (MFDs) and High-Volume Printers (HVPs)	Prohibit printing FTI to printers outside of the agency's internal network	Functional	Intersects With	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	8	3.3.5 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.5.b-2	Multifunction Devices (MFDs) and High-Volume Printers (HVPs)	Ensure printed FTI is sent only to authorized printers (e.g., multifunction devices, standalone printers, high-volume printers)	Functional	Intersects With	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	8	3.3.5 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.5.c-2	Multifunction Devices (MFDs) and High-Volume Printers (HVPs)	Require adequate labeling and protection of all printed FTI	Functional	Intersects With	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	8	3.3.5 has multiple series of the same bullet points, so we added numbers at the end to separate them and improve mappability.
3.3.6	Network Boundary and Infrastructure	Agencies must implement boundary protection devices throughout their system architecture, including routers, firewalls, switches, and intrusion detection systems to protect FTI and FTI systems. The agency's managed interfaces employing boundary protection must deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception). Inbound services shall be prohibited unless a valid business case can establish their necessity. All remote access must be routed and monitored through a managed solution and accomplished using multifactor authentication per the requirements of NIST Control IA-2, Identification and Authentication (Organizational Users). FTI end users and privileged administrators may access the FTI environment over a secured wireless local area network (WLAN) infrastructure that complies with the Institute of Electrical and Electronic Engineers (IEEE) 802.11i wireless security standard and uses WPA2-certified equipment and software. All networking devices responsible for protecting the FTI environment or used to access the FTI environment must be included in the agency's FTI inventory. Additional network protection requirements are available on the Office of Safeguards website.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
3.3.7	Virtual Desktop Infrastructure	A virtual desktop infrastructure (VDI) provides users access to enterprise resources, including a virtual desktop from locations both internal to and external to the agency's networks. In a VDI environment, a user can access FTI by connecting to a virtual workstation via a vendor-specific agent, connection client, or through an Internet browser from practically any mobile device with Internet access. Using VDI environments is the only manner in which agencies may authorize their users to leverage personally owned devices to access and/or manage information systems that receive, process, store, access, protect and/or transmit FTI. See AC-20, Use of External Systems and the IRS Office of Safeguards website for more information.	Functional	Subset Of	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	10	
3.3.8	Public-Facing Systems	FTI is considered nonpublic information and may never be posted or shared on an unauthenticated publicly accessible system (e.g., public website). Agencies may have business needs to provide FTI to its individual constituents, customers, clients and/or stakeholders using interactive applications. Examples of such systems include tax applications meant to provide account information to taxpayers or practitioners, state-based marketplace systems, child support online portals, etc. Publicly facing systems are typically internet-based applications but may also include interactive voice response technology. Should an agency choose to provide FTI through a publicly facing system, it must implement the following requirements:	Functional	Intersects With	Web Security	WEB-01	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.	8	
3.3.8.a	Public-Facing Systems	The system architecture is configured as a multi-tier architecture with physically and/or logically separate systems that provide layered security of the FTI. Access to FTI in a back-end database must be brokered through multiple layers such that a public user cannot query the database directly.	Functional	Intersects With	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized Technology Assets, Applications and/or Services (TAAS) on certain services, protocols and ports.	8	
3.3.8.b	Public-Facing Systems	Each individual technology (e.g., application server, web server software, firewall) within the system architecture that receives, processes, stores, accesses, protects and/or transmits FTI is hardened in accordance with the requirements in this publication, the appropriate SCSEM and is subject to the agency's security testing capability.	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
3.3.8.c	Public-Facing Systems	Access to FTI via the system must only occur when following strong identity proofing and authentication processes consistent with the latest guidance in NIST SP 800-63-3, Digital Identity Guidelines and the other documents in the 800-63 suite: NIST SP 800-63A, Enrollment and Identity Proofing, NIST SP 800-63B, Authentication and Lifecycle Management and NIST SP800-63C, Federation and Assurances. Consistent with choosing a moderate-level baseline for security controls, the Office of Safeguards has determined that public-facing systems must implement Identity Assurance Level (IAL) 2 to confirm the identity at the point an account is established and then must use Authentication Assurance Level (AAL) 2 to confirm the veracity of the account's use upon each user login. Agencies may use Federation Assurance Level (FAL) 2 should they leverage federated identities. IAL2: There is evidence that supports the real-world existence of the claimed identity and the evidence verifies that the applicant is appropriately associated with this real-world identity. Either remote or physical identity proofing may be used depending on the evidence provided during the identity proofing step. AAL2: There is a high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocols. Approved cryptographic techniques are required. FAL2: There is a need to use federated identities to leverage sufficient encryption such that the agency is 1) the only party capable of decrypting the assertion from the third-party identity provider and 2) the identity provider cryptographically signs the assertion.	Functional	Intersects With	Web Security	WEB-01	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.	8	
4.0	NIST 800-53 SECURITY AND PRIVACY CONTROLS	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4.1	ACCESS CONTROL	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AC-1	Access Control Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
AC-1	Access Control Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
AC-1	Access Control Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
AC-2	Account Management	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5	
AC-2	Account Management	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
AC-2	Account Management	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
AC-2	Account Management	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
AC-2(CE-1)	Automated System Account Management	Support the management of system accounts using automated mechanisms. Supplemental Guidance: Automated mechanisms can include internal system functions and email, telephonic, and text messaging notifications.	Functional	Intersects With	Automated System Account Management (Directory Services)	IAC-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
AC-2(CE-2)	Removal of Temporary and Emergency Accounts	Automatically disable and remove temporary and emergency accounts after two (2) business days.	Functional	Subset Of	Removal of Temporary / Emergency Accounts	IAC-15.2	Automated mechanisms exist to disable or remove temporary and emergency accounts after an organization-defined time period for each type of account.	10	
AC-2(CE-3)	Disable Accounts	Disable accounts within 120 days when the accounts:	Functional	Subset Of	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	10	
AC-2(CE-3).a	Disable Accounts	Have expired;	Functional	Subset Of	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	10	
AC-2(CE-3).b	Disable Accounts	Are no longer associated to a user or individual;	Functional	Subset Of	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	10	
AC-2(CE-3).c	Disable Accounts	Are in violation of organizational policy; or	Functional	Subset Of	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
AC-2(CE-3).d	Disable Accounts	Have been inactive for 120 days for non-privileged accounts and 60 days for privileged accounts	Functional	Subset Of	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	10	
AC-2(CE-4)	Automated Audit Actions	Automatically audit account creation, modification, enabling, disabling and removal actions.	Functional	Subset Of	Automated Audit Actions	IAC-15.4	Automated mechanisms exist to audit account creation, modification, enabling, disabling and removal actions and notify organization-defined personnel or roles.	10	
AC-2(CE-7)	Privileged User Accounts:	N/A	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
AC-2(CE-7).a	Privileged User Accounts:	Establish and administer privileged user accounts in accordance with a role-based access scheme; an attribute-based access scheme	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
AC-2(CE-7).b	Privileged User Accounts:	Monitor privileged role or attribute assignments;	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
AC-2(CE-7).c	Privileged User Accounts:	Monitor changes to roles or attributes; and	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
AC-2(CE-7).d	Privileged User Accounts:	Revoke access when privileged role or attribute assignments are no longer appropriate.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
AC-2(CE-9)	Restrictions on Use of Shared and Group Accounts	Only permit the use of shared and group accounts that meet agency-defined conditions for establishing shared and group accounts. Supplemental Guidance: Before permitting the use of shared or group accounts, organizations consider the increased risk due to the lack of accountability with such accounts. This includes service accounts that can be used for computer logon by a user (e.g., interactive logon is not disabled).	Functional	Subset Of	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	10	
AC-2(CE-12)	Account Monitoring for Atypical Usage:	Supplemental Guidance: Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals.	Functional	Subset Of	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	10	
AC-2(CE-12).a	Account Monitoring for Atypical Usage:	Monitor system accounts for agency-defined atypical usage; and	Functional	Subset Of	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	10	
AC-2(CE-12).b	Account Monitoring for Atypical Usage:	Report atypical usage of system accounts to agency-defined personnel or roles.	Functional	Subset Of	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	10	
AC-2(CE-13)	Disable Accounts for High-Risk Individual	Disable accounts of users posing a significant risk within one (1) day of discovery of the risk. Supplemental Guidance: Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm. Such harm includes the potential adverse impacts to organizational operations and assets, individuals, other organizations, the state, or the Nation. Close coordination and cooperation among authorizing officials, system administrators and human resource managers is essential for timely execution of this control enhancement.	Functional	Intersects With	High-Risk Terminations	HRS-09.2	Mechanisms exist to expedite the process of removing "high risk" individual's access to Technology Assets, Applications, Services and/or Data (TAASD) upon termination, as determined by management.	5	
AC-2(CE-13)	Disable Accounts for High-Risk Individual	Disable accounts of users posing a significant risk within one (1) day of discovery of the risk. Supplemental Guidance: Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm. Such harm includes the potential adverse impacts to organizational operations and assets, individuals, other organizations, the state, or the Nation. Close coordination and cooperation among authorizing officials, system administrators and human resource managers is essential for timely execution of this control enhancement.	Functional	Intersects With	Account Disabling for High Risk Individuals	IAC-15.6	Mechanisms exist to disable accounts immediately upon notification for users posing a significant risk to the organization.	5	
AC-3	Access Enforcement	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
AC-3	Access Enforcement	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
AC-3	Access Enforcement	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
AC-3(CE-9)	Controlled Release	Release information outside of the system only if:	Functional	Subset Of	Controlled Release	DCH-03.3	Automated mechanisms exist to validate cybersecurity and data protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).	10	
AC-3(CE-9).a	Controlled Release	The receiving system accessing, processing, storing, or transmitting FTI provides Publication 1075 required protections; and	Functional	Subset Of	Controlled Release	DCH-03.3	Automated mechanisms exist to validate cybersecurity and data protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).	10	
AC-3(CE-9).b	Controlled Release	Agency-defined controls, Publication 1075 requirements, FedRAMP ATO are used to validate the appropriateness of the information designated for release.	Functional	Subset Of	Controlled Release	DCH-03.3	Automated mechanisms exist to validate cybersecurity and data protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).	10	
AC-3(CE-11)	Restrict Access to Specific Information Types	Restrict access to data repositories containing Federal Tax Information.	Functional	Subset Of	Sensitive / Regulated Data Access Enforcement	CFG-08	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to restrict access to sensitive/regulated data.	10	
AC-4	Information Flow Enforcement	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	10	
AC-5	Separation of Duties	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
AC-5	Separation of Duties	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Dual Authorization for Change	CHG-04.3	Mechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or Services (TAAS).	5	
AC-5	Separation of Duties	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
AC-5	Separation of Duties	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	
AC-6	Least Privilege	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
AC-6	Least Privilege	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
AC-6(CE-1)	Authorize Access to Security Functions	Authorize Access for Security Functions to:	Functional	Subset Of	Authorize Access to Security Functions	IAC-21.1	Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.	10	
AC-6(CE-1).a	Authorize Access to Security Functions	Explicitly authorize access to security functions deployed in hardware, software, and firmware; and	Functional	Subset Of	Authorize Access to Security Functions	IAC-21.1	Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.	10	
AC-6(CE-1).b	Authorize Access to Security Functions	Security-relevant information.	Functional	Subset Of	Authorize Access to Security Functions	IAC-21.1	Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.	10	
AC-6(CE-2)	Non-Privileged Access for Nonsecurity Functions	Require that users of system accounts or roles with access to security functions including but 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 nonsecurity functions.	Functional	Subset Of	Non-Privileged Access for Non-Security Functions	IAC-21.2	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.	10	
AC-6(IRS-Defined)-1	N/A	Prohibit accounts with administrative privileges (including local administrator rights) from web browsing and other Internet connections outside of the local protected boundary unless such risk is accepted in writing by the agency's CISO.	Functional	Subset Of	Non-Privileged Access for Non-Security Functions	IAC-21.2	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.	10	
AC-6(IRS-Defined)-2	N/A	Block accounts with administrative privileges (including local administrator rights) from access to email unless such risk is accepted in writing by the agency's CISO.	Functional	Subset Of	Non-Privileged Access for Non-Security Functions	IAC-21.2	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.	10	
AC-6(CE-6)	Privileged Access by Non-Organizational Users	Prohibit privileged access to the system by nonorganizational users.	Functional	Subset Of	Privileged Access by Non-Organizational Users	IAC-05.2	Mechanisms exist to prohibit privileged access by non-organizational users.	10	
AC-6(CE-7)	Review of User Privileges	N/A	Functional	Subset Of	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	10	
AC-6(CE-7).a	Review of User Privileges	Review annually the privileges assigned to FTI to validate the need for such privileges; and	Functional	Subset Of	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	10	
AC-6(CE-7).b	Review of User Privileges	Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.	Functional	Subset Of	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	10	
AC-6(CE-8)	Privilege Levels for Code Execution	Prevent the following software from executing at higher privilege levels than users executing the software: agency-defined software. Supplemental Guidance: This item should be tracked on the agency's POA&M.	Functional	Subset Of	Privilege Levels for Code Execution	IAC-21.7	Automated mechanisms exist to prevent applications from executing at higher privilege levels than the user's privileges.	10	
AC-6(CE-9)	Auditing Use of Privileged Functions	Audit the execution of privileged functions.	Functional	Subset Of	Auditing Use of Privileged Functions	IAC-21.4	Mechanisms exist to audit the execution of privileged functions.	10	
AC-6(CE-10)	Prohibit Non-privileged Users from Executing Privileged Functions	Prevent non-privileged users from executing privileged functions. Supplemental Guidance: If individuals with administrator rights require email 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 agency assets receiving, processing, storing, accessing, protecting and/or transmitting FTI. Supplemental Guidance: If individuals with administrator rights require email 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 agency assets storing, processing, transmitting, or protecting FTI.	Functional	Subset Of	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-21.5	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.	10	
AC-7	Unsuccessful Logon Attempts	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	10	
AC-7(CE-2)	Purge or Wipe Mobile Device	Purge or wipe information from mobile devices based on agencydefined purging or wiping requirements and techniques after ten (10) consecutive, unsuccessful device logon attempts. Supplemental Guidance: This control enhancement applies only to mobile devices for which a logon occurs. The logon is to the mobile device, not to any one account on the device. Successful logons to accounts on mobile devices reset the unsuccessful logon count to zero. Purging or wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms.	Functional	Subset Of	Remote Purging	MDM-05	Mechanisms exist to remotely purge selected information from mobile devices.	10	
AC-8	System Use Notification	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	System Use Notification (Logon Banner)	SEA-18	Mechanisms exist to utilize system use notification / logon banners that display an approved system use notification message or banner before granting access to Technology Assets, Applications and/or Services (TAAS)	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
AC-11	Device Lock	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Session Lock	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	5	
AC-11(CE-1)	Pattern-Hiding Displays	Conceal, via the device lock, information previously visible on the display with a publicly viewable image. Supplemental Guidance: The pattern-hiding display can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator or a blank screen, with the caveat that controlled unclassified information is not displayed.	Functional	Subset Of	Pattern-Hiding Displays	IAC-24.1	Mechanisms exist to implement pattern-hiding displays to conceal information previously visible on the display during the session lock.	10	
AC-12	Session Termination	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Session Termination	IAC-25	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	10	
AC-12(CE-1)	User-Initiated Logouts	Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to systems accessing, processing, storing, or transmitting FTI.	Functional	Subset Of	User-Initiated Logouts / Message Displays	IAC-25.1	Mechanisms exist to provide a logout capability and display an explicit logout message to users indicating the reliable termination of the session.	10	
AC-14	Permitted Actions Without Identification or Authentication	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Permitted Actions Without Identification or Authorization	IAC-26	Mechanisms exist to identify and document the supporting rationale for specific user actions that can be performed on a system without identification or authentication.	10	
AC-17	Remote Access	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
AC-17(CE-1)	Monitoring and Control	Employ automated mechanisms to monitor and control remote access methods.	Functional	Subset Of	Automated Monitoring & Control	NET-14.1	Automated mechanisms exist to monitor and control remote access sessions.	10	
AC-17(CE-2)	Protection of Confidentiality and Integrity Using Encryption	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	Functional	Subset Of	Protection of Confidentiality / Integrity Using Encryption	NET-14.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	10	
AC-17(CE-3)	Managed Access Control Points	Route remote accesses through authorized and managed network access control points.	Functional	Subset Of	Managed Access Control Points	NET-14.3	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	10	
AC-17(CE-4)	Privileged Commands and Access	Supplemental Guidance: Rationale must be documented in agency's SSR as it relates to the FTI environment.	Functional	Subset Of	Remote Privileged Commands & Sensitive Data Access	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.	10	
AC-17(CE-4).a	Privileged Commands and Access	Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: compelling operational needs defined by the agency; and	Functional	Subset Of	Remote Privileged Commands & Sensitive Data Access	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.	10	
AC-17(CE-4).b	Privileged Commands and Access	Document the rationale for remote access in the security plan for the system.	Functional	Subset Of	Remote Privileged Commands & Sensitive Data Access	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.	10	
AC-17(CE-9)	Disconnect or Disable Access	Provide the capability to disconnect or disable remote access to the system within agency-defined time period.	Functional	Subset Of	Expeditious Disconnect / Disable Capability	NET-14.8	Mechanisms exist to provide the capability to expeditiously disconnect or disable a user's remote access session.	10	
AC-18	Wireless Access	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
AC-18(CE-1)	Authentication and Encryption	Protect wireless access to the system using authentication of both users and devices and encryption.	Functional	Subset Of	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by:(1) Authenticating devices trying to connect; and(2) Encrypting transmitted data.	10	
AC-18(CE-3)	Disable Wireless Networking	Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment. Supplemental Guidance: Disable (through automated means, where technically possible) unapproved wireless networking capabilities of desktops, laptops, printers, copiers, fax machines, SCADA systems and other devices; and monitor through automated means for unauthorized changes. One alternative yet acceptable approach to "monitoring through automated means" is regularly pushing out settings that restrict unapproved wireless connections.	Functional	Subset Of	Disable Wireless Networking	NET-15.2	Mechanisms exist to disable unnecessary wireless networking capabilities that are internally embedded within system components prior to issuance to end users.	10	
AC-18(IRS-Defined)-1	N/A	Guest wireless networks operated by or on behalf of the agency, data center or vendor managed facilities must be completely logically separate from all other secured internal networks.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
AC-18(IRS-Defined)-2	N/A	Monitor for unauthorized wireless access to the information system and enforce requirements for wireless connections to the information system.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
AC-18(IRS-Defined)-3	N/A	Employ security mechanisms for wireless networks consistent with the sensitivity of the information to be transmitted. FIPS 140 validated encryption must be employed in all wireless networks used to access FTI and/or manage an FTI environment.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
AC-18(IRS-Defined)-4	N/A	Perform both attack monitoring and vulnerability monitoring on the wireless network to support WLAN security. Additional requirements for protecting FTI on wireless networks are provided in Section 3.3.6, Network Boundary and Infrastructure.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
AC-19	Access Control for Mobile Devices	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Access Control For Mobile Devices	MDM-02	Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	10	
AC-19(CE-5)	Full Device and Container-Based Encryption	Employ full-device encryption using the latest FIPS 140 validated encryption on areas where FTI resides to protect the confidentiality and integrity of information on agency-owned mobile devices and mobile devices that are part of a BYOD implementation. POA&M findings must be documented and tracked when no such encryption technology solutions are available to address a specific device. Additional requirements on protecting FTI accessed by mobile devices are provided in Section 3.3.4, Mobile Devices, Section 2.C.7, Offshore Operations and on the Office of Safeguards website.	Functional	Subset Of	Full Device & Container-Based Encryption	MDM-03	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	10	
AC-20	Use of External Systems	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	10	
AC-20(CE-2)	Portable Storage Devices - Restricted Use	Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using organizational-defined policy.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
AC-20(CE-3)	Non-Organizationally Owned Systems and Components - Restricted Use	Restrict the use of nonorganizationally owned systems or system components to process, store, or transmit organizational information using Publication 1075 requirements. Supplemental Guidance: The IRS Office of Safeguards allows connections from external information systems only in the event the agency has configured a virtual desktop infrastructure (VDI) solution to receive, secure and manage remote connections.	Functional	Subset Of	Non-Organizationally Owned Technology Assets, Applications and/or Services (TAAS)	DCH-13.4	Mechanisms exist to restrict the use of non-organizationally owned Technology Assets, Applications and/or Services (TAAS) to process, store or transmit organizational information.	10	
AC-20(IRS-Defined)	N/A	Approval by the agency CISO is required for connection of non-government furnished or contractor-owned IT devices (including USB-connected portable storage and mobile devices) to agencyowned systems or networks receiving, processing, storing, accessing, protecting and/or transmitting FTI. This requirement does not apply to networks and systems intended for use by the general public. Additional VDI requirements are provided in Section 3.3.7, Virtual Desktop Infrastructure and on the Office of Safeguards website.	Functional	Subset Of	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	10	
AC-20(CE-5)	Portable Storage Devices - Prohibited Use	Prohibit the use of organization-controlled portable storage devices by authorized individuals on external systems.	Functional	Subset Of	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	10	
AC-21	Information Sharing	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	5	
AC-21	Information Sharing	\	Functional	Intersects With	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5	
AC-22	Publicly Accessible Content	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	10	
AC-23	Data Mining Protection	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Data Mining Protection	DCH-16	Mechanisms exist to protect data storage objects against unauthorized data mining and data harvesting techniques.	5	
4.2	AWARENESS AND TRAINING	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AT-1	Awareness and Training Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
AT-1	Awareness and Training Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
AT-1	Awareness and Training Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
AT-2	Awareness Training	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
AT-2(CE-1)	Practical Exercises	Provide practical exercises in literacy training that simulate events and incidents. Supplemental Guidance: Practical exercises may include, for example, no-notice social engineering attempts to collect information, gain unauthorized access or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links. Privacy-related practical exercises may include, for example, practice modules with quizzes on handling personally identifiable information and affected individuals in various scenarios.	Functional	Intersects With	Simulated Cyber Attack Scenario Training	SAT-02.1	Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.	5	
AT-2(CE-2)	Insider Threat	Provide literacy training on recognizing and reporting potential indicators of insider threat. Supplemental Guidance: Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence and other serious violations of organizational policies, procedures, directives, rules or practices. Security and privacy awareness training includes how to communicate the concerns of employees and management regarding potential indicators of insider threat through organizational channels in accordance with established policies and procedures.	Functional	Subset Of	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
AT-2(CE-3)	Social Engineering and Mining	Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining. Supplemental Guidance: Social engineering is an attempt to trick someone into revealing information or taking an action that can be used to attack or compromise systems. Examples of social engineering include phishing, pretexting, baiting, quid pro quo, and tailgating. Social mining is an attempt, in a social setting, to gather information about the organization that may support future attacks. Security and privacy awareness training includes information on how to communicate concerns of employees and management regarding potential and actual instances of social engineering and mining through organizational channels based on established policies and procedures. Treasury Directive: Train users and provide means to ensure workstations are adequately protected from theft, particularly regarding laptops acting as workstations.	Functional	Subset Of	Social Engineering & Mining	SAT-02.2	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.	10	
AT-2(IRS-Defined)-1	N/A	Distribute security and privacy awareness reminders/updates to all users on at least a quarterly basis. Supplemental Guidance: This is in addition to annual awareness training. Security awareness updates may be sent via email. Unlike the need to track annual training by individual, agencies are not required to track quarterly awareness updates by individual.	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
AT-2(IRS-Defined)-2	N/A	Conduct phishing email simulation exercises on at least a quarterly basis.	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
AT-2(CE-4)	Suspicious Communications and Anomalous System Behavior	Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using agency-defined indicators of malicious code	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	
AT-3	Role-Based Training	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	5	
AT-4	Training Records	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Security, Compliance & Resilience Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including:(1) Initial security, compliance and resilience awareness training;(2) Recurring awareness training; and(3) Technology Assets, Applications and/or Services (TAAS)-specific training.	10	
AT-6	Training Feedback	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Simulated Cyber Attack Scenario Training	SAT-02.1	Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.	5	
4.3	AUDIT AND ACCOUNTABILITY	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AU-1	Audit and Accountability Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
AU-1	Audit and Accountability Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
AU-1	Audit and Accountability Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
AU-2	Audit Events	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
AU-2	Audit Events	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
AU-3	Content of Audit Records	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:(1) Establish what type of event occurred;(2) When (date and time) the event occurred;(3) Where the event occurred;(4) The source of the event;(5) The outcome (success or failure) of the event; and(6) The identity of any user/subject associated with the event.	10	
AU-3(CE-1)	Additional Audit Information	Generate audit records containing the following additional information:	Functional	Intersects With	Sensitive Event Log Information	MON-03.1	Mechanisms exist to protect sensitive/regulated data contained in log files.	5	
AU-3(CE-1)	Additional Audit Information	Details that facilitate the reconstruction of events if	Functional	Intersects With	Sensitive Event Log Information	MON-03.1	Mechanisms exist to protect sensitive/regulated data contained in log files.	5	
AU-3(CE-1)	Additional Audit Information	Unauthorized activity occurs or is suspected; or	Functional	Intersects With	Sensitive Event Log Information	MON-03.1	Mechanisms exist to protect sensitive/regulated data contained in log files.	5	
AU-3(CE-1)	Additional Audit Information	A malfunction occurs or is suspected.	Functional	Intersects With	Sensitive Event Log Information	MON-03.1	Mechanisms exist to protect sensitive/regulated data contained in log files.	5	
AU-3(CE-3)	Limit Personally Identifiable Information Elements	Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: agencydefined elements.	Functional	Subset Of	Limit Personal Data (PD) In Audit Records	MON-03.5	Mechanisms exist to limit Personal Data (PD) contained in audit records to the elements identified in the Data Privacy Risk Assessment (DPRA).	10	
AU-4	Audit Storage Capacity	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Event Log Storage Capacity	MON-04	Mechanisms exist to allocate and proactively manage sufficient event log storage capacity to reduce the likelihood of such capacity being exceeded.	10	
AU-5	Response to Audit Processing Failures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Response To Event Log Processing Failures	MON-05	Mechanisms exist to alert appropriate personnel in the event of a log processing failure and take actions to remedy the disruption.	10	
AU-5(CE-1)	Storage Warning Capacity	Provide a warning to the SA and ISSO within 24 hours when allocated audit logs storage volume reaches a specified percentage of repository maximum audit log storage capacity.	Functional	Subset Of	Event Log Storage Capacity Alerting	MON-05.2	Automated mechanisms exist to alert appropriate personnel when the allocated volume reaches an organization-defined percentage of maximum event log storage capacity.	10	
AU-6	Audit Review, Analysis and Reporting	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
AU-6	Audit Review, Analysis and Reporting	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Audit Level Adjustments	MON-02.6	Mechanisms exist to adjust the level of audit review, analysis and reporting based on evolving threat information from law enforcement, industry associations or other credible sources of threat intelligence.	5	
AU-6(CE-1)	Automated Process Integration	Integrate audit record review, analysis, and reporting processes using automated mechanisms to support organizational processes for investigation and response to suspicious activities.	Functional	Intersects With	Sensitive Event Log Information	MON-03.1	Mechanisms exist to protect sensitive/regulated data contained in log files.	5	
AU-6(CE-3)	Correlate Audit Repositories	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
AU-6(CE-7)	Permitted Actions	Specify the permitted actions for each role or user associated with the review, analysis, and reporting of audit record information.	Functional	Subset Of	Permitted Actions	MON-02.5	Mechanisms exist to specify the permitted actions for both users and Technology Assets, Applications and/or Services (TAAS) associated with the review, analysis and reporting of audit information.	10	
AU-6(CE-9)	Correlation with Information from Nontechnical Sources	Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness. Supplemental Guidance: Nontechnical sources include records that document organizational policy violations related to harassment incidents and the improper use of information assets. Such information can lead to a directed analytical effort to detect potential malicious insider activity. Organizations limit access to information that is available from nontechnical sources due to its sensitive nature. Limited access minimizes the potential for inadvertent release of privacy-related information to individuals who do not have a need to know. The correlation of information from nontechnical sources with audit record information generally occurs only when individuals are suspected of being involved in an incident. Organizations obtain legal advice prior to initiating such actions.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
AU-7	Audit Reduction and Report Generation	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5	
AU-7(CE-1)	Automatic Processing	Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: likelihood of potential inappropriate access or unauthorized disclosure of FTI. Supplemental Guidance: Events of interest is the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed.	Functional	Intersects With	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5	
AU-8	Time Stamps	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	5	
AU-8	Time Stamps	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Time Stamps	MON-07	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs.	5	
AU-9	Protection of Audit	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	10	
AU-9(CE-4)	Access by Subset of Privileged Users	Authorize access to management of audit logging functionality to only authorized system administrators.	Functional	Subset Of	Access by Subset of Privileged Users	MON-08.2	Mechanisms exist to restrict access to the management of event logs to privileged users with a specific business need.	10	
AU-11	Audit Record Retention	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	10	
AU-12	Audit Generation	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5	
AU-12(CE-1)	System-Wide and Time-Correlated Audit Trail	Compile audit records from systems that receive, process, store, access, protect and/or transmit FTI into a system-wide logical audit trail that is timecorrelated to within agency-defined level of tolerance for the relationship between time stamps of individual records in the audit trail.	Functional	Subset Of	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	10	
AU-16	Cross-Organizational Auditing Logging	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Cross-Organizational Monitoring	MON-14	Mechanisms exist to coordinate sanitized event logs among external organizations to identify anomalous events when event logs are shared across organizational boundaries, without giving away sensitive or critical business data.	5	
AU-16(CE-1)	Identity Preservation	Preserve the identity of individuals in cross-organizational audit trails.	Functional	Intersects With	Cross-Organizational Monitoring	MON-14	Mechanisms exist to coordinate sanitized event logs among external organizations to identify anomalous events when event logs are shared across organizational boundaries, without giving away sensitive or critical business data.	5	
AU-16(CE-2)	Sharing of Audit Information	Provide cross-organizational audit information to agency-defined organizations based on agency-defined cross-organizational sharing agreements.	Functional	Subset Of	Sharing of Event Logs	MON-14.1	Mechanisms exist to share event logs with third-party organizations based on specific cross-organizational sharing agreements.	10	
4.4	ASSESSMENT, AUTHORIZATION AND MONITORING	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CA-1	Assessment, Authorization and Monitoring Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
CA-1	Assessment, Authorization and Monitoring Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
CA-1	Assessment, Authorization and Monitoring Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
CA-2	Control Assessments	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
CA-2	Control Assessments	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	5	
CA-2	Control Assessments	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
CA-2	Control Assessments	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
CA-2	Control Assessments	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
CA-2(CE-1)	Independent Assessors	Employ independent assessors or assessment teams to conduct control assessments. Supplemental Guidance: Independent assessors or assessment teams are individuals or groups conducting impartial assessments of systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest regarding development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors should not create a mutual or conflicting interest with the agencies where the assessments are being conducted; assess their own work; act as management or employees of the agencies they are serving; or place themselves in positions of advocacy for the agencies acquiring their services. Independent assessments can be obtained from elements within agencies (e.g., internal audit departments, security offices, etc.) or can be contracted to public or private sector entities outside of the agency	Functional	Subset Of	Assessor Independence	IAO-02.1	Mechanisms exist to ensure assessors or assessment teams have the appropriate independence to conduct security, compliance and/or resilience control assessments.	10	
CA-3	Information Exchange	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection:(1) Interface characteristics;(2) Security, compliance and resilience requirements; and;(3) The nature of the information communicated.	5	
CA-5	Plan of Action and Milestones	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner);(8) Resources required to conduct remediation actions;(9) Planned remedial actions to the	5	
CA-5(IRS-Defined)-1	N/A	Agencies must ensure that the individual and/or office responsible for correcting each weakness is identified in the appropriate POA&M.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner);(8) Resources required to conduct remediation actions;(9) Planned remedial actions to the	5	
CA-5(IRS-Defined)-2	N/A	Agencies must enter all new weaknesses into appropriate POA&Ms within two (2) months for weaknesses identified during assessments. Supplemental Guidance: The results of scans/automated testing can be added to POA&Ms as multiple items or one finding per weakness for like systems. Additional information is available in Section 2.D.9, Plan of Action and Milestones.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	Milestones (POA&M) or similar methodology) that formally documents, at a minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner);(8) Resources required to conduct remediation actions;(9) Planned remedial actions to the deficiency(ies);(10) Proposed remediation timeline; and(11) Disposition	5	
CA-6	Authorization	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	10	
CA-7	Continuous Monitoring	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
CA-7(CE-1)	Independent Assessors	Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis. Supplemental Guidance: Agencies can maximize the value of control assessments during the continuous monitoring process by requiring that assessments be conducted by assessors with appropriate levels of independence. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not create a mutual or conflicting interest with the agencies where the assessments are being conducted; assess their own work; act as management or employees of the agencies they are serving; or place themselves in advocacy positions for the agencies acquiring their services. Independent assessments can be obtained from elements within agencies (e.g., internal audit departments, security offices, etc.) or can be contracted to public or private sector entities outside of the agency.	Functional	Intersects With	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	5	
CA-7(CE-4)	Risk Monitoring	Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:	Functional	Subset Of	Risk Monitoring	RSK-11	Mechanisms exist to ensure risk monitoring as an integral part of the continuous monitoring strategy that includes monitoring the effectiveness of security, compliance and resilience controls, compliance and change management.	10	
CA-7(CE-4).a	Risk Monitoring	Effectiveness monitoring;	Functional	Subset Of	Risk Monitoring	RSK-11	Mechanisms exist to ensure risk monitoring as an integral part of the continuous monitoring strategy that includes monitoring the effectiveness of security, compliance and resilience controls, compliance and change management.	10	
CA-7(CE-4).b	Risk Monitoring	Compliance monitoring; and	Functional	Subset Of	Risk Monitoring	RSK-11	Mechanisms exist to ensure risk monitoring as an integral part of the continuous monitoring strategy that includes monitoring the effectiveness of security, compliance and resilience controls, compliance and change management.	10	
CA-7(CE-4).c	Risk Monitoring	Change monitoring.	Functional	Subset Of	Risk Monitoring	RSK-11	Mechanisms exist to ensure risk monitoring as an integral part of the continuous monitoring strategy that includes monitoring the effectiveness of security, compliance and resilience controls, compliance and change management.	10	
CA-8	Penetration Testing	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	10	
CA-9	Internal System Connections	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Internal System Connections	NET-05.2	Mechanisms exist to control internal system connections through authorizing internal connections of systems and documenting, for each internal connection, the interface characteristics, security requirements and the nature of the information communicated.	10	
CA-9(CE-1)	Compliance Checks	Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.	Functional	Subset Of	Endpoint Security Validation	NET-14.7	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions, patch levels, etc.) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).	10	
4.5	CONFIGURATION MANAGEMENT	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CM-1	Configuration Management Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
CM-1	Configuration Management Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
CM-1	Configuration Management Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
CM-2	Baseline Configuration	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations:(1) At least annually;(2) When required due to so; or(3) As part of system component installations and upgrades.	5	
CM-2	Baseline Configuration	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
CM-2(CE-2)	Automation Support for Accuracy and Currency	Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using automated mechanisms. Supplemental Guidance: Automated mechanisms that help agencies maintain consistent baseline configurations for systems include, for example, hardware and software inventory tools, configuration management tools and network management tools. Such tools can be deployed and/or allocated at the system level, or at the operating system or component level including, for example, on workstations, servers, notebook computers, network components or mobile devices. Tools can be used, for example, to track version numbers on operating systems, applications, types of software installed and current patch levels.	Functional	Subset Of	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	10	
CM-2(CE-3)	Retention of Previous Configurations	Retain older versions of baseline configurations of the system to support rollback.	Functional	Subset Of	Retention Of Previous Configurations	CFG-02.3	Mechanisms exist to retain previous versions of baseline configuration to support roll back.	10	
CM-2(IRS-Defined)	N/A	Agencies must use SCSEMs provided on the Office of Safeguards website to ensure secure configurations of all agency information technology and communication systems receiving, processing, storing, accessing, protecting and/or transmitting FTI.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations:(1) At least annually;(2) When required due to so; or(3) As part of system component installations and upgrades.	5	
CM-2(IRS-Defined)	N/A	Agencies must use SCSEMs provided on the Office of Safeguards website to ensure secure configurations of all agency information technology and communication systems receiving, processing, storing, accessing, protecting and/or transmitting FTI.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
CM-2(CE-7)	Configure Systems and Components for High-Risk Areas	Supplemental Guidance: When it is known that systems or system components will be in high-risk areas external to the organization, additional controls may be implemented to counter the increased threat in such areas. For example, organizations can take actions for notebook computers used by individuals departing on and returning from travel that may include international stops or layovers. Actions include determining the locations that are of concern, defining the required configurations for the components, ensuring that components are configured as intended before travel is initiated, and applying controls to the components after travel is completed. Specially configured notebook computers include computers with sanitized hard drives, limited applications, minimum sensitive data (e.g., FTI), and more stringent configuration settings. Controls applied to mobile devices upon return from travel include examining the mobile device for signs of physical tampering and purging and reimaging disk drives. Protecting information that resides on mobile devices is addressed in the MP (Media Protection) family.	Functional	Subset Of	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	10	
CM-2(CE-7).a	Configure Systems and Components for High-Risk Areas	Issue a specifically configured computing device with more stringent configuration settings and the minimum-needed access to FTI to individuals traveling to locations that are deemed to be of significant risk; and	Functional	Subset Of	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	10	
CM-2(CE-7).b	Configure Systems and Components for High-Risk Areas	Apply the following controls to the systems or components when the individuals return from travel: examine for signs of tampering, reformat storage media before reintroduction to the FTI. Environment	Functional	Subset Of	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	10	
CM-3	Configuration Change Control	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
CM-3	Configuration Change Control	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
CM-3(CE-2)	Testing, Validation and Documentation of Changes	Test, validate, and document changes to the system before finalizing the implementation of the changes.	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	5	
CM-3(CE-4)	Security and Privacy Representative	Require ISSO/ISSM and Privacy Representatives to be members of the Configuration Control Board. Supplemental Guidance: Information security representatives can include, for example, Senior Agency Information Security Officers, system security officers or system security managers. Representation by personnel with information security expertise is important because changes to system configurations can have unintended side effects, some of which may be security-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security state of organizational systems.	Functional	Subset Of	Security, Compliance & Resilience Representative for Asset Lifecycle Changes	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data protection representative in the configuration change control review process.	10	
CM-4	Security and Privacy Impact Analyses	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	10	
CM-4(CE-2)	Verification of Controls	After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.	Functional	Subset Of	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	10	
CM-5	Access Restrictions for Change	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
CM-5(CE-5)	Privilege Limitation for Production and Operations	N/A	Functional	Subset Of	Permissions To Implement Changes	CHG-04.4	Mechanisms exist to limit operational privileges for implementing changes.	10	
CM-5(CE-5).a	Privilege Limitation for Production and Operations	Limit privileges to change system components and system-related information within a production or operational environment; and	Functional	Subset Of	Permissions To Implement Changes	CHG-04.4	Mechanisms exist to limit operational privileges for implementing changes.	10	
CM-5(CE-5).b	Privilege Limitation for Production and Operations	Review and reevaluate privileges semi-annually.	Functional	Subset Of	Permissions To Implement Changes	CHG-04.4	Mechanisms exist to limit operational privileges for implementing changes.	10	
CM-5(IRS-Defined)-1	N/A	Restrict administration of configurations to only authorized administrators.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
CM-5(IRS-Defined)-2	N/A	Verify the authenticity and integrity of Basic Input/Output System (BIOS) or Unified Extensible Firmware Interface (UEFI) updates to ensure that the BIOS or UEFI is protected from modification outside of the secure update process. Supplemental Guidance: Inventory of BIOS or UEFI information should be incorporated into existing inventory control systems, where feasible. Most agencies will rely upon the manufacturer as the source for the authenticated BIOS or UEFI. System BIOS or UEFI updates should be performed using a secure authenticated update process. After BIOS or UEFI updates, the configuration baseline should be validated to confirm that the computer system is still in compliance with the agency's defined policy. The BIOS or UEFI image and configuration baseline should be continuously monitored and deviations from the baseline should be investigated, documented, and remediated as part of incident response activities.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
CM-6	Configuration Settings	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
CM-6	Configuration Settings	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	5	
CM-6(IRS-Defined)	N/A	The agency shall ensure that all devices across the enterprise that store agency data are appropriately reviewed for security purposes prior to connection or reconnection to the agency's network, (e.g. checks for malicious code, updates to malware detection software, critical software updates and patches, operating system integrity and disabled hardware).	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
CM-6(IRS-Defined)	N/A	The agency shall ensure that all devices across the enterprise that store agency data are appropriately reviewed for security purposes prior to connection or reconnection to the agency's network, (e.g. checks for malicious code, updates to malware detection software, critical software updates and patches, operating system integrity and disabled hardware).	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	5	
CM-7	Least Functionality	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	10	
CM-7(CE-1)	Periodic Review	N/A	Functional	Subset Of	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	10	
CM-7(CE-1).a	Periodic Review	Review the system annually to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and	Functional	Subset Of	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	10	
CM-7(CE-1).b	Periodic Review	Disable or remove identified functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure.	Functional	Subset Of	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	10	
CM-7(CE-5)	Authorized Software – Allow By Exception	N/A	Functional	Subset Of	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	10	
CM-7(CE-5).a	Authorized Software – Allow By Exception	Identify software programs authorized to execute on the system;	Functional	Subset Of	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	10	
CM-7(CE-5).b	Authorized Software – Allow By Exception	Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and	Functional	Subset Of	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	10	
CM-7(CE-5).c	Authorized Software – Allow By Exception	Review and update the list of authorized software programs at a minimum annually.	Functional	Subset Of	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	10	
CM-7(IRS-Defined)	N/A	Periodically scan FTI networks to detect and remove any unauthorized or unlicensed software.	Functional	Subset Of	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	10	
CM-7(CE-9)	Prohibiting the Use of Unauthorized Hardware	N/A	Functional	Subset Of	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	10	
CM-7(CE-9).a	Prohibiting the Use of Unauthorized Hardware	Identify agency-defined hardware components authorized for system use;	Functional	Subset Of	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	10	
CM-7(CE-9).b	Prohibiting the Use of Unauthorized Hardware	Prohibit the use or connection of unauthorized hardware components;	Functional	Subset Of	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	10	
CM-7(CE-9).c	Prohibiting the Use of Unauthorized Hardware	Review and update the list of authorized hardware components annually.	Functional	Subset Of	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	10	
CM-8	System Component Inventory	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Component Duplication Avoidance	AST-02.3	Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components that prevents assets from being duplicated in other asset inventories.	5	
CM-8(CE-1)	Updates During Installation and Removal	Update the inventory of system components as part of component installations, removals, and system updates.	Functional	Subset Of	Updates During Installations / Removals	AST-02.1	Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.	10	
CM-8(CE-3)	Automated Unauthorized Component Detection	Supplemental Guidance: This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within systems or in other separate devices. Isolation can be achieved, for example, by placing unauthorized system components in separate domains or subnets or otherwise quarantining such components. This type of component isolation is commonly referred to as sandboxing.	Functional	Subset Of	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.	10	
CM-8(CE-3).a	Automated Unauthorized Component Detection	Detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms at all times; and	Functional	Subset Of	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.	10	
CM-8(CE-3).b	Automated Unauthorized Component Detection	Take the following actions when unauthorized components are detected:	Functional	Subset Of	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.	10	
CM-8(CE-3).b.1	Automated Unauthorized Component Detection	Disable network access by such components.	Functional	Subset Of	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.	10	
CM-8(CE-3).b.2	Automated Unauthorized Component Detection	Isolate the components.	Functional	Subset Of	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
CM-8(CE-3).b.3	Automated Unauthorized Component Detection	Notify designated Agency IT personnel	Functional	Subset Of	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.	10	
CM-9	Configuration Management Plan	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
CM-9	Configuration Management Plan	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5	
CM-10	Software Usage Restrictions	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Software Usage Restrictions	CFG-04	Mechanisms exist to enforce software usage restrictions to comply with applicable contract agreements and copyright laws.	10	
CM-11	User-Installed Software	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5	
CM-11	User-Installed Software	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	
CM-12	Information Location	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Information Location	DCH-24	Mechanisms exist to identify and document the location of information and the specific system components on which the information resides.	10	
CM-12(CE-1)	Automated Tools to Support Information Location	Use automated tools to identify FTI on system components to ensure controls are in place to protect organizational information and individual privacy. Supplemental Guidance: This control enhancement gives agencies the capability to check systems and selected system components for FTI to confirm such information resides on the component and to ensure that the required protection measures are in place for that component. Include all FTI systems and system components in the agency's FTI inventory. See NIST Control PM-29, Inventory of Personally Identifiable Information.	Functional	Subset Of	Information Location	DCH-24	Mechanisms exist to identify and document the location of information and the specific system components on which the information resides.	10	
CM-13	Data Action Mapping	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive/regulated data is stored, transmitted or processed.	10	
CM-14	Signed Components	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Signed Components	CHG-04.2	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.	5	
4.6	CONTINGENCY PLANNING	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CP-1	Contingency Planning Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
CP-1	Contingency Planning Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
CP-1	Contingency Planning Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
CP-2	Contingency Plan	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
CP-2	Contingency Plan	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Ongoing Contingency Planning	BCD-06	decommissioned business practices, including third-party services);(3) Technologies (e.g., new, altered or decommissioned technologies);(4) Data (e.g., changes to data flows and/or data repositories);(5) Facilities (e.g., new,	5	
CP-2(CE-1)	Coordinate with Related Plans	Coordinate contingency plan development with organizational elements responsible for related plans. Supplemental Guidance: Plans related to contingency plans for FTI include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan and Occupant Emergency Plans. Agencies should coordinate with agency IT personnel and when applicable, data center and vendor personnel to protect the confidentiality of FTI.	Functional	Subset Of	Coordinate with Related Plans	BCD-01.1	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	10	
CP-2(CE-3)	Resume Essential Missions and Business Functions	Plan for the resumption of essential mission and business functions within an agency-defined specified time-period of contingency plan activation,	Functional	Intersects With	Resume All Missions & Business Functions	BCD-02.1	Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.	5	
CP-2(CE-3)	Resume Essential Missions and Business Functions	Plan for the resumption of essential mission and business functions within an agency-defined specified time-period of contingency plan activation,	Functional	Intersects With	Resume Essential Missions & Business Functions	BCD-02.3	Mechanisms exist to resume essential missions and business functions within an organization-defined time period of contingency plan activation.	5	
CP-2(CE-8)	Identify Critical Assets	Identify critical system assets supporting essential mission and business functions.	Functional	Subset Of	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	10	
CP-3	Contingency Training	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Contingency Training	BCD-03	Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.	10	
CP-4	Contingency Plan Testing	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	
CP-4	Contingency Plan Testing	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
CP-4(CE-1)	Coordinate with Related Plans	Coordinate contingency plan testing with organizational elements responsible for related plans. Supplemental Guidance: Plans related to contingency plans for FTI include, for example, business continuity plans, disaster recovery plans, continuity of operations plans, crisis communications plans, critical infrastructure plans, cyber incident response plans and occupant emergency plans. Agencies should coordinate with agency IT personnel and when applicable, data center and vendor personnel to protect the confidentiality of FTI.	Functional	Subset Of	Coordinated Testing with Related Plans	BCD-04.1	Mechanisms exist to coordinate contingency plan testing with internal and external elements responsible for related plans.	10	
CP-9	System Backup	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
CP-9(CE-8)	Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of backup information containing FTI. Supplemental Guidance: The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. This control enhancement applies to system backup information in storage at primary and alternate locations to ensure only those authorized individuals have access to FTI.	Functional	Subset Of	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	10	
CP-10	System Recovery and Reconstitution	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5	
CP-10	System Recovery and Reconstitution	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
CP-10	System Recovery and Reconstitution	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
CP-10(CE-2)	Transaction Recovery	Implement transaction recovery for systems that are transaction-based. Supplemental Guidance: Transaction-based systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.	Functional	Subset Of	Transaction Recovery	BCD-12.1	Mechanisms exist to utilize specialized backup mechanisms that will allow transaction recovery for transaction-based Technology Assets, Applications and/or Services (TAAS) in accordance with Recovery Point Objectives (RPOs).	10	
4.7	IDENTIFICATION AND AUTHENTICATION	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
IA-1	Identification and Authentication Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
IA-1	Identification and Authentication Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
IA-1	Identification and Authentication Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
IA-2(CE-1)	Multifactor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts. Supplemental Guidance: Regardless of the type of access (i.e., local, network or remote) privileged accounts must always authenticate using multifactor options, except in the event of direct terminal access from within a restricted area (as defined in Section 2.B.3, Restricted Area Access). Local access is any access to agency systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks. Network access is access to agency systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between agency controlled endpoints and non-agency-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:(1) Remote network access;(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or(3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IA-2(CE-1)	Multifactor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts. Supplemental Guidance: Regardless of the type of access (i.e., local, network or remote) privileged accounts must always authenticate using multifactor options, except in the event of direct terminal access from within a restricted area (as defined in Section 2.B.3, Restricted Area Access). Local access is any access to agency systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks. Network access is access to agency systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between agency controlled endpoints and non-agency-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network.	Functional	Intersects With	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5	
IA-2(CE-1)	Multifactor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts. Supplemental Guidance: Regardless of the type of access (i.e., local, network or remote) privileged accounts must always authenticate using multifactor options, except in the event of direct terminal access from within a restricted area (as defined in Section 2.B.3, Restricted Area Access). Local access is any access to agency systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks. Network access is access to agency systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between agency controlled endpoints and non-agency-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network.	Functional	Intersects With	Information Assurance Enabled Products	TDA-02.2	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-approved.	5	
IA-2(CE-1)	Multifactor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts. Supplemental Guidance: Regardless of the type of access (i.e., local, network or remote) privileged accounts must always authenticate using multifactor options, except in the event of direct terminal access from within a restricted area (as defined in Section 2.B.3, Restricted Area Access). Local access is any access to agency systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks. Network access is access to agency systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between agency controlled endpoints and non-agency-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network.	Functional	Intersects With	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	5	
IA-2(CE-1)	Multifactor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts. Supplemental Guidance: Regardless of the type of access (i.e., local, network or remote) privileged accounts must always authenticate using multifactor options, except in the event of direct terminal access from within a restricted area (as defined in Section 2.B.3, Restricted Area Access). Local access is any access to agency systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks. Network access is access to agency systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between agency controlled endpoints and non-agency-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network.	Functional	Intersects With	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	
IA-2(CE-1)	Multifactor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts. Supplemental Guidance: Regardless of the type of access (i.e., local, network or remote) privileged accounts must always authenticate using multifactor options, except in the event of direct terminal access from within a restricted area (as defined in Section 2.B.3, Restricted Area Access). Local access is any access to agency systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks. Network access is access to agency systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between agency controlled endpoints and non-agency-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network.	Functional	Intersects With	Network Access to Non-Privileged Accounts	IAC-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	5	
IA-2(CE-1)	Multifactor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts. Supplemental Guidance: Regardless of the type of access (i.e., local, network or remote) privileged accounts must always authenticate using multifactor options, except in the event of direct terminal access from within a restricted area (as defined in Section 2.B.3, Restricted Area Access). Local access is any access to agency systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks. Network access is access to agency systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between agency controlled endpoints and non-agency-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network.	Functional	Intersects With	Hardware Token-Based Authentication	IAC-10.7	Automated mechanisms exist to ensure organization-defined token quality requirements are satisfied for hardware token-based authentication.	5	
IA-2(CE-2)	Multifactor Authentication to Non-Privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts. Supplemental Guidance: Regardless of the type of access (i.e., local, network or remote) non-privileged accounts must always authenticate using multifactor options. Local access is any access to agency systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks. Network access is access to agency systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between agency-controlled endpoints and non-agency-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network.	Functional	Intersects With	Information Assurance Enabled Products	TDA-02.2	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-approved.	5	
IA-2(CE-2)	Multifactor Authentication to Non-Privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts. Supplemental Guidance: Regardless of the type of access (i.e., local, network or remote) non-privileged accounts must always authenticate using multifactor options. Local access is any access to agency systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks. Network access is access to agency systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between agency-controlled endpoints and non-agency-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network.	Functional	Intersects With	Network Access to Non-Privileged Accounts	IAC-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	5	
IA-2(CE-2)	Multifactor Authentication to Non-Privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts. Supplemental Guidance: Regardless of the type of access (i.e., local, network or remote) non-privileged accounts must always authenticate using multifactor options. Local access is any access to agency systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks. Network access is access to agency systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between agency-controlled endpoints and non-agency-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network.	Functional	Intersects With	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IA-2(CE-2)	Multifactor Authentication to Non-Privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts. Supplemental Guidance: Regardless of the type of access (i.e., local, network or remote) non-privileged accounts must always authenticate using multifactor options. Local access is any access to agency systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks. Network access is access to agency systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between agency-controlled endpoints and non-agency-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network.	Functional	Intersects With	Hardware Token-Based Authentication	IAC-10.7	Automated mechanisms exist to ensure organization-defined token quality requirements are satisfied for hardware token-based authentication.	5	
IA-2(CE-2)	Multifactor Authentication to Non-Privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts. Supplemental Guidance: Regardless of the type of access (i.e., local, network or remote) non-privileged accounts must always authenticate using multifactor options. Local access is any access to agency systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks. Network access is access to agency systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between agency-controlled endpoints and non-agency-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network.	Functional	Intersects With	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	
IA-2(CE-2)	Multifactor Authentication to Non-Privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts. Supplemental Guidance: Regardless of the type of access (i.e., local, network or remote) non-privileged accounts must always authenticate using multifactor options. Local access is any access to agency systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks. Network access is access to agency systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between agency-controlled endpoints and non-agency-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:(1) Remote network access;(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or(3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	5	
IA-2(CE-2)	Multifactor Authentication to Non-Privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts. Supplemental Guidance: Regardless of the type of access (i.e., local, network or remote) non-privileged accounts must always authenticate using multifactor options. Local access is any access to agency systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks. Network access is access to agency systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between agency-controlled endpoints and non-agency-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network.	Functional	Intersects With	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5	
IA-2(CE-6)	Access to Accounts – Separate Device	Implement multi-factor authentication for remote access to privileged accounts and non-privileged accounts such that:	Functional	Subset Of	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	10	
IA-2(CE-6).a	Access to Accounts – Separate Device	One of the factors is provided by a device separate from the system gaining access; and	Functional	Subset Of	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	10	
IA-2(CE-6).b	Access to Accounts – Separate Device	The device meets Authenticator Assurance Level 2 (AAL) per NIST SP 800-63.	Functional	Subset Of	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	10	
IA-2(CE-8)	Access to Accounts – Replay Resistant	Implement replay-resistant authentication mechanisms for access to privileged accounts with network access. Supplemental Guidance: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as time synchronous or challengeresponse one-time authenticators.	Functional	Subset Of	Replay-Resistant Authentication	IAC-02.2	Automated mechanisms exist to employ replay-resistant authentication.	10	
IA-3	Device Identification and Authentication	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5	
IA-3(CE-1)	Cryptographic Bidirectional Authentication	Authenticate all devices before establishing a remote network connection using bidirectional authentication that is cryptographically based.	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5	
IA-4	Identifier Management	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
IA-4	Identifier Management	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	5	
IA-4(CE-4)	Identify User Status	Manage individual identifiers by uniquely identifying each individual as agency-defined characteristic identifying individual status (e.g., Contractor). Supplemental Guidance: Characteristics identifying the status of individuals include, for example, contractors and foreign nationals. Identifying the status of individuals by specific characteristics provides additional information about the people with whom agency personnel are communicating. For example, it might be useful for an agency employee to know that one of the individuals on an email message is a contractor.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
IA-4(CE-4)	Identify User Status	Manage individual identifiers by uniquely identifying each individual as agency-defined characteristic identifying individual status (e.g., Contractor). Supplemental Guidance: Characteristics identifying the status of individuals include, for example, contractors and foreign nationals. Identifying the status of individuals by specific characteristics provides additional information about the people with whom agency personnel are communicating. For example, it might be useful for an agency employee to know that one of the individuals on an email message is a contractor.	Functional	Intersects With	User Identity (ID) Management	IAC-09.1	Mechanisms exist to ensure proper user identification management for non-consumer users and administrators.	5	
IA-4(CE-4)	Identify User Status	Manage individual identifiers by uniquely identifying each individual as agency-defined characteristic identifying individual status (e.g., Contractor). Supplemental Guidance: Characteristics identifying the status of individuals include, for example, contractors and foreign nationals. Identifying the status of individuals by specific characteristics provides additional information about the people with whom agency personnel are communicating. For example, it might be useful for an agency employee to know that one of the individuals on an email message is a contractor.	Functional	Intersects With	Identity User Status	IAC-09.2	Mechanisms exist to identify contractors and other third-party users through unique username characteristics.	5	
IA-4(IRS-Defined)	N/A	Change all default vendor-set or factory-set administrator accounts prior to implementation (e.g., during installation or immediately after installation).	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
IA-4(IRS-Defined)	N/A	Change all default vendor-set or factory-set administrator accounts prior to implementation (e.g., during installation or immediately after installation).	Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	5	
IA-5	Authenticator Management	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
IA-5	Authenticator Management	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	
IA-5(CE-1)	Password-Based Authentication	For password-based authentication: Supplemental Guidance: If all parameters of this control are not able to be implemented through technical means, compensations and mitigations must be documented and implemented. For example: If a component is unable to enforce 4 types of characters (numbers, uppercase letters, lowercase letters, and special characters) for complexity requirements, then the number of characters required should be increased to compensate. Users should be encouraged to make their passwords (or passphrases) as lengthy as they want, within reason.	Functional	Subset Of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
IA-5(CE-1).a	Password-Based Authentication	Maintain a list of commonly-used, expected, or compromised passwords and update the list every three (3) years and when organizational passwords are suspected to have been compromised directly or indirectly;	Functional	Intersects With	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	5	
IA-5(CE-1).b	Password-Based Authentication	Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);	Functional	Intersects With	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	5	
IA-5(CE-1).c	Password-Based Authentication	Transmit passwords only over cryptographically-protected channels;	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
IA-5(CE-1).d	Password-Based Authentication	Store passwords using an approved salted key derivation function, preferably using a keyed hash;	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
IA-5(CE-1).e	Password-Based Authentication	Require immediate selection of a new password upon account recovery;	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
IA-5(CE-1).f	Password-Based Authentication	Allow user selection of long passwords and passphrases, including spaces and all printable characters;	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IA-5(CE-1).g	Password-Based Authentication	Employ automated tools to assist the user in selecting strong password authenticators; and	Functional	Intersects With	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	5	
IA-5(CE-1).h	Password-Based Authentication	Enforce the following composition and complexity rules:	Functional	Subset Of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
IA-5(CE-1).h.1	Password-Based Authentication	Enforce minimum password length of fourteen (14) characters.	Functional	Subset Of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
IA-5(CE-1).h.2	Password-Based Authentication	Enforce minimum password complexity to contain a combination of numbers, uppercase letters, lowercase letters, and special characters.	Functional	Subset Of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
IA-5(CE-1).h.3	Password-Based Authentication	Enforce at least one (1) character change when new passwords are selected for use.	Functional	Subset Of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
IA-5(CE-1).h.4	Password-Based Authentication	Store and transmit only cryptographically protected passwords.	Functional	Subset Of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
IA-5(CE-1).h.5	Password-Based Authentication	Enforce password lifetime restrictions:	Functional	Subset Of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
IA-5(CE-1).h.5.i	Password-Based Authentication	One (1) day minimum and 90 days maximum.	Functional	Subset Of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
IA-5(CE-1).h.5.ii	Password-Based Authentication	Service accounts passwords shall expire within 366 days (inclusive).	Functional	Subset Of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
IA-5(CE-1).h.6	Password-Based Authentication	Password History/Reuse:	Functional	Subset Of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
IA-5(CE-1).h.6.i	Password-Based Authentication	For all systems: 24 generations.	Functional	Subset Of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
IA-5(CE-1).h.6.ii	Password-Based Authentication	For systems unable to implement history/reuse restriction by generations but are able to restrict history/reuse for a specified time period, passwords shall not be reusable for a period of six (6) months.	Functional	Subset Of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
IA-5(CE-1).h.7	Password-Based Authentication	Allow the use of a temporary password for system logons with an immediate change to a permanent password.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
IA-5(IRS-Defined)-1	N/A	Train users not to use a single dictionary word as their password.	Functional	Subset Of	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	10	
IA-5(IRS-Defined)-2	N/A	For IT devices using a personal identification number (PIN) as an authenticator for MFA, enforce the following requirements:	Functional	Subset Of	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	10	
IA-5(IRS-Defined)-2.a	N/A	Minimum length of eight (8) digits. If the system does not enforce a minimum length of 8 digits, the maximum length possible must be used;	Functional	Subset Of	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	10	
IA-5(IRS-Defined)-2.b	N/A	Enforce complex sequences (e.g., 73961548 – no repeating digits and no sequential digits);	Functional	Subset Of	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	10	
IA-5(IRS-Defined)-2.c	N/A	Do not store with the SmartCard; and	Functional	Subset Of	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	10	
IA-5(IRS-Defined)-2.d	N/A	Do not share.	Functional	Subset Of	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	10	
IA-5(CE-2)	Public Key-Based Authentication	N/A	Functional	Subset Of	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	10	
IA-5(CE-2).a	Public Key-Based Authentication	For public key-based authentication	Functional	Subset Of	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	10	
IA-5(CE-2).a.1	Public Key-Based Authentication	Enforce authorized access to the corresponding private key; and	Functional	Subset Of	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	10	
IA-5(CE-2).a.2	Public Key-Based Authentication	Map the authenticated identity to the account of the individual or group; and	Functional	Subset Of	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	10	
IA-5(CE-2).b	Public Key-Based Authentication	When public key infrastructure (PKI) is used:	Functional	Subset Of	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	10	
IA-5(CE-2).b.1	Public Key-Based Authentication	Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and	Functional	Subset Of	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	10	
IA-5(CE-2).b.2	Public Key-Based Authentication	Implement a local cache of revocation data to support path discovery and validation.	Functional	Subset Of	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	10	
IA-5(CE-5)	Change Authenticators Prior to Delivery	Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation. Supplemental Guidance: This typically does not apply to developers of commercial off-the-shelf information technology products.	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	
IA-5(CE-6)	Protection of Authenticators	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	Functional	Intersects With	User Responsibilities for Account Management	IAC-18	Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.).	5	
IA-5(CE-6)	Protection of Authenticators	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
IA-5(CE-7)	No Embedded Unencrypted Static Authenticators	Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.	Functional	Subset Of	No Embedded Unencrypted Static Authenticators	IAC-10.6	Mechanisms exist to ensure that unencrypted, static authenticators are not embedded in applications, scripts or stored on function keys.	10	
IA-5(CE-12)	Biometric Authentication Performance	For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements defined in NIST SP 800-63.	Functional	Subset Of	Biometric Authentication	IAC-10.12	Mechanisms exist to ensure biometric-based authentication satisfies organization-defined biometric quality requirements for false positives and false negatives.	10	
IA-6	Authenticator Feedback	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Authenticator Feedback	IAC-11	Mechanisms exist to obscure the feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	10	
IA-7	Cryptographic Module Authentication	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Cryptographic Module Authentication	IAC-12	Mechanisms exist to ensure cryptographic modules adhere to applicable statutory, regulatory and contractual requirements for security strength.	5	
IA-7	Cryptographic Module Authentication	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Automated Authentication Through Cryptographic Modules	CRY-02	Automated mechanisms exist to enable systems to authenticate to a cryptographic module.	5	
IA-8	Identification and Authentication (Non-Organizational Users)	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	10	
IA-8(CE-2)	Acceptance of External Credentials	Supplemental Guidance: This control enhancement applies to agency systems that are accessible to the public, for example, public-facing websites or web portals. External credentials must be certified as compliant with NIST Special Publication 800-63.	Functional	Subset Of	Acceptance of Third-Party Credentials	IAC-03.2	Automated mechanisms exist to accept Federal Identity, Credential and Access Management (FICAM)-approved third-party credentials.	10	
IA-8(CE-2).a	Acceptance of External Credentials	Accept only external authenticators that are NIST-compliant; and	Functional	Subset Of	Acceptance of Third-Party Credentials	IAC-03.2	Automated mechanisms exist to accept Federal Identity, Credential and Access Management (FICAM)-approved third-party credentials.	10	
IA-8(CE-2).b	Acceptance of External Credentials	Document and maintain a list of accepted external authenticators.	Functional	Subset Of	Acceptance of Third-Party Credentials	IAC-03.2	Automated mechanisms exist to accept Federal Identity, Credential and Access Management (FICAM)-approved third-party credentials.	10	
IA-8(CE-4)	Use of Defined Profiles	Conform to the following profiles for identity management: NIST or FICAM-issued profiles. Supplemental Guidance: This control enhancement addresses open identity management standards. To ensure that these identity management standards are viable, robust, reliable, sustainable, and interoperable as documented, the United States Government assesses and scopes the standards and technology implementations against applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines. The result is NIST-issued implementation profiles of approved protocols.	Functional	Subset Of	Use of FICAM-Issued Profiles	IAC-03.3	Mechanisms exist to conform systems to Federal Identity, Credential and Access Management (FICAM)-issued profiles.	10	
IA-8(IRS-Defined)	N/A	Deploy identification and authentication technology consistent with the results of the eauthentication risk analysis. See Section 3.3.8, Public-Facing Systems, for additional information regarding public-facing identification and authentication.	Functional	Subset Of	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	10	
IA-9	Service Identification and Authentication	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS)	IAC-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).	10	
IA-11	Re-Authentication	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Re-Authentication	IAC-14	Mechanisms exist to force users and devices to re-authenticate according to organization-defined circumstances that necessitate re-authentication.	10	
IA-12	Identity Proofing	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Identity Proofing (Identity Verification)	IAC-28	Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.	10	
IA-12(CE-1)	Supervisor Authorization	Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.	Functional	Intersects With	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	5	
IA-12(CE-2)	Identity Evidence	Require evidence of individual identification be presented to the registration authority. Supplemental Guidance: Requiring identity evidence, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity, or at least increases the work factor of potential adversaries. Acceptable forms of evidence are consistent with the risk to the systems, roles and privileges associated with the user's account.	Functional	Subset Of	Identity Evidence	IAC-28.2	Mechanisms exist to require evidence of individual identification to be presented to the registration authority.	10	
IA-12(CE-3)	Identity Evidence Validation and Verification	Require that the presented identity evidence be validated and verified through NIST SP 800-63 compliant methods of validation and verification. Supplemental Guidance: Validating and verifying identity evidence increases the assurance that accounts, identifiers, and authenticators are being issued to the correct user. Validation refers to the process of confirming that the evidence is genuine and authentic, and that the data contained in the evidence is correct, current, and related to an actual person or individual. Verification confirms and establishes a linkage between the claimed identity and the actual existence of the user presenting the evidence. Acceptable methods for validating and verifying identity evidence are consistent with the risk to the systems, roles and privileges associated with the user's account.	Functional	Subset Of	Identity Evidence Validation & Verification	IAC-28.3	Mechanisms exist to require that the presented identity evidence be validated and verified through organizational-defined methods of validation and verification.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IA-12(CE-5)	Address Confirmation	Require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record. Supplemental Guidance: To make it more difficult for adversaries to pose as legitimate users during the identity proofing process, agencies must use out-of-band methods to increase assurance that the individual associated with an address of record was the same person that participated in the registration. Confirmation can take the form of a temporary enrollment code or a notice of proofing. The delivery address for these artifacts are obtained from records and not self-asserted by the user. The address can include a physical or a digital address. A home address is an example of a physical address. Email addresses and telephone numbers are examples of digital addresses. See Section 3.3.8, Public-Facing Systems, for additional information regarding multifactor requirements and solutions.	Functional	Subset Of	Address Confirmation	IAC-28.5	Mechanisms exist to require that a notice of proofing be delivered through an out-of-band channel to verify the user's address (physical or digital).	10	
4.8	INCIDENT RESPONSE	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
IR-1	Incident Response Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
IR-1	Incident Response Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
IR-1	Incident Response Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	5	
IR-1	Incident Response Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	
IR-1	Incident Response Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
IR-2	Incident Response Training	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	
IR-2(CE-1)	Simulated Events	Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations. Supplemental Guidance: This control can be met by performing a table-top exercise using simulated events. Simulated events must include an event where FTI is compromised.	Functional	Subset Of	Simulated Incidents	IRO-05.1	Mechanisms exist to incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.	10	
IR-2(CE-3)	Breach	Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	
IR-3	Incident Response Testing	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	
IR-3(CE-2)	Coordination with Related Plans	Coordinate incident response testing with organizational elements responsible for related plans. Supplemental Guidance: Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Occupant Emergency Plans and Critical Infrastructure Plans. Agencies should coordinate with agency IT personnel and when applicable, data center and vendor personnel to protect the confidentiality of FTI.	Functional	Subset Of	Coordination with Related Plans	IRO-06.1	Mechanisms exist to coordinate incident response testing with organizational elements responsible for related plans.	10	
IR-3(CE-3)	Continuous Improvement	Use qualitative and quantitative data from testing to:	Functional	Subset Of	Continuous Incident Response Improvements	IRO-04.3	Mechanisms exist to use qualitative and quantitative data from incident response testing to:(1) Determine the effectiveness of incident response processes;(2) Continuously improve incident response processes; and(3) Provide incident response measures and metrics that are accurate, consistent and in a reproducible format.	10	
IR-3(CE-3).a	Continuous Improvement	Determine the effectiveness of incident response processes;	Functional	Subset Of	Continuous Incident Response Improvements	IRO-04.3	Mechanisms exist to use qualitative and quantitative data from incident response testing to:(1) Determine the effectiveness of incident response processes;(2) Continuously improve incident response processes; and(3) Provide incident response measures and metrics that are accurate, consistent and in a reproducible format.	10	
IR-3(CE-3).b	Continuous Improvement	Continuously improve incident response processes; and	Functional	Subset Of	Continuous Incident Response Improvements	IRO-04.3	Mechanisms exist to use qualitative and quantitative data from incident response testing to:(1) Determine the effectiveness of incident response processes;(2) Continuously improve incident response processes; and(3) Provide incident response measures and metrics that are accurate, consistent and in a reproducible format.	10	
IR-3(CE-3).c	Continuous Improvement	Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.	Functional	Subset Of	Continuous Incident Response Improvements	IRO-04.3	Mechanisms exist to use qualitative and quantitative data from incident response testing to:(1) Determine the effectiveness of incident response processes;(2) Continuously improve incident response processes; and(3) Provide incident response measures and metrics that are accurate, consistent and in a reproducible format.	10	
IR-4	Incident Handling	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
IR-4(CE-1)	Automated Incident Handling Processes	Support the incident handling process using automated mechanisms. Supplemental Guidance: Automated mechanisms supporting incident handling processes include, for example, online incident management systems; and tools that support collection of live response data, full network packet capture and forensic analysis.	Functional	Subset Of	Automated Incident Handling Processes	IRO-02.1	Automated mechanisms exist to support the incident handling process.	10	
IR-4(CE-6)	Insider Threats	Implement an incident handling capability for incidents involving insider threats.	Functional	Intersects With	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5	
IR-4(CE-8)	Correlation with External Organizations	Coordinate with contractors, data centers, counties, and other agencies to correlate and share incidents involving FTI to achieve a cross-organization perspective on incident awareness and more effective incident responses. Supplemental Guidance: The coordination of incident information with external organizations—including mission or business partners, customers, and developers—can provide significant benefits. Crossorganizational coordination can serve as an important risk management capability. This capability allows organizations to leverage information from a variety of sources to effectively respond to incidents and breaches that could potentially affect the organization's operations, assets, and individuals.	Functional	Subset Of	Correlation with External Organizations	IRO-02.5	Mechanisms exist to coordinate with approved third-parties to achieve a cross-organization perspective on incident awareness and more effective incident responses.	10	
IR-5	Incident Monitoring	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	10	
IR-6	Incident Reporting	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	5	
IR-6	Incident Reporting	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	5	
IR-6	Incident Reporting	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	5	
IR-6(CE-1)	Automated Reporting	Report incidents using automated mechanisms. Supplemental Guidance: Automated mechanisms for tracking incidents and for collecting and analyzing incident information include, for example, Computer Incident Response Centers or other electronic databases of incidents and network monitoring devices.	Functional	Subset Of	Automated Reporting	IRO-10.1	Automated mechanisms exist to assist in the reporting of cybersecurity and data protection incidents.	10	
IR-6(CE-2)	Vulnerabilities Related to Incidents	Report system vulnerabilities associated with reported incidents to designated agency personnel. Supplemental Guidance: Reported incidents that uncover system vulnerabilities are analyzed by organizational personnel including system owners, mission and business owners, senior agency information security officers, senior agency officials for privacy, authorizing officials, and the risk executive (function). The analysis can serve to prioritize and initiate mitigation actions to address the discovered system vulnerability.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	
IR-6(CE-3)	Supply Chain Coordination	Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident. Supplemental Guidance: Agencies involved in supply chain activities include, for example, system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include, for example, compromises/breaches involving system components, information technology products, development processes or personnel and distribution processes or warehousing facilities. Organizations determine the appropriate information to share considering the value gained from support by external organizations with the potential for harm due to controlled unclassified information being released to outside organizations of perhaps questionable trustworthiness.	Functional	Intersects With	Vulnerabilities Related To Incidents	IRO-10.3	Mechanisms exist to report system vulnerabilities associated with reported cybersecurity and data protection incidents to organization-defined personnel or roles.	5	
IR-7	Incident Response Assistance	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for TAAS related to the incident.	5	
IR-7(CE-1)	Automation Support for Availability of Information and Support	Increase the availability of incident response information and support using automated mechanisms. Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or the assistance capability can proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.	Functional	Subset Of	Incident Reporting Assistance	IRO-11	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	10	
IR-7(CE-2)	Coordination with External Providers	N/A	Functional	Subset Of	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	10	
IR-7(CE-2).a	Coordination with External Providers	Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability; and	Functional	Subset Of	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	10	
IR-7(CE-2).b	Coordination with External Providers	Identify organizational incident response team members to the external providers.	Functional	Subset Of	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	10	
IR-8	Incident Response Plan	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IR-8(CE-1)	Breaches	Include the following in the Incident Response Plan for breaches involving personally identifiable information:	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
IR-8(CE-1).a	Breaches	A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
IR-8(CE-1).b	Breaches	An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
IR-8(CE-1).c	Breaches	Identification of applicable privacy requirements.	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
IR-9	Information Spillage Response	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive/regulated data spills.	5	
4.9	MAINTENANCE	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
MA-1	System Maintenance Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10	
MA-1	System Maintenance Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Remote Maintenance Notifications	MNT-05.2	Mechanisms exist to require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time).	5	
MA-1	System Maintenance Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5	
MA-1	System Maintenance Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
MA-1	System Maintenance Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
MA-2	Controlled Maintenance	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	10	
MA-3	Maintenance Tools	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5	
MA-3(CE-1)	Inspect Tools	Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications. Supplemental Guidance: If, upon inspection of maintenance tools, agencies determine that the tools have been modified in an improper/unauthorized manner or contain malicious code, the incident is handled consistent with agency policies and procedures for incident handling.	Functional	Subset Of	Inspect Tools	MNT-04.1	Mechanisms exist to inspect maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.	10	
MA-3(CE-2)	Inspect Media	Check media containing diagnostic and test programs for malicious code before the media are used in the system. Supplemental Guidance: If, upon inspection of media containing maintenance diagnostic and test programs, agencies determine that the media contain malicious code, the incident is handled consistent with agency incident handling policies and procedures.	Functional	Subset Of	Inspect Media	MNT-04.2	Mechanisms exist to check media containing diagnostic and test programs for malicious code before the media are used.	10	
MA-3(CE-3)	Prevent Unauthorized Removal	Prevent the removal of maintenance equipment containing organizational information by: Supplemental Guidance: Organizational information includes all information specifically owned by agencies and information provided to agencies in which agencies serve as information stewards.	Functional	Subset Of	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.	10	
MA-3(CE-3).a	Prevent Unauthorized Removal	Verifying that there is no organizational information contained on the equipment;	Functional	Subset Of	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.	10	
MA-3(CE-3).b	Prevent Unauthorized Removal	Sanitizing or destroying the equipment;	Functional	Subset Of	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.	10	
MA-3(CE-3).c	Prevent Unauthorized Removal	Retaining the equipment within the facility; or	Functional	Subset Of	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.	10	
MA-3(CE-3).d	Prevent Unauthorized Removal	Obtaining an exemption from a designated agency official(s) explicitly authorizing removal of the equipment from the facility.	Functional	Subset Of	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.	10	
MA-3(CE-4)	Restricted Tool Use	Restrict the use of maintenance tools to authorized personnel only.	Functional	Subset Of	Restrict Tool Usage	MNT-04.4	Automated mechanisms exist to restrict the use of maintenance tools to authorized maintenance personnel and/or roles.	10	
MA-3(CE-5)	Execution with Privilege	Monitor the use of maintenance tools that execute with increased privilege.	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5	
MA-4	Nonlocal Maintenance	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	5	
MA-4	Nonlocal Maintenance	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Remote Maintenance Notifications	MNT-05.2	Mechanisms exist to require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time).	5	
MA-4	Nonlocal Maintenance	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5	
MA-4(CE-1)	Logging and Review	N/A	Functional	Subset Of	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5	
MA-4(CE-1).a	Logging and Review	Log events defined in AU-2a for nonlocal maintenance and diagnostic sessions; and	Functional	Subset Of	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5	
MA-4(CE-1).b	Logging and Review	Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.	Functional	Subset Of	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5	
MA-4(CE-4)	Authentication and Separation of Maintenance Sessions	Protect nonlocal maintenance sessions by:	Functional	Subset Of	Separation of Maintenance Sessions	MNT-05.7	Mechanisms exist to protect maintenance sessions through replay-resistant sessions that are physically or logically separated communications paths from other network sessions.	10	
MA-4(CE-4).a	Authentication and Separation of Maintenance Sessions	Employing multifactor authentication consistent with NIST 800-63 Digital Identity Guidelines requirements; and	Functional	Subset Of	Separation of Maintenance Sessions	MNT-05.7	Mechanisms exist to protect maintenance sessions through replay-resistant sessions that are physically or logically separated communications paths from other network sessions.	10	
MA-4(CE-4).b	Authentication and Separation of Maintenance Sessions	Separating the maintenance sessions from other network sessions with the system by either:	Functional	Subset Of	Separation of Maintenance Sessions	MNT-05.7	Mechanisms exist to protect maintenance sessions through replay-resistant sessions that are physically or logically separated communications paths from other network sessions.	10	
MA-4(CE-4).b.1	Authentication and Separation of Maintenance Sessions	Physically separated communications paths; or	Functional	Subset Of	Separation of Maintenance Sessions	MNT-05.7	Mechanisms exist to protect maintenance sessions through replay-resistant sessions that are physically or logically separated communications paths from other network sessions.	10	
MA-4(CE-4).b.2	Authentication and Separation of Maintenance Sessions	Logically separated communications paths.	Functional	Subset Of	Separation of Maintenance Sessions	MNT-05.7	Mechanisms exist to protect maintenance sessions through replay-resistant sessions that are physically or logically separated communications paths from other network sessions.	10	
MA-4(CE-6)	Cryptographic Protection	Implement the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: Virtual Private Network (VPN) connection.	Functional	Subset Of	Remote Maintenance Cryptographic Protection	MNT-05.3	Cryptographic mechanisms exist to protect the integrity and confidentiality of remote, non-local maintenance and diagnostic communications.	10	
MA-4(CE-7)	Disconnect Verification	Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.	Functional	Subset Of	Remote Maintenance Disconnect Verification	MNT-05.4	Mechanisms exist to provide remote disconnect verification to ensure remote, non-local maintenance and diagnostic sessions are properly terminated.	10	
MA-5	Maintenance Personnel	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Authorized Maintenance Personnel	MNT-06	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	10	
MA-5(CE-5)	Non-System Maintenance	Ensure that non-escorted personnel performing maintenance activities not directly associated with the system but in the physical proximity of the system, have required access authorizations.	Functional	Subset Of	Non-System Related Maintenance	MNT-06.2	Mechanisms exist to ensure that non-escorted personnel performing non-IT maintenance activities in the physical proximity of systems have required access authorizations.	10	
MA-6	Timely Maintenance	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Timely Maintenance	MNT-03	Mechanisms exist to obtain maintenance support and/or spare parts for Technology Assets, Applications and/or Services (TAAS) within a defined Recovery Time Objective (RTO).	10	
4.10	MEDIA PROTECTION	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
MP-1	Media Protection Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
MP-1	Media Protection Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
MP-1	Media Protection Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
MP-2	Media Access	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
MP-2	Media Access	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	5	
MP-3	Media Marking	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
MP-3	Media Marking	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Automated Marking	DCH-04.1	Automated mechanisms exist to mark physical media and digital files to indicate the distribution limitations, handling requirements and applicable security markings (if any) of the information to aid Data Loss Prevention (DLP) technologies.	5	
MP-4	Media Storage	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Media Storage	DCH-06	Mechanisms exist to:(1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and(2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	10	
MP-5	Media Transport	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	10	
MP-5(CE-3)	Custodians	Employ an identified custodian during transport of system media outside of controlled areas.	Functional	Subset Of	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	10	
MP-6	Media Sanitization	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	5	
MP-6(CE-1)	Review, Approve, Track, Document, and Verify	Review, approve, track, document, and verify media sanitization and disposal actions.	Functional	Subset Of	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	10	
MP-6(IRS-Defined)-1	N/A	Clear or purge any sensitive data from the system BIOS or UEFI before a computer system is disposed of and leaves the agency. Reset the BIOS or UEFI to the manufacturer's default profile, to ensure the removal of sensitive settings such as passwords or keys.	Functional	Subset Of	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
MP-6(IRS-Defined)-2	N/A	Media provided by foreign visitors (end users) may only be loaded into a standalone agency system. The system must remain standalone until such time as it is sanitized. Additionally, no other media loaded into the standalone system can be loaded into a non-standalone agency system until sanitized. Supplemental Guidance: The control above permits, for example, foreign visitors to provide files for presentation at an agency conference or meeting provided the computer is standalone. If such a file is required for other purposes, the preferred means for obtaining it would be to ask the visitor to email it. The control also seeks to minimize the risk that malicious code on the standalone machine will be moved via media to other systems. Additional requirements for protecting FTI during media sanitization are provided on the Office of Safeguards website.	Functional	Subset Of	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	5	
MP-7	Media Use	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
MP-7	Media Use	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
MP-7	Media Use	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Prohibit Use Without Owner	DCH-10.2	Mechanisms exist to prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.	5	
MP-7(IRS-Defined)	N/A	Develop policy to disable all portable storage devices with the exception of those required for explicit business need, which shall be restricted to specific workstations or laptops. In the absence of an agency-developed and issued policy, the default policy is:	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
MP-7(IRS-Defined).a	N/A	That the connection of non-agency portable storage devices is disallowed; and	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
MP-7(IRS-Defined).b	N/A	Technical controls are implemented to enforce the policy (e.g., Implement data loss prevention software to limit the use of removable media to known devices, blacklist usb-storage, prevent the mounting of USB storage, Deny All Access to All Removable Storage Classes).	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
4.11	PHYSICAL AND ENVIRONMENTAL PROTECTION	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
PE-1	Physical and Environmental Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
PE-1	Physical and Environmental Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
PE-1	Physical and Environmental Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
PE-1(IRS-Defined)-1	N/A	Develop policy and procedures as needed to address their specific building access systems (e.g., restriction of physical access, identification and authentication and audit logging), that are critical to the security of a facility.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
PE-1(IRS-Defined)-2	N/A	Develop and implement a clean desk policy for the protection of FTI (e.g., paper output, electronic storage media) to preclude unauthorized disclosures.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
PE-1(IRS-Defined)-3	N/A	Designate restricted IT areas that house IT assets such as, but not limited to, mainframes, servers, controlled interface equipment, associated peripherals and communications equipment.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
PE-2	Physical Access Authorizations	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	10	
PE-3	Physical Access Control	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
PE-3(CE-2)	Facility and Systems	Perform security checks at a minimum daily at the physical perimeter of the facility or system for exfiltration of information or removal of system components.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
PE-4	Access Control for Transmission	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
PE-5	Access Control for Output Devices	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Access Control for Output Devices	PES-12.2	Physical security mechanisms exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output.	10	
PE-6	Monitoring Physical Access	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	10	
PE-6(CE-1)	Intrusion Alarms and Surveillance Equipment	Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.	Functional	Subset Of	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	10	
PE-8	Visitor Access Records	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	10	
PE-16	Delivery and Removal	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Delivery & Removal	PES-10	Physical security mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access.	10	
PE-17	Alternate Work Site	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Alternate Work Site	PES-11	Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	10	
4.12	PLANNING	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
PL-1	Planning Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
PL-1	Planning Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
PL-1	Planning Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
PL-1	Planning Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
PL-1	Planning Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
PL-2	System Security and Privacy Plans	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Plan / Coordinate with Other Organizational Entities	IAO-03.1	Mechanisms exist to plan and coordinate Information Assurance Program (IAP) activities with affected stakeholders before conducting such activities in order to reduce the potential impact on operations.	5	
PL-2	System Security and Privacy Plans	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including chan	5	
PL-2	System Security and Privacy Plans	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that:(1) Contain sufficient detail to assess the security of the network's architecture;(2) Reflect the current architecture of the network environment; and(3) Document all sensitive/regulated data flows.	5	
PL-2(IRS-Defined)	N/A	Include or reference a plan for media sanitization and disposition that addresses all system media and backups in the agency's system security and privacy plans. See Section MP-6: Media Sanitization for additional information on media sanitization.	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including chan	5	
PL-4	Rules of Behavior	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5	
PL-4	Rules of Behavior	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
PL-4	Rules of Behavior	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5	
PL-4(CE-1)	Social Media and Networking Restrictions	Include in the rules of behavior, restrictions on:	Functional	Subset Of	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	10	
PL-4(CE-1).a	Social Media and Networking Restrictions	Use of social media, social networking sites, and external sites/applications;	Functional	Subset Of	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	10	
PL-4(CE-1).b	Social Media and Networking Restrictions	Posting organizational information on public websites; and	Functional	Subset Of	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	10	
PL-4(CE-1).c	Social Media and Networking Restrictions	Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.	Functional	Subset Of	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	10	
PL-4(IRS-Defined)	N/A	Unless superseded by centrally-issued cross-agency policy, establish usage restrictions and implementation guidance for using Internet-supported technologies (e.g. Instant messaging) based on the potential for these technologies to cause damage or disruption to the information system or the agency's accomplishment of its mission. Document the use of Internet-supporting technologies.	Functional	Subset Of	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	10	
PL-8	Security and Privacy Architectures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5	
PL-8(CE-1)	Defense-In-Depth	Design the security and privacy architectures for the system using a defensein-depth approach that:	Functional	Subset Of	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
PL-8(CE-1).a	Defense-In-Depth	Allocates system communication and other relevant controls to information systems processing, storing, and transmitting FTI; and	Functional	Subset Of	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	10	
PL-8(CE-1).b	Defense-In-Depth	Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner.	Functional	Subset Of	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	10	
4.13	PROGRAM MANAGEMENT	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
PM-1	Information Security Program Plan	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
PM-1	Information Security Program Plan	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
PM-1	Information Security Program Plan	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
PM-2	Information Security Program Leadership Role	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
PM-3	Information Security and Privacy Resources	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
PM-4	Plan of Action and Milestones Process	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
PM-4	Plan of Action and Milestones Process	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable;(7) Point of Contact (POC) (e.g., asset/process owner);(8) Resources required to conduct remediation actions;(9) Planned remedial actions to the	5	
PM-5	System Inventory	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
PM-5	System Inventory	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:(1) Accurately reflects the current TAASD in use;(2) Identifies authorized software products, including business justification details;(3) Is at the level of granularity deemed necessary for tracking and reporting;(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and(5) Is available for review and audit by designated organizational personnel.	5	
PM-5(CE-1)	Inventory of Personally Identifiable Information	Establish, maintain, and update continually an inventory of all systems, applications, and projects that process personally identifiable information.	Functional	Intersects With	Inventory of Personal Data (PD)	PRI-05.5	Mechanisms exist to establish and maintain a current inventory of all Technology Assets, Applications and/or Services (TAAS) that collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD).	5	
PM-5(CE-1)	Inventory of Personally Identifiable Information	Establish, maintain, and update continually an inventory of all systems, applications, and projects that process personally identifiable information.	Functional	Intersects With	Personal Data (PD) Inventory Automation Support	PRI-05.6	Automated mechanisms exist to determine if Personal Data (PD) is maintained in electronic form.	5	
PM-7	Enterprise Architecture	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5	
PM-7(IRS-Defined)	N/A	Review and update the security enterprise architecture data based on the enterprise architecture timeframes.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5	
PM-9	Risk Management Strategy	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
PM-10	Authorization Process	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
PM-12	Insider Threat Program	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross-discipline insider threat incident handling team.	10	
PM-14	Testing, Training and Monitoring	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Personal Data (PD) Control Testing, Training & Monitoring	PRI-08	Mechanisms exist to conduct testing, training and monitoring activities for Personal Data (PD) controls.	5	
PM-14	Testing, Training and Monitoring	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
PM-18	Privacy Program Plan	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
PM-19	Privacy Program Leadership Role	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Chief Privacy Officer (CPO)	PRI-01.1	Mechanisms exist to appoints a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement, applicable data privacy requirements and manage data privacy risks through the organization-wide data privacy program.	10	
PM-21	Accounting of Disclosures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
PM-29	Risk Management Program Leadership Roles	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
PM-29	Risk Management Program Leadership Roles	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
PM-29	Risk Management Program Leadership Roles	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
4.14	PERSONNEL SECURITY	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
PS-1	Personnel Security Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
PS-1	Personnel Security Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
PS-1	Personnel Security Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
PS-2	Position Risk Designation	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
PS-2	Position Risk Designation	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
PS-3	Personnel Screening	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	
PS-4	Personnel Termination	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	10	
PS-5	Personnel Transfer	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.	10	
PS-6	Access Agreements	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	5	
PS-6	Access Agreements	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	5	
PS-6(CE-3)	Post-Employment Requirements	N/A	Functional	Subset Of	Post-Employment Requirements Awareness	HRS-06.2	Mechanisms exist to notify individuals of their applicable, legally-binding post-employment requirements for the protection of sensitive/regulated data.	10	
PS-6(CE-3).a	Post-Employment Requirements	Notify individuals of applicable, legally binding post-employment requirements for protection of organizational information; and	Functional	Subset Of	Post-Employment Requirements Awareness	HRS-06.2	Mechanisms exist to notify individuals of their applicable, legally-binding post-employment requirements for the protection of sensitive/regulated data.	10	
PS-6(CE-3).b	Post-Employment Requirements	Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.	Functional	Subset Of	Post-Employment Requirements Awareness	HRS-06.2	Mechanisms exist to notify individuals of their applicable, legally-binding post-employment requirements for the protection of sensitive/regulated data.	10	
PS-7	External Personnel Security	Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.	Functional	Subset Of	Third-Party Personnel	HRS-10	Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.	10	
PS-8	Personnel Sanctions	Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.	Functional	Subset Of	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	10	
PS-9	Position Descriptions	Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
4.15	PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
PT-1	Personally Identifiable Information Processing and Transparency Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
PT-1	Personally Identifiable Information Processing and Transparency Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
PT-1	Personally Identifiable Information Processing and Transparency Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
PT-1	Personally Identifiable Information Processing and Transparency Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
PT-2	Authority to Process Personally Identifiable Information	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD), either generally or in support of a specific business process.	5	
PT-2	Authority to Process Personally Identifiable Information	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that:(1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and(2) Authorizes the use of PD when such information is required for internal testing, training and research.	5	
PT-2	Authority to Process Personally Identifiable Information	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is	5	
PT-2	Authority to Process Personally Identifiable Information	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	5	
4.16	RISK ASSESSMENT	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
RA-1	Risk Assessment Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
RA-1	Risk Assessment Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RA-1	Risk Assessment Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
RA-3	Risk Assessment	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
RA-3	Risk Assessment	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
RA-3(CE-1)	Supply Chain Risk Assessment	Supplemental Guidance: Supply chain-related events include, for example, disruption, theft, use of defective components, insertion of counterfeits, malicious development practices, improper delivery practices and insertion of malicious code. These events can have a significant impact on the confidentiality, integrity or availability of a system and its information and therefore, can also adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations, the state and the Nation. The supply chain-related events may be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.	Functional	Subset Of	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	10	
RA-3(CE-1).c	Supply Chain Risk Assessment	Assess supply chain risks associated with Federal Tax Information and	Functional	Subset Of	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	10	
RA-3(CE-1).d	Supply Chain Risk Assessment	Update the supply chain risk assessment every three (3) years, when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.	Functional	Subset Of	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	10	
RA-5	Vulnerability Monitoring and Scanning	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
RA-5	Vulnerability Monitoring and Scanning	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	
RA-5(CE-2)	Update by Vulnerabilities to be Scanned	Update the system vulnerabilities to be scanned at least every 30 days; prior to a new scan; when new vulnerabilities are identified and reported.	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	
RA-5(CE-4)	Discoverable Information	Determine information about the system that is discoverable and take appropriate corrective actions.	Functional	Subset Of	Acceptable Discoverable Information	VPM-06.8	Mechanisms exist to define what information is allowed to be discoverable by adversaries and take corrective actions to remediate non-compliant Technology Assets, Applications and/or Services (TAAS).	10	
RA-5(CE-5)	Privileged Access	Implement privileged access authorization to all information system components for selected vulnerability scanning activities. Supplemental Guidance: In certain situations, the nature of the vulnerability scanning may be more intrusive or the system component that is the subject of the scanning may contain classified or controlled unclassified information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.	Functional	Subset Of	Privileged Access	VPM-06.3	Mechanisms exist to implement privileged access authorization for selected vulnerability scanning activities.	10	
RA-5(IRS-Defined)	N/A	Implement a vulnerability management process for IT software systems (including wireless networks) to complement their patch management process.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
RA-7	Risk Response	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Risk Response	RSK-06.1	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related:(1) Assessments;(2) Audits; and/or(3) Incidents.	10	
RA-8	Privacy Impact Assessments	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
4.17	SYSTEM AND SERVICES ACQUISITION	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SA-1	System and Services Acquisition Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
SA-1	System and Services Acquisition Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
SA-1	System and Services Acquisition Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
SA-1	System and Services Acquisition Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
SA-2	Allocation of Resources	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	10	
SA-3	System Development Life Cycle	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5	
SA-3	System Development Life Cycle	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
SA-3(CE-2)	Use of Live Data	Supplemental Guidance: Live data is also referred to as operational data. The use of live data in preproduction environments can result in significant risk to agencies. Agencies can minimize such risk by using test or dummy data during the design, development and testing of systems, system components and system services. To use live FTI in a test or development environment, agencies must submit a notification as described in Section 2.E.6, Notification Reporting Requirements.	Functional	Subset Of	Use of Live Data	TDA-10	Mechanisms exist to approve, document and control the use of live data in development and test environments.	10	
SA-3(CE-2).a	Use of Live Data	Approve, document, and control the use of live data in preproduction environments for the system, system component, or system service; and	Functional	Subset Of	Use of Live Data	TDA-10	Mechanisms exist to approve, document and control the use of live data in development and test environments.	10	
SA-3(CE-2).b	Use of Live Data	Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments.	Functional	Subset Of	Use of Live Data	TDA-10	Mechanisms exist to approve, document and control the use of live data in development and test environments.	10	
SA-4	Acquisition Process	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	
SA-4	Acquisition Process	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
SA-4	Acquisition Process	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	
SA-4	Acquisition Process	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	5	
SA-4(CE-1)	Functional Properties of Controls	Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.	Functional	Intersects With	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security, compliance and resilience controls to be utilized within Technology Assets, Applications and/or Services (TAAS) in sufficient detail to permit analysis and testing of the controls.	5	
SA-4(CE-1)	Functional Properties of Controls	Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that:(1) Contain sufficient detail to assess the security of the network's architecture;(2) Reflect the current architecture of the network environment; and(3) Document all sensitive/regulated data flows.	5	
SA-4(CE-2)	Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; organization-defined design and implementation information for the security controls to be employed at sufficient level of detail to permit analysis and testing of controls.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that:(1) Contain sufficient detail to assess the security of the network's architecture;(2) Reflect the current architecture of the network environment; and(3) Document all sensitive/regulated data flows.	5	
SA-4(CE-2)	Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; organization-defined design and implementation information for the security controls to be employed at sufficient level of detail to permit analysis and testing of controls.	Functional	Intersects With	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
SA-4(CE-2)	Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; organization-defined design and implementation information for the security controls to be employed at sufficient level of detail to permit analysis and testing of controls.	Functional	Intersects With	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security, compliance and resilience controls to be utilized within Technology Assets, Applications and/or Services (TAAS) in sufficient detail to permit analysis and testing of the controls.	5	
SA-4(CE-8)	Continuous Monitoring Plan for Controls	Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the organization.	Functional	Subset Of	Continuous Monitoring Plan	TDA-09.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a plan for the continuous monitoring of security, compliance and/or resilience control effectiveness.	10	
SA-4(CE-9)	Functions, Ports, Protocols and Services in Use	Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.	Functional	Subset Of	Ports, Protocols & Services In Use	TDA-02.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended for use.	10	
SA-4(CE-12)	Data Ownership	Supplemental Guidance: The contactor must provide the agency with certification of destruction using NIST approved standards or certification that the data has been returned.	Functional	Intersects With	Personal Data (PD) Lineage	PRI-09	Mechanisms exist to maintain a process to document the lineage of Personal Data (PD) by recording how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes PD.	5	
SA-4(CE-12)	Data Ownership	Supplemental Guidance: The contactor must provide the agency with certification of destruction using NIST approved standards or certification that the data has been returned.	Functional	Intersects With	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	5	
SA-4(CE-12)	Data Ownership	Supplemental Guidance: The contactor must provide the agency with certification of destruction using NIST approved standards or certification that the data has been returned.	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	5	
SA-4(CE-12).a	Data Ownership	Include organizational data ownership requirements in the acquisition contract; and	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	5	
SA-4(CE-12).b	Data Ownership	Require all data to be removed from the contractor's system and returned to the organization within 7 calendar days prior to contract termination.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
SA-4(IRS-Defined)-1	N/A	Information systems that receive, process, store, access, protect and/or transmit FTI must be located, operated, and accessed within the United States. When a contract developer is used, agencies must document, through contract requirements, that all FTI systems (i.e., beyond commercial products used as components) are located within the United States and are developed physically within the United States by United States citizens or those with lawful resident status. Supplemental Guidance: This includes any contractor systems or cloud environments where FTI is received, processed, stored, accessed, protected and/or transmitted. See Section 2.C.7, Offshore Operations, for additional information.	Functional	Subset Of	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	10	
SA-4(IRS-Defined)-2	N/A	In acquiring information technology, agencies must use common security configurations, when applicable, by (a) requiring vendors to configure IT with common security configurations (when available and applicable, e.g., Center for Internet Security benchmarks) prior to delivery or (b) configuring acquired IT to meet agency-tailored, secure parameters (e.g., configurations that meet Publication 1075 and applicable SCSEM requirements) after delivery but prior to deployment. Supporting Guidance: In the latter case, agencies do not need to require that vendors securely configure IT for delivery.	Functional	Subset Of	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	10	
SA-5	System Documentation	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe:(1) Secure configuration, installation and operation of the TAAS;(2) Effective use and maintenance of security features/functions; and(3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5	
SA-5	System Documentation	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	5	
SA-8	Security Engineering Principles	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
SA-8	Security Engineering Principles	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	
SA-9	External System Services	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	10	
SA-9(CE-1)	Risk Assessments and Organizational Approvals	N/A	Functional	Subset Of	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	10	
SA-9(CE-1).a	Risk Assessments and Organizational Approvals	Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and	Functional	Subset Of	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	10	
SA-9(CE-1).b	Risk Assessments and Organizational Approvals	Verify that the acquisition or outsourcing of dedicated information security services is approved by a designated agency official.	Functional	Subset Of	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	10	
SA-9(CE-2)	Identification of Functions, Ports, Protocols and Services	Require providers of external information system services that process, store, or transmit FTI to identify the functions, ports, protocols, and other services required for the use of such services.	Functional	Subset Of	External Connectivity Requirements - Identification of Ports, Protocols & Services	TPM-04.2	Mechanisms exist to require External Service Providers (ESPs) to identify and document the business need for ports, protocols and other services it requires to operate its Technology Assets, Applications and/or Services (TAAS).	10	
SA-9(CE-3)	Establish and Maintain Trust Relationship with Providers	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: IRS Publication 1075 requirements for information systems that process, store, or transmit FTI.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
SA-9(CE-3)	Establish and Maintain Trust Relationship with Providers	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: IRS Publication 1075 requirements for information systems that process, store, or transmit FTI.	Functional	Intersects With	Conflict of Interests	TPM-04.3	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	5	
SA-9(CE-3)	Establish and Maintain Trust Relationship with Providers	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: IRS Publication 1075 requirements for information systems that process, store, or transmit FTI.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
SA-9(CE-3)	Establish and Maintain Trust Relationship with Providers	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: IRS Publication 1075 requirements for information systems that process, store, or transmit FTI.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to:(1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and(2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
SA-9(CE-3)	Establish and Maintain Trust Relationship with Providers	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: IRS Publication 1075 requirements for information systems that process, store, or transmit FTI.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	
SA-9(CE-3)	Establish and Maintain Trust Relationship with Providers	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: IRS Publication 1075 requirements for information systems that process, store, or transmit FTI.	Functional	Intersects With	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	5	
SA-9(CE-5)	Processing, Storage and Service Location	Restrict the location of accessing, processing, storage, transmission of FTI to The U.S. and territories based on IRS Publication 1075 requirements.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	
SA-9(CE-5)	Processing, Storage and Service Location	Restrict the location of accessing, processing, storage, transmission of FTI to The U.S. and territories based on IRS Publication 1075 requirements.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5	
SA-9(CE-5)	Processing, Storage and Service Location	Restrict the location of accessing, processing, storage, transmission of FTI to The U.S. and territories based on IRS Publication 1075 requirements.	Functional	Intersects With	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	5	
SA-9(CE-6)	Organization-Controlled Cryptographic Keys	Maintain exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system.	Functional	Subset Of	External System Cryptographic Key Control	CRY-09.7	Mechanisms exist to maintain control of cryptographic keys for encrypted material stored or transmitted through an external system.	10	
SA-9(CE-8)	Processing and Storage Location – U.S. Jurisdiction	Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.	Functional	Intersects With	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	5	
SA-9(CE-8)	Processing and Storage Location – U.S. Jurisdiction	Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	
SA-10	Developer Configuration Management	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Developer Configuration Management	TDA-14	Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation.	10	
SA-10(CE-1)	Software and Firmware Integrity Verification	Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components. Supplemental Guidance: Verification of the integrity of software and firmware can be accomplished though confirmation of the hash value. For example, checksums from well-known and safe hash functions. MD5 is not considered a safe hash function to use.	Functional	Subset Of	Software / Firmware Integrity Verification	TDA-14.1	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components.	10	
SA-10(CE-3)	Hardware Integrity Verification	Require the developer of the system, system component, or system service to enable integrity verification of hardware components.	Functional	Subset Of	Hardware Integrity Verification	TDA-14.2	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of hardware components.	10	
SA-10(CE-7)	Security and Privacy Representatives	Require agency designated security and privacy representatives to be included in the configuration change management and control process.	Functional	Subset Of	Security, Compliance & Resilience Representatives For Product Changes	TDA-02.7	Mechanisms exist to include appropriate security, compliance and resilience representatives in the product feature and/or functionality change control review process.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
SA-11	Developer Testing and Evaluation	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results.	10	
SA-11(CE-1)	Static Code Analysis	Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.	Functional	Subset Of	Static Code Analysis	TDA-09.2	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	10	
SA-11(CE-4)	Manual Code Reviews	Require the developer of the system, system component, or system service to perform a manual code review of FTI-related applications using the following processes, procedures, and/or techniques: agency-defined manual review process.	Functional	Subset Of	Manual Code Review	TDA-09.7	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ a manual code review process to identify and remediate unique flaws that require knowledge of the application's requirements and design.	10	
SA-11(CE-5)	Penetration Testing	Require the developer of the system, system component, or system service to perform penetration testing:	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	
SA-11(CE-5)	Penetration Testing	Require the developer of the system, system component, or system service to perform penetration testing:	Functional	Intersects With	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made Technology Assets, Applications and/or Services (TAAS).	5	
SA-11(CE-5)	Penetration Testing	Require the developer of the system, system component, or system service to perform penetration testing:	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results.	5	
SA-11(CE-5)	Penetration Testing	Require the developer of the system, system component, or system service to perform penetration testing:	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for:(1) Statutory, regulatory and contractual compliance obligations;(2) Monitoring capabilities;(3) Mobile devices;(4) Databases;(5) Application security;(6) Embedded technologies (e.g., IoT, OT, etc.);(7) Vulnerability management;(8) Malicious code;(9) Insider threats;(10) Performance/load testing; and/or(11) Artificial Intelligence and Autonomous Technologies (AAT).	5	
SA-11(CE-5)	Penetration Testing	Require the developer of the system, system component, or system service to perform penetration testing:	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
SA-11(CE-5).a	Penetration Testing	At the following level of rigor: at a minimum Whitebox testing; and	Functional	Subset Of	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	10	
SA-11(CE-5).b	Penetration Testing	Under the following constraints: where FTI is processed, stored, or transmitted.	Functional	Subset Of	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	10	
SA-11(CE-6)	Attack Surface Reviews	Require the developer of the system, system component, or system service to perform attack surface reviews.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results.	5	
SA-11(CE-6)	Attack Surface Reviews	Require the developer of the system, system component, or system service to perform attack surface reviews.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
SA-15	Development Process, Standards and Tools	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
SA-15(CE-3)	Criticality Analysis	Require the developer of the system, system component, or system service to perform a criticality analysis: Supplemental Guidance: This control enhancement provides developer input to the criticality analysis performed by agencies. Developer input is essential to such analysis because agencies may not have access to detailed design documentation for system components that are developed as commercial offthe-shelf products. Such design documentation includes, for example, functional specifications, high-level designs, low-level designs and source code and hardware schematics.	Functional	Subset Of	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	10	
SA-15(CE-3).a	Criticality Analysis	At the following decision points in the system development life cycle: the agency-defined breadth/depth; and	Functional	Subset Of	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	10	
SA-15(CE-3).b	Criticality Analysis	At the following level of rigor: post-design phases of the SDLC.	Functional	Subset Of	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	10	
SA-22	Unsupported System Components	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by:(1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and(2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5	
SA-22	Unsupported System Components	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Alternate Sources for Continued Support	TDA-17.1	Mechanisms exist to provide in-house support or contract external providers for support with unsupported Technology Assets, Applications and/or Services (TAAS).	5	
4.18	SYSTEM AND COMMUNICATIONS PROTECTION	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SC-1	System and Communications Protection Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
SC-1	System and Communications Protection Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
SC-1	System and Communications Protection Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
SC-1	System and Communications Protection Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
SC-2	Application Partitioning	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.	10	
SC-2(CE-1)	Interfaces for Non-Privileged Users	Prevent the presentation of system management functionality at interfaces to non-privileged users.	Functional	Subset Of	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.	10	
SC-4	Information in Shared System Resources	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Information In Shared Resources	SEA-05	Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.	10	
SC-7	Boundary Protection	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
SC-7(CE-3)	Access Points	Limit the number of external network connections to the system.	Functional	Subset Of	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its Technology Assets, Applications and/or Services (TAAS).	10	
SC-7(CE-4)	External Telecommunications Services	N/A	Functional	Subset Of	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	10	
SC-7(CE-4).a	External Telecommunications Services	Implement a managed interface for each external telecommunication service;	Functional	Subset Of	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	10	
SC-7(CE-4).b	External Telecommunications Services	Establish a traffic flow policy for each managed interface;	Functional	Subset Of	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	10	
SC-7(CE-4).c	External Telecommunications Services	Protect the confidentiality and integrity of the information being transmitted across each interface;	Functional	Subset Of	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	10	
SC-7(CE-4).d	External Telecommunications Services	Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;	Functional	Subset Of	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	10	
SC-7(CE-4).e	External Telecommunications Services	Review exceptions to the traffic flow policy at a minimum quarterly and remove exceptions that are no longer supported by an explicit mission or business need;	Functional	Subset Of	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	10	
SC-7(CE-4).f	External Telecommunications Services	Prevent unauthorized exchange of control plane traffic with external networks;	Functional	Subset Of	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	10	
SC-7(CE-4).g	External Telecommunications Services	Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and	Functional	Subset Of	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	10	
SC-7(CE-4).h	External Telecommunications Services	Filter unauthorized control plane traffic from external networks.	Functional	Subset Of	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	10	
SC-7(CE-5)	Deny by Default – Allow by Exception	Deny network communications traffic by default and allow network communications traffic by exception on information systems where FTI is accessed, processed, stored, or transmitted.	Functional	Subset Of	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
SC-7(CE-7)	Prevent Split Tunneling for Remote Devices	Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using:	Functional	Subset Of	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	10	
SC-7(CE-7).a	Prevent Split Tunneling for Remote Devices	Individual users shall not have the ability to configure split tunneling	Functional	Subset Of	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	10	
SC-7(CE-7).b	Prevent Split Tunneling for Remote Devices	Auditing must be performed semi-annually on each workstation with split tunneling enabled. Auditing must include:	Functional	Subset Of	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	10	
SC-7(CE-7).b.1	Prevent Split Tunneling for Remote Devices	Only those users authorized for split tunneling have it enabled in their user profile or policy object	Functional	Subset Of	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	10	
SC-7(CE-7).b.2	Prevent Split Tunneling for Remote Devices	There is a continued need for split tunneling for the user	Functional	Subset Of	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	10	
SC-7(CE-7).b.3	Prevent Split Tunneling for Remote Devices	Only the correct and authorized split tunneling configurations are present on the workstation	Functional	Subset Of	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	10	
SC-7(CE-7).c	Prevent Split Tunneling for Remote Devices	Host Checking is enabled and configured on the VPN server;	Functional	Subset Of	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	10	
SC-7(CE-7).c.1	Prevent Split Tunneling for Remote Devices	Ensure the OS is supported	Functional	Subset Of	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	10	
SC-7(CE-7).c.2	Prevent Split Tunneling for Remote Devices	Ensure that anti-malware is installed and up to date	Functional	Subset Of	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	10	
SC-7(CE-7).c.3	Prevent Split Tunneling for Remote Devices	The most current hotfixes are applied	Functional	Subset Of	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	10	
SC-7(CE-7).c.4	Prevent Split Tunneling for Remote Devices	Agency-defined additional parameters	Functional	Subset Of	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	10	
SC-7(CE-8)	Route Traffic to Authenticated Proxy Servers	Route internal communications traffic to external networks through authenticated proxy servers at managed interfaces. Supplemental Guidance: External networks are networks outside of organizational control. A proxy server is a server (i.e., system or application) that acts as an intermediary for clients requesting system resources from non-organizational or other organizational servers. These system resources can include, for example, files, connections, web pages or services. Client requests established through an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers providing access to the Internet. Proxy servers can support logging of individual Transmission Control Protocol sessions and blocking specific Uniform Resource Locators, Internet Protocol addresses and domain names. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites.	Functional	Intersects With	Route Internal Traffic to Proxy Servers	NET-18.1	Mechanisms exist to route internal communications traffic to external networks through organization-approved proxy servers at managed interfaces.	5	
SC-7(CE-8)	Route Traffic to Authenticated Proxy Servers	Route internal communications traffic to external networks through authenticated proxy servers at managed interfaces. Supplemental Guidance: External networks are networks outside of organizational control. A proxy server is a server (i.e., system or application) that acts as an intermediary for clients requesting system resources from non-organizational or other organizational servers. These system resources can include, for example, files, connections, web pages or services. Client requests established through an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers providing access to the Internet. Proxy servers can support logging of individual Transmission Control Protocol sessions and blocking specific Uniform Resource Locators, Internet Protocol addresses and domain names. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
SC-7(CE-9)	Restrict Threatening Outgoing Communications Traffic	N/A	Functional	Subset Of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
SC-7(CE-9).a	Restrict Threatening Outgoing Communications Traffic	Detect and deny outgoing communications traffic posing a threat to external systems; and	Functional	Subset Of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
SC-7(CE-9).b	Restrict Threatening Outgoing Communications Traffic	Audit the identity of internal users associated with denied communications.	Functional	Subset Of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	10
SC-7(CE-10)	Prevent Exfiltration	N/A	Functional	Subset Of	Prevent Unauthorized Exfiltration	NET-03.5	Automated mechanisms exist to prevent the unauthorized exfiltration of sensitive/regulated data across managed interfaces.	10	10
SC-7(CE-10).a	Prevent Exfiltration	Prevent the exfiltration of information; and	Functional	Subset Of	Prevent Unauthorized Exfiltration	NET-03.5	Automated mechanisms exist to prevent the unauthorized exfiltration of sensitive/regulated data across managed interfaces.	10	
SC-7(CE-10).b	Prevent Exfiltration	Conduct exfiltration tests at least semi-annually.	Functional	Subset Of	Prevent Unauthorized Exfiltration	NET-03.5	Automated mechanisms exist to prevent the unauthorized exfiltration of sensitive/regulated data across managed interfaces.	10	
SC-7(CE-11)	Restrict Incoming Communications Traffic	Only allow incoming communications from agencydefined authorized sources to be routed to agency-defined authorized destinations.	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	
SC-7(CE-11)	Restrict Incoming Communications Traffic	Only allow incoming communications from agencydefined authorized sources to be routed to agency-defined authorized destinations.	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
SC-7(CE-12)	Host-Based Protection	Implement firewalls and intrusion detection systems at access points and end user equipment as appropriate.	Functional	Subset Of	Host-Based Security Function Isolation	END-16.1	Mechanisms exist to implement underlying software separation mechanisms to facilitate security function isolation.	10	
SC-7(CE-15)	Networked Privileged Accesses	Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.	Functional	Subset Of	Route Privileged Network Access	NET-18.3	Automated mechanisms exist to route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.	10	
SC-7(CE-17)	Automated Enforcement of Protocol Format	Enforce adherence to protocol formats.	Functional	Subset Of	Web Application Firewall (WAF)	WEB-03	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.	10	
SC-7(CE-18)	Fail Secure	Prevent systems from entering unsecure states in the event of an operations failure of a boundary protection area.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	
SC-7(IRS-Defined)-1	N/A	Agencies shall implement and manage boundary protection (typically using firewalls) at trust boundaries. Each trust boundary shall be monitored and communications across each boundary shall be controlled. Supplemental Guidance: For the purposes of this requirement, trust boundary is defined as a border between two connected zones with different trust levels. Supplemental Guidance: This requirement is meant for border firewalls only. Internal firewalls used for network segmentation do not need to be stateful. Supplemental Guidance: This capability should be placed inline. Wherever possible, intrusion prevention capabilities should be utilized.	Functional	Subset Of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
SC-7(IRS-Defined)-2	N/A	Agencies must block known malicious sites (inbound or outbound), as identified to the agency from US-CERT, MS-ISAC or other sources, at each Internet Access Point (unless explicit instructions are provided to agencies not to block specific sites). Blocking is to be accomplished within two business days following release of such sites. Supplemental Guidance: US-CERT issues a monthly list of known malicious/suspicious sites as well as ad hoc notices as needed. MS-ISAC provides information to its member organizations about potential threat vectors as well. Supplemental Guidance: Malicious beaconing activity can sometimes be detected by enabling log capture on network devices such as proxies, DNS servers and routers to record a log of possible communications with specific domains. Creating logs allows an administrator to see precisely which internal network hosts are originating communications to those domains. The internal IP addresses responsible for the communications should be the first places for incident response and mitigation for removal of malware.	Functional	Subset Of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
SC-8	Transmission Confidentiality and Integrity	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
SC-8	Transmission Confidentiality and Integrity	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
SC-8(CE-1)	Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission.	Functional	Intersects With	Alternate Physical Protection	CRY-01.1	Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to physical safeguards.	5	
SC-8(CE-1)	Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
SC-8(CE-1)	Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
SC-8(IRS-Defined)	N/A	Agencies shall ensure appropriate transmission protections are in place commensurate with the highest sensitivity of information to be discussed over video and voice telecommunication and teleconferences. Supporting Guidance: Voice, video and multimedia communications can occur over traditional or digital telephone systems, cellular or other wireless networks or data networks. Transmitting voice, video, or multimedia communications over packet-switched networks (such as Local Area Networks) that were designed for data transfer rather than over dedicated circuit networks raises security concerns. Supporting Guidance: Wireless communications are vulnerable to interception, denial of service and deception. Under any circumstances, use of wireless to transmit or receive information sensitive to disclosure can present significant risks. When implementing this policy, bureaus should recognize the convergence of (point-to-point) PTP devices with those described.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
SC-8(IRS-Defined)	N/A	Agencies shall ensure appropriate transmission protections are in place commensurate with the highest sensitivity of information to be discussed over video and voice telecommunication and teleconferences. Supporting Guidance: Voice, video and multimedia communications can occur over traditional or digital telephone systems, cellular or other wireless networks or data networks. Transmitting voice, video, or multimedia communications over packet-switched networks (such as Local Area Networks) that were designed for data transfer rather than over dedicated circuit networks raises security concerns. Supporting Guidance: Wireless communications are vulnerable to interception, denial of service and deception. Under any circumstances, use of wireless to transmit or receive information sensitive to disclosure can present significant risks. When implementing this policy, bureaus should recognize the convergence of (point-to-point) PTP devices with those described.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
SC-10	Network Disconnect	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Network Connection Termination	NET-07	Mechanisms exist to terminate network connections at the end of a session or after an organization-defined time period of inactivity.	10	
SC-12	Cryptographic Key Establishment and Management	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	5	
SC-13	Cryptographic Protection	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
SC-13	Cryptographic Protection	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Export-Controlled Cryptography	CRY-01.2	Mechanisms exist to address the exporting of cryptographic technologies in compliance with relevant statutory and regulatory requirements.	5	
SC-13	Cryptographic Protection	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
SC-15	Collaborative Computing Devices and Applications	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Collaborative Computing Devices	END-14	Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions:(1) Networked whiteboards; (2) Video teleconference cameras; and(3) Teleconference microphones.	5	
SC-15(CE-4)	Explicitly Indicate Current Participants	Provide an explicit indication of current participants in meetings that involve FTI. Supplemental Guidance: Explicitly indicating current participants prevents unauthorized individuals from participating in collaborative computing sessions without the explicit knowledge of other participants.	Functional	Subset Of	Explicitly Indicate Current Participants	END-14.2	Automated mechanisms exist to provide an explicit indication of current participants in online meetings and teleconferences.	10	
SC-17	Public Key Infrastructure Certificates	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	5	
SC-18	Mobile Code	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
SC-18(CE-1)	Identify Unacceptable Code and Take Corrective Actions	Identify unacceptable mobile code and take corrective actions.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
SC-18(CE-1)	Identify Unacceptable Code and Take Corrective Actions	Identify unacceptable mobile code and take corrective actions.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
SC-18(CE-1)	Identify Unacceptable Code and Take Corrective Actions	Identify unacceptable mobile code and take corrective actions.	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5	
SC-18(CE-2)	Acquisition, Development and Use	Verify that the acquisition, development, and use of mobile code to be deployed in the system meets IRS Publication 1075 requirements.	Functional	Intersects With	Software Licensing Restrictions	AST-02.7	Mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions.	5	
SC-18(CE-2)	Acquisition, Development and Use	Verify that the acquisition, development, and use of mobile code to be deployed in the system meets IRS Publication 1075 requirements.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5	
SC-20(CE-2)	Data Origin and Integrity	Provide data origin and integrity protection artifacts for internal name/address resolution queries.	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5	
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	NET-10.2	Mechanisms exist to perform data origin authentication and data integrity verification on the Domain Name Service (DNS) resolution responses received from authoritative sources when requested by client systems.	10	
SC-22	Architecture and Provisioning for Name/Address Resolution Service	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Architecture & Provisioning for Name / Address Resolution Service	NET-10.1	Mechanisms exist to ensure systems that collectively provide Domain Name Service (DNS) resolution service are fault-tolerant and implement internal/external role separation.	10	
SC-23	Session Authenticity	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Session Integrity	NET-09	Mechanisms exist to protect the authenticity and integrity of communications sessions.	10	
SC-23(CE-1)	Invalidate Session Identifies at Logout	Invalidate session identifiers upon user logout or other session termination.	Functional	Subset Of	Invalidate Session Identifiers at Logout	NET-09.1	Automated mechanisms exist to invalidate session identifiers upon user logout or other session termination.	10	
SC-23(CE-3)	Unique System-Generate Session Identifiers	Generate a unique session identifier for each session with session with agency-defined randomness requirements and recognize only session identifiers that are system-generated Supplemental Guidance: Generating unique session identifiers curtails the ability of adversaries to reuse previously valid session IDs. Employing the concept of randomness in the generation of unique session identifiers protects against brute-force attacks to determine future session identifiers.	Functional	Subset Of	Unique System-Generated Session Identifiers	NET-09.2	Automated mechanisms exist to generate and recognize unique session identifiers for each session.	10	
SC-23(CE-5)	Allowed Certificate Authorities	Only allow the use of agency-defined certificate authorities for verification of the establishment of protected sessions.	Functional	Subset Of	Certificate Authorities	CRY-11	Automated mechanisms exist to enable the use of organization-defined Certificate Authorities (CAs) to facilitate the establishment of protected sessions.	10	
SC-28	Protection of Information at Rest	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
SC-28	Protection of Information at Rest	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
SC-28(CE-1)	Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage.	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
SC-28(CE-1)	Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
SC-28(CE-1)	Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
SC-28(CE-1)	Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage.	Functional	Intersects With	Encrypting Data In Storage Media	DCH-07.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	5	
SC-35	External Malicious Code Identification	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Honeyclients	SEA-12	Mechanisms exist to utilize honeyclients that proactively seek to identify malicious websites and/or web-based malicious code.	10	
SC-39	Process Isolation	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Process Isolation	SEA-04	Mechanisms exist to implement a separate execution domain for each executing process.	10	
SC-45	System Time Synchronization	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	5	
SC-45(CE-1)	System Time Synchronization	Synchronization with Authoritative Time Source:	Functional	Subset Of	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	10	
SC-45(CE-1).a	System Time Synchronization	Compare the internal system clocks daily with an agency-defined authoritative time source; and	Functional	Subset Of	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	10	
SC-45(CE-1).b	System Time Synchronization	Synchronize the internal system clocks to the authoritative time source when the time difference is greater than agency-defined time period.	Functional	Subset Of	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	10	
4.19	SYSTEM AND INFORMATION INTEGRITY	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SI-1	System and Information Integrity Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
SI-1	System and Information Integrity Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
SI-1	System and Information Integrity Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
SI-2	Flaw Remediation	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
SI-2	Flaw Remediation	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
SI-2	Flaw Remediation	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	
SI-2(CE-2)	Automated Flaw Remediation Status	Determine if system components have applicable securityrelevant software and firmware updates installed using automated mechanisms at a minimum monthly; daily for networked workstations and malicious code protection	Functional	Intersects With	Automated Remediation Status	VPM-05.2	Automated mechanisms exist to determine the state of system components with regard to flaw remediation.	5	
SI-2(CE-3)	Time to Remediate Flaws and Benchmarks for Corrective Actions	N/A	Functional	Subset Of	Time To Remediate / Benchmarks For Corrective Action	VPM-05.3	Mechanisms exist to track the effectiveness of remediation operations through metrics reporting.	10	
SI-2(CE-3).a	Time to Remediate Flaws and Benchmarks for Corrective Actions	Measure the time between flaw identification and flaw remediation; and	Functional	Subset Of	Time To Remediate / Benchmarks For Corrective Action	VPM-05.3	Mechanisms exist to track the effectiveness of remediation operations through metrics reporting.	10	
SI-2(CE-3).b	Time to Remediate Flaws and Benchmarks for Corrective Actions	Establish the following benchmarks for taking corrective actions: Agency defined based on criticality.	Functional	Subset Of	Time To Remediate / Benchmarks For Corrective Action	VPM-05.3	Mechanisms exist to track the effectiveness of remediation operations through metrics reporting.	10	
SI-2(CE-4)	Automated Patch Management Tools	Employ automated patch management tools to facilitate flaw remediation to all FTI systems that includes but not limited to mainframes, workstations, applications, and network components	Functional	Intersects With	Automated Remediation Status	VPM-05.2	Automated mechanisms exist to determine the state of system components with regard to flaw remediation.	5	
SI-2(CE-4)	Automated Patch Management Tools	Employ automated patch management tools to facilitate flaw remediation to all FTI systems that includes but not limited to mainframes, workstations, applications, and network components	Functional	Intersects With	Automated Software & Firmware Updates	VPM-05.4	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
SI-2(CE-4)	Automated Patch Management Tools	Employ automated patch management tools to facilitate flaw remediation to all FTI systems that includes but not limited to mainframes, workstations, applications, and network components	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	
SI-2(CE-4)	Automated Patch Management Tools	Employ automated patch management tools to facilitate flaw remediation to all FTI systems that includes but not limited to mainframes, workstations, applications, and network components	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
SI-2(CE-5)	Automatic Software and Firmware Updates	Install security-relevant software and firmware updates automatically to all FTI systems.	Functional	Intersects With	Automated Software & Firmware Updates	VPM-05.4	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.	5	
SI-2(CE-6)	Removal of Previous Versions of Software and Firmware	Remove previous versions of security relevant software and firmware components after updated versions have been installed.	Functional	Subset Of	Removal of Previous Versions	VPM-05.5	Mechanisms exist to remove old versions of software and firmware components after updated versions have been installed.	10	
SI-2(IRS-Defined)	N/A	The agency shall ensure that, upon daily power up and connection to the agency's network, workstations (as defined in policy and including remote connections using GFE workstations) are checked to ensure that the most recent agency-approved patches have been applied and that any absent or new patches are applied as necessary or otherwise checked not less than once every 24 hours (excluding weekends, holidays, etc.)	Functional	Subset Of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	10	
SI-3	Malicious Code Protection	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
SI-3	Malicious Code Protection	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
SI-3	Malicious Code Protection	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
SI-3	Malicious Code Protection	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5	
SI-3	Malicious Code Protection	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
SI-3	Malicious Code Protection	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	
SI-3	Malicious Code Protection	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
SI-3(IRS-Defined)-1	N/A	All removable media must be scanned for malicious code upon introduction of the media into any system on the network and before users may access the media.	Functional	Subset Of	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	10	
SI-3(IRS-Defined)-2	N/A	Not less than daily, the agency shall check for updates to malicious code scanning tools, including anti-virus (AV) and anti-spyware software and intrusion detection tools and when updates are available, implement on all devices on which such tools reside.	Functional	Subset Of	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	10	
SI-4	System Monitoring	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
SI-4	System Monitoring	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
SI-4	System Monitoring	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
SI-4	System Monitoring	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
SI-4(CE-1)	System-wide Intrusion Detection System	Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.	Functional	Subset Of	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	10	
SI-4(CE-2)	Automated Tools and Mechanisms for Real-Time Analysis	Employ automated tools and mechanisms to support near real-time analysis of events. Supplemental Guidance: Automated tools and mechanisms include, for example, host-based, networkbased, transport-based, or storage-based event monitoring tools and mechanisms or Security Information and Event Management technologies that provide real-time analysis of alerts and notifications generated by organizational systems.	Functional	Subset Of	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	10	
SI-4(CE-4)	Inbound and Outbound Communications Traffic	N/A	Functional	Subset Of	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	10	
SI-4(CE-4).a	Inbound and Outbound Communications Traffic	Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;	Functional	Subset Of	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	10	
SI-4(CE-4).b	Inbound and Outbound Communications Traffic	Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions.	Functional	Subset Of	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	10	
SI-4(CE-5)	System-Generated Alerts	Alert the appropriate agency personnel when the following system generated indications of compromise or potential compromise occur: suspicious activity reported from firewalls, intrusion detection systems, malware detection systems, and other agency-defined security tools that report indications of compromise or potential compromise. Supplemental Guidance: Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated, or they may be transmitted, for example, telephonically, by electronic mail messages or by text messaging. Organizational personnel on the alert notification list can include, for example, system administrators, mission or business owners, system owners, system security officers or privacy officers. This control enhancement focuses on the security alerts generated by the system. Alternatively, alerts generated by organizations in SI-4(12) focus on information sources external to the system such as suspicious activity reports and reports on potential insider threats.	Functional	Subset Of	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	10	
SI-4(CE-10)	Visibility of Encrypted Communications	Make provisions so that agency-defined encrypted communications traffic is visible to agency-defined system monitoring tools and mechanisms. Supplemental Guidance: Organizations balance the need to encrypt communications traffic to protect data confidentiality with the need to maintain visibility into such traffic from a monitoring perspective. Organizations determine whether the visibility requirement applies to internal encrypted traffic, encrypted traffic intended for external destinations, or a subset of the traffic types.	Functional	Subset Of	Visibility of Encrypted Communications	NET-18.2	Mechanisms exist to configure the proxy to make encrypted communications traffic visible to monitoring tools and mechanisms.	10	
SI-4(CE-11)	Analyze Communications Traffic Anomalies	Analyze outbound communications traffic at the external interfaces to the system and selected agency defined interior points within the system to discover anomalies. Supplemental Guidance: Agency defined interior points include subnetworks and subsystems. Anomalies within agency systems include large file transfers, long-time persistent connections, attempts to access information from unexpected locations, the use of unusual protocols and ports, the use of unmonitored network protocols (e.g., IPv6 usage during IPv4 transition) and attempted communications with suspected malicious external addresses.	Functional	Subset Of	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	10	
SI-4(CE-12)	Automated Organization-Generated Alerts	Alert agency-defined personnel or roles using automated mechanisms when the following indications of inappropriate or unusual activities with security or privacy implications occur: agency-defined activities that trigger events.	Functional	Intersects With	Automated Alerts	MON-01.12	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.	5	
SI-4(CE-12)	Automated Organization-Generated Alerts	Alert agency-defined personnel or roles using automated mechanisms when the following indications of inappropriate or unusual activities with security or privacy implications occur: agency-defined activities that trigger events.	Functional	Intersects With	Real-Time Alerts of Event Logging Failure	MON-05.1	Mechanisms exist to provide 24x7x365 near real-time alerting capability when an event log processing failure occurs.	5	
SI-4(CE-18)	Analyze Traffic and Covert Exfiltration	Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information at agency defined interior points within the system.	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
SI-4(CE-18)	Analyze Traffic and Covert Exfiltration	Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information at agency defined interior points within the system.	Functional	Intersects With	Analyze Traffic for Covert Exfiltration	MON-11.1	Automated mechanisms exist to analyze network traffic to detect covert data exfiltration.	5	
SI-4(CE-24)	Indicators of Compromise	Discover, collect, and distribute to organization-defined personnel or roles, indicators of compromise provided by government and non-government sources.	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5	
SI-4(CE-24)	Indicators of Compromise	Discover, collect, and distribute to organization-defined personnel or roles, indicators of compromise provided by government and non-government sources.	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications.	5	
SI-4(IRS-Defined)	N/A	All Internet Access Points/portals shall capture and retain, for at least one year, inbound and outbound traffic header information, with the exclusion of approved Internet "anonymous" connections, as may be approved by the agency CISO. Supplemental Guidance: If/when this information is captured and retained (one year) by DHS via Project Einstein (or a similar service) (for the Internet access point at hand) duplicative capturing/retention is not required.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
SI-5	Security Alerts, Advisories and Directives	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
SI-5	Security Alerts, Advisories and Directives	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
SI-5	Security Alerts, Advisories and Directives	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
SI-7	Software, Firmware and Information Integrity	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	5	
SI-7	Software, Firmware and Information Integrity	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
SI-7	Software, Firmware and Information Integrity	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
SI-7(CE-1)	Integrity Checks	Perform an integrity check of software, firmware, and information at startup; at the identification of a new threat to which the information system is susceptible; the installation of new hardware, software, or firmware; or at a minimum annually.	Functional	Subset Of	Integrity Checks	END-06.1	Mechanisms exist to validate configurations through integrity checking of software and firmware.	10	
SI-7(CE-7)	Integration of Detection and Response	Incorporate the detection of the following unauthorized changes into the organizational incident response capability:	Functional	Subset Of	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
SI-7(CE-7).a	Integration of Detection and Response	Unauthorized changes to baseline configuration setting; and	Functional	Subset Of	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	10	
SI-7(CE-7).b	Integration of Detection and Response	Unauthorized elevation of system privileges.	Functional	Subset Of	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	10	
SI-7(CE-10)	Protection of Boot Firmware	Implement the following mechanisms to protect the integrity of boot firmware in system where FTI is accessed, processed, stored, and transmitted: verifying the checksum of downloaded firmware.	Functional	Subset Of	Protection of Boot Firmware	END-06.6	Automated mechanisms exist to protect the integrity of boot firmware in systems.	10	
SI-8	Spam Protection	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	10	
SI-8(CE-2)	Automatic Updates	Automatically update spam protection mechanisms at a minimum quarterly.	Functional	Subset Of	Automatic Spam and Phishing Protection Updates	END-08.2	Mechanisms exist to automatically update anti-phishing and spam protection technologies when new releases are available in accordance with configuration and change management practices.	10	
SI-10	Information Input Validation	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
SI-10	Information Input Validation	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
SI-11	Error Handling	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Error Handling	TDA-19	Mechanisms exist to handle error conditions by:(1) Identifying potentially security-relevant error conditions;(2) Generating error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited; and(3) Revealing error messages only to authorized personnel.	10	
SI-12	Information Management and Retention	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
SI-12	Information Management and Retention	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to:(1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law;(2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and(3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
SI-12(CE-2)	Minimize Personally identifiable Information in Testing, Training, and Research	Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: Submission of the DTR form for review and approval by IRS Office of Safeguards.	Functional	Intersects With	Limit Sensitive / Regulated Data In Testing, Training & Research	DCH-18.2	Mechanisms exist to minimize the use of sensitive/regulated data for research, testing, or training, in accordance with authorized, legitimate business practices.	5	
SI-12(CE-2)	Minimize Personally identifiable Information in Testing, Training, and Research	Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: Submission of the DTR form for review and approval by IRS Office of Safeguards.	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that:(1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and(2) Authorizes the use of PD when such information is required for internal testing, training and research.	5	
SI-16	Memory Protection	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Memory Protection	SEA-10	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	10	
4.20	SUPPLY CHAIN RISK MANAGEMENT	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SR-1	Supply Chain Risk Management Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
SR-1	Supply Chain Risk Management Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
SR-1	Supply Chain Risk Management Policy and Procedures	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
SR-2	Supply Chain Risk Management Plan	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
SR-2	Supply Chain Risk Management Plan	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to:(1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and(2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
SR-2(CE-1)	Establish SCRM Team	Establish a supply chain risk management team consisting of agencydefined personnel to lead and support the following SCRM activities: provide expertise in acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects and dependencies of systems.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to:(1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and(2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
SR-3	Supply Chain Controls and Processes	See FDE for specific NIST SP 800-53 control details.	Functional	Subset Of	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	10	
SR-3(CE-2)	Limitation of Harm	Employ the following controls to limit harm from potential adversaries identifying and targeting the organizational supply chain: agency-defined controls. Supplemental Guidance: Controls that can be implemented to reduce the probability of adversaries successfully identifying and targeting the supply chain include avoiding the purchase of custom or nonstandardized configurations, employing approved vendor lists with standing reputations in industry, following pre-agreed maintenance schedules and update and patch delivery mechanisms, maintaining a contingency plan in case of a supply chain event, using procurement carve-outs that provide exclusions to commitments or obligations, using diverse delivery routes, and minimizing the time between purchase decisions and delivery.	Functional	Subset Of	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	10	
SR-3(CE-3)	Sub-Tier Flow Down	Ensure that the controls included in the contracts of prime contractors are also included in the contracts of s.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
SR-3(CE-3)	Sub-Tier Flow Down	Ensure that the controls included in the contracts of prime contractors are also included in the contracts of s.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
SR-6	Supplier Assessments and Reviews	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5	
SR-10	Inspection of Systems and Components	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5	
SR-10	Inspection of Systems and Components	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Technology Asset Inspections	AST-15.1	Mechanisms exist to physically and logically inspect critical technology assets to detect evidence of tampering.	5	
SR-11	Component Authenticity	See FDE for specific NIST SP 800-53 control details.	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5	
SR-11(CE-1)	Anti-Counterfeit Training	Train agency-defined personnel or roles to detect counterfeit system components (including hardware, software, and firmware).	Functional	Subset Of	Anti-Counterfeit Training	TDA-11.1	Mechanisms exist to train personnel to detect counterfeit system components, including hardware, software and firmware.	10	
SR-11(CE-2)	Configuration Control for Component Service and Repair	Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: hardware used to receive, access, process, store, transmit or protect FTI.	Functional	Subset Of	Maintain Configuration Control During Maintenance	MNT-07	Mechanisms exist to maintain proper physical security and configuration control over technology assets awaiting service or repair.	10	