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: National Industrial Security Program Operating Manual (NISPOM) (2020)
Focal Document URL: https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-nispom-2020.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
§117.1(a)	Purpose.	(a) This part implements policy, assigns responsibilities, establishes requirements, and provides procedures, consistent with E.O. 12829, "National Industrial Security Program"; E.O. 10865, "Safeguarding Classified Information within Industry"; 32 CFR part 2004; and DoD Instruction (DoDI) 5220.22, " NISP" (available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/522022p.pdf?ver=2018-05-01-073158-710) for the protection of classified information that is disclosed to, or developed by contractors, licensees, grantees, and certificate holders of the U.S. Government (USG) (referred to in this part as contractors).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.1(b)	Purpose.	(b) This part, also in accordance with E.O. 12829, E.O. 13587,"Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information"; E.O. 13691, "Promoting Private Sector Cybersecurity Information Sharing"; E.O. 12333, "United States Intelligence Activities"; 42, U.S.C. 2011 et seq. (also known as and referred to in this part as the "(AEA) of 1954, as amended); " 50 U.S.C. Ch. 44 (also known as the "National Security Act of 1947," as amended); 50 U.S.C. 3501 et seq. (also known as the "Central Intelligence Agency Act of 1949," as amended); Pub. L. 108-458 (also known as the "Intelligence Reform and Terrorism Prevention Act of 2004"); and 32 CFR part 2004:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.1(b)(1)	Purpose.	(1) Prescribes industrial security procedures and practices, under E.O. 12829 or successor orders, to safeguard USG classified information that is developed by or disclosed to contractors, licensees, and grantees of the USG.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.1(b)(2)	Purpose.	(2) Prescribes requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information and protect special classes of classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.1(b)(3)	Purpose.	(3) Prescribes that contractors will implement the provisions of this part no later than 6 months from the effective date of this part and after any future published changes.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.2(a)	Applicability.	(a) This part applies to:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.2(a)(1)	Applicability.	(1) The Office of the Secretary of Defense, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this part as the "DoD Components").	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.2(a)(2)	Applicability.	(2) All executive branch departments and agencies.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.2(a)(3)	Applicability.	(3) All industrial, educational, commercial, or other non-USG entities granted access to classified information by the USG executive branch departments and agencies or by foreign governments.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.2(a)(4)	Applicability.	(4) The release of classified information by the USG to contractors, who are required to safeguard classified information released during all phases of the contracting, licensing, and grant process, including the preparation and submission of bids and proposals, negotiation, award, performance, and termination. It also applies to classified information not released under a contract, license, certificate or grant, and to FGI furnished to contractors that requires protection in the interest of national security.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.2(b)	Applicability.	(b) This part does not:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.2(b)(1)	Applicability.	(1) Limit in any manner the authority of USG executive branch departments and agencies to grant access to classified information under the cognizance of their department or agency to any individual designated by them. The granting of such access is outside the scope of the NISP and is accomplished pursuant to E.O. 12968, E.O. 13526, E.O. 13691, the AEA, and applicable disclosure policies.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.2(b)(2)	Applicability.	(2) Apply to criminal proceedings in the courts or authorize contractors or their employees to disclose classified information in connection with any criminal proceedings. Defendants and their representative in criminal proceedings in U.S. District Courts, Courts of Appeal, and the U.S. Supreme Court may gain access to classified information in accordance with 18 U.S.C. Appendix 3, Section 1, also known as and referred to in this part as the "Classified Information Procedures Act," as amended.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.3(a)	Acronyms and Definitions.	(a) Acronyms. Unless otherwise noted, these acronyms and their terms are for the purposes of this part.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.3(b)	Acronyms and Definitions.	(b) Definitions. Unless otherwise noted, these terms and their definitions are for the purposes of this part.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.4n/a	Policy.	E.O. 12829 established the NISP to serve as a single, integrated, cohesive industrial security program to protect classified information and preserve our Nation's economic and technological interests.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.4(a)	Policy.	(a) When contracts, licenses, agreements, and grants to contractors require access to classified information, national security requires that this information be safeguarded in a manner equivalent to its protection within the executive branch of the USG.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.4(b)	Policy.	(b) National security requires that the industrial security program promote the economic and technological interests of the United States. Redundant, overlapping, or unnecessary requirements impede those interests.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.5n/a	Information collections.	The information collection requirements are:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.5(a)	Information collections.	(a) Standard Form (SF) 328 "Certificate Pertaining to Foreign Interest" (available at: https://www.gsa.gov/forms-library/certificate-pertaining-foreign-interests) in and , is assigned Office of Management and Budget (OMB) Control Number 0704-0579. The expiration date of this information collection is listed in the DoD Information Collections System at https://apps.sp.pentagon.mil/sites/dodiic/Pages/default.aspx.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.5(b)	Information collections.	(b) NRC collection. "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data," is assigned OMB Control Number: 3150-0047. Under this collection, NRC-regulated facilities and other organizations are required to provide information and maintain records to ensure that an adequate level of protection is provided to NRC-classified information and material.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.5(c)	Information collections.	(c) DOE collection. "Security," a NISP CSA information collection, is assigned OMB Control Number: 1910-1800. This information collection, which includes facility security clearance information, is used by the DOE to exercise management, oversight, and control over its contractors' management and operation of DOE's Government-owned contractor-operated facilities, and over its offsite contractors. The contractor management, oversight, and control functions relate to the ways in which DOE contractors provide goods and services for DOE organizations and activities in accordance with the terms of their contracts and the applicable statutory, regulatory, and mission support requirements of the Department. Information collected from private industry and private individuals is used to protect national security and critical assets entrusted to the Department.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.5(d)	Information collections.	(d) DoD collection. "National Industrial Security System," a CSA information collection, is assigned OMB Control Number: 0704-0571. Department of Defense (DD) Form 254, "Contract Security Classification Specification," (available at: https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd0254.pdf), is assigned OMB Control Number 0704-0567 in accordance with the procedures in Volume 2 of DoD Manual (available at: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022_vol2.pdf?ver=2018-08-01-114445-000) and (DoDM) 8910.01, "DoD Information Collections Manual: Procedures for DoD Public Information Collections" (available at: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/891001m_vol2.pdf?ver=2017-06-20-125411-733). The expiration date of this information collection is listed in the DoD Information Collections System at https://apps.sp.pentagon.mil/sites/dodiic/Pages/default.aspx.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.5(e)	Information collections.	(e) CIA collection. The CIA is exempt from reporting information collections for the purposes of this part in accordance with paragraph 8.a. (2)(d) of Enclosure 3 of Volume 2 of DoDM 8910.01 (available at: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/891001m_vol2.pdf?ver=2017-06-20-125411-733).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(a)	Responsibilities.	(a) Under Secretary of Defense for Intelligence & Security (USD(I&S)). The USD(I&S), on behalf of the Secretary of Defense, and in accordance with E.O. 12829, 32 CFR part 2004, and DoDI 5220.22:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(a)(1)	Responsibilities.	(1) Carries out the direction in section 201 of E.O. 12829 that the Secretary of Defense issue and maintain this part and changes to it. USD(I&S) does so in consultation with all affected agencies (E.O. 12829 section 201), with the concurrence of the Secretary of Energy, the Chairman of the NRC, the DNI, and the Secretary of Homeland Security (E.O.12829 section 201), and in consultation ISOO (E.O. 12829 section 102).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(a)(2)	Responsibilities.	(2) Acts as the CSA for DoD.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(a)(3)	Responsibilities.	(3) Provides policy and management of the NISP for non-DoD executive branch agencies who enter into inter-agency security agreements with DoD to provide industrial security services required when classified information is disclosed to contractors in accordance with E.O. 12829, as amended.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(b)	Responsibilities.	(b) Director, DCSA. Under the authority, direction, and control of the USD(I&S), and in accordance with DoDI 5220.22 and DoD Directive (DoDD) 5105.42, "Defense Security Service (DSS)" (available at: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/510542p.pdf?ver=2019-01-14-090012-283) the Director, DCSA:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(b)(1)	Responsibilities.	(1) Oversees and manages DCSA, which serves as the DoD CSO.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(b)(2)	Responsibilities.	(2) Administers the NISP as a separate program element on behalf of DoD GCAs and those agencies with agreements with DoD for security services.	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
§117.6(b)(3)	Responsibilities.	(3) Provides security oversight of the NISP as the DoD CSO on behalf of DoD components and those non-DoD executive branch agencies who enter into agreements with DoD as noted in paragraph (a)(3) of this section. The Director, DCSA, will be relieved of this oversight function for DoD special access programs (SAPs) when the Secretary of Defense or the Deputy Secretary of Defense approves a carve-out provision in accordance with DoDD 5205.07, "DoD SAP Policy" (available at: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520507p.pdf?ver=2020-02-04-142942-827).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(c)	Responsibilities.	(c) Secretary of Energy. In addition to the responsibilities in paragraph (h) of this section, the Secretary of Energy:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(c)(1)	Responsibilities.	(1). Prescribes procedures for the portions of this part pertaining to information classified under the AEA (i.e., (RD), (FRD), and TFNI).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(c)(2)	Responsibilities.	(2) Retains authority over access to information classified under the AEA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(c)(3)	Responsibilities.	(3) Inspects and monitors contractor, licensee, certificate holder, and grantee programs and facilities that involve access to information classified under the AEA, as necessary.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(d)	Responsibilities.	(d) Chairman of the NRC. In addition to the responsibilities in paragraph (h) of this section, the Chairman of the NRC:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(d)(1)	Responsibilities.	(1) Prescribes procedures for the portions of this part that pertain to information classified under the AEA to include functions overseeing reactor safety and security; administering reactor licensing and renewal; licensing radioactive materials; radionuclide safety; and managing the storage, security, recycling, and disposal of spent fuel.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(d)(2)	Responsibilities.	(2) Retains authority over access to information under NRC programs classified under the AEA and 10 CFR part 95.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(d)(3)	Responsibilities.	(3) Inspects and monitors contractor, licensee, certificate holder, and grantee programs and facilities that involve access to information under NRC programs classified pursuant to the AEA and 10 CFR part 95 where appropriate.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(e)	Responsibilities.	(e) Director of National Intelligence. In addition to the responsibilities in paragraph (h) of this section, the Director of National Intelligence:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(e)(1)	Responsibilities.	(1) Prescribes procedures for the portions of this part pertaining to intelligence sources, methods, and activities, including, but not limited to, SCI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(e)(2)	Responsibilities.	(2) Retains authority over access to intelligence sources, methods, and activities, including SCI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(e)(3)	Responsibilities.	(3) Provides guidance on the security requirements for intelligence sources and methods of information, including, but not limited to, SCI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(f)	Responsibilities.	(f) Secretary of Homeland Security. In accordance with E.O. 12829, E.O. 13691, and in addition to the responsibilities in paragraph (h) of this section, the Secretary of Homeland Security:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(f)(1)	Responsibilities.	(1) Prescribes procedures for the portions of this part that pertain to the CCIPP.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(f)(2)	Responsibilities.	(2) Retains authority over access to information under the CCIPP.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(f)(3)	Responsibilities.	(3) Inspects and monitors contractor, licensee, certificate holder, and grantee programs and facilities that involve access to CCIPP.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(g)	Responsibilities.	(g) All the CSA heads. The CSA heads:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(g)(1)	Responsibilities.	(1) Oversee the security of classified contracts and activities under their purview.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(g)(2)	Responsibilities.	(2) Provide oversight of contractors under their security cognizance.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(g)(3)	Responsibilities.	(3) Minimize redundant and duplicative security review and audit activities of contractors, including such activities conducted at contractor locations where multiple CSAs have equities.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(g)(4)	Responsibilities.	(4) Execute appropriate intra-agency and inter-agency agreements to avoid redundant and duplicate reviews.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(g)(5)	Responsibilities.	(5) Designate one or more CSOs for security administration.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(g)(6)	Responsibilities.	(6) Designate subordinate officials, in accordance with governing policies, to act as the authorizing official. Authorizing officials will:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(g)(6)(i)	Responsibilities.	(i) Assess and authorize contractors to process classified information on information systems.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(g)(6)(ii)	Responsibilities.	(ii) Conduct oversight of such information system processing, and provide information system security guidelines in accordance with Federal information system security control policies, standards, and procedures. Minimize redundant and duplicative security review and audit activity of contractors, including such activity conducted at contractor locations where multiple CSAs have equities.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(h)	Responsibilities.	(h) Component heads. In accordance with applicable CSA direction, the component heads:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(h)(1)	Responsibilities.	(1) Oversee compliance with procedures identified by the applicable CSA or designated CSO..	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(h)(2)	Responsibilities.	(2) Provide oversight of contractor personnel visiting or working on USG installations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(h)(3)	Responsibilities.	(3) Promptly apprise the CSO of information received or developed that could adversely affect a cleared contractor, licensee, or grantee, and their employees, to hold an FCL or PCL, or that otherwise raises substantive doubt about their ability to safeguard classified information entrusted to them.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(h)(4)	Responsibilities.	(4) Propose changes to this part as deemed appropriate and provide them to the applicable CSA for submission to the OUSD(I&S) Counterintelligence, Law Enforcement and Security Directorate.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(i)	Responsibilities.	(i) Director, ISOO. The Director, ISOO:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(i)(1)	Responsibilities.	(1) Oversees the NSIP and agency compliance with it, in accordance with E.O. 12829.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(i)(2)	Responsibilities.	(2) Issues and maintains the NISP implementing directive (32 CFR part 2004), in accordance with E.O. 12829, to provide guidance to the CSAs and USG agencies under the NISP.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.6(i)(3)	Responsibilities.	(3) Chairs the NISP Policy Advisory Committee. Addresses complaints and suggestions from contractors, as detailed in the NISP Policy Advisory Committee bylaws.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (a)	Procedures.	(a) General. Contractors will protect all classified information that they are provided access to or that they possess. This responsibility applies at both contractor and USG locations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)	Procedures.	(b) Contractor Security Officials. Contractors will appoint security officials who are U.S. citizens, except in exceptional circumstances (see § 117.9(m) and § 117.11(e)).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(1)	Procedures.	(1) Appointed security officials listed in paragraphs (b)(2), (b)(3), and (b)(4) of this section must:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(1)(i)	Procedures.	(i) Oversee the implementation of the requirements of this rule. Depending upon the size and complexity of the contractor's security operations, a single contractor employee may serve in more than one position.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(1)(ii)	Procedures.	(ii) Undergo the same security training that is required for all other contractor employees pursuant to §117.12, in addition to their position specific training.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(1)(iii)	Procedures.	(iii) Be designated in writing with their designation documented in accordance with CSA guidance.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(1)(iv)	Procedures.	(iv) Undergo a personnel security investigation and national security eligibility determination for access to classified information at the level of the entity's eligibility determination for access to classified information (e.g., FCL level) and be on the KMP list for the cleared facility.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(2)	Procedures.	(2) SMO. The SMO is the contractor's official responsible for the entity policy and strategy. The SMO is an entity employee occupying a position in the entity with ultimate authority over the facility's operations and the authority to direct actions necessary for the safeguarding of classified information in the facility. This includes the authority to direct actions necessary to safeguard classified information when the access to classified information by the facility's employees is solely at other contractor facilities or USG locations. The SMO will:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(2)(i)	Procedures.	(i) Ensure the contractor maintains a system of security controls in accordance with the requirements of this part.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(2)(ii)	Procedures.	(ii) Appoint a contractor employee or employees, in writing, as the FSO and appoint the same employee or a different employee as the ITPSO. The SMO may appoint a single employee for both roles or may appoint one employee as the FSO and a different employee as the ITPSO.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(2)(iii)	Procedures.	(iii) Remain fully informed of the facility's classified operations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(2)(iv)	Procedures.	(iv) Make decisions based on classified threat reporting and their thorough knowledge, understanding, and appreciation of the threat information and the potential impacts caused by a loss of classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(2)(v)	Procedures.	(v) Retain accountability for the management and operations of the facility without delegating that accountability to a subordinate manager.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(3)	Procedures.	(3) FSO. The FSO will:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(3)(i)	Procedures.	(i) Supervise and direct security measures necessary for implementing the applicable requirements of this part and the related USG security requirements to ensure the protection of classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(3)(ii)	Procedures.	(ii) Complete security training pursuant to §117.12 and as deemed appropriate by the CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(4)	Procedures.	(4) ITPSO. The ITPSO will establish and execute an insider threat program.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(4)(i)	Procedures.	(i) If the appointed ITPSO is not also the FSO, the ITPSO will ensure that the FSO is an integral member of the contractor's insider threat program.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(4)(ii)	Procedures.	(ii) The ITPSO will complete training pursuant to §117.12.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(4)(iii)	Procedures.	(iii) An entity family may choose to establish an entity family-wide insider threat program with one senior official appointed, in writing, to establish, and execute the program as the ITPSO. Each cleared entity using the entity-wide ITPSO must separately appoint that person as its ITPSO for that facility. The ITPSO will provide an implementation plan to the CSA for executing the insider threat program across the entity family.	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
§117.7 (b)(5)	Procedures.	(5) ISSM. Contractors who are, or will be, processing classified information on an information system located at the contractor facility will appoint an employee to serve as the ISSM. The ISSM must be eligible for access to classified information to the highest level of the information processed on the system(s) under their responsibility. The contractor will ensure that the ISSM is adequately trained and possesses technical competence commensurate with the complexity of the contractor's classified information system. The contractor will notify the applicable CSA if there is a change in the ISSM. The ISSM will oversee development, implementation, and evaluation of the contractor's classified information system program. ISSM responsibilities are in § 117.18.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (b)(6)(i)	Procedures.	(6) Employees performing security duties. Those employees whose official duties include performance of NISP- related security functions will complete security training tailored to the security functions performed. This training requirement also applies to consultants whose official duties include security functions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (c)	Procedures.	(c) Other KMP. In addition to the SMO, the FSO, and the ITPSO, the contractor will include on the KMP list, subject to CSA concurrence, any other officials who either hold majority interest or stock in the entity, or who have direct or indirect authority to influence or decide issues affecting the management or operations of the contractor or issues affecting classified contract performance. The CSA may either:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (c)(1)	Procedures.	(1) Require these KMP to be determined to be eligible for access to classified information as a requirement for the entity's eligibility determination or;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (c)(2)	Procedures.	(2) Allow the entity to formally exclude these KMP from access to classified information. The entity's governing board will affirm the exclusion by issuing a formal action (see table), and provide a copy of the exclusion action to the CSA. The entity's governing board will document this exclusion action. See TABLE 1 TO PARAGRAPH (c)(2)—EXCLUSION RESOLUTIONS	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (d)	Procedures.	(d) Insider Threat Program. Pursuant to this rule and CSA provided guidance to supplement unique CSA mission requirements, the contractor will establish and maintain an insider threat program to gather, integrate, and report relevant and available information indicative of a potential or actual insider threat, consistent with E.O. 13587 and Presidential Memorandum ''National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.''	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (e)	Procedures.	(e) Standard practice procedures. The contractor will implement all applicable provisions of this rule at each of its cleared facility locations. The contractor will prepare written procedures when the CSA determines them to be necessary to reasonably exclude the possibility of loss or compromise of classified information, and in accordance with additional CSA- provided guidance, as applicable.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (f)	Procedures.	(f) Cooperation with Federal agencies. Contractors will cooperate with Federal agencies and their officially credentialed USG or contractor representatives during official reviews, investigations concerning the protection of classified information, or personnel security investigations of present or former employees and others (e.g., consultants or visitors). At a minimum, cooperation includes:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (f)(1)	Procedures.	(1) Providing suitable arrangements within the facility for conducting private interviews with employees during normal working hours;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (f)(2)	Procedures.	(2) Providing, when requested, relevant employment or personnel files, security records, supervisory files, records pertinent to insider threat (e.g., security, cybersecurity, and human resources) and any other records pertaining to an individual under investigation that are, in the possession or control of the contractor or the contractor's representatives or located in the contractor's offices;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (f)(3)	Procedures.	(3) Providing access to employment and security records that are located at an offsite location; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (f)(4)	Procedures.	(4) Rendering other necessary assistance.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (g)	Procedures.	(g) Security training and briefings. Contractors will advise all cleared employees, including those assigned to USG locations or operations outside the United States, of their individual responsibility for classification management and for safeguarding classified information. Contractors will provide security training to cleared employees consisting of initial briefings, refresher briefings, and debriefings in accordance with § 117.12. United States, of their individual responsibility for classification management and for safeguarding classified information. Contractors will provide security training to cleared employees consisting of initial briefings, refresher briefings, and debriefings in accordance with § 117.12.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (h)	Procedures.	(h) Security reviews	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (h)(1)	Procedures.	(1) USG reviews. The applicable CSA will conduct recurring oversight reviews of contractors' NISP security programs to verify that the contractor is protecting classified information and implementing the provisions of this rule. The contractor's participation in the security review is required for maintaining the entity's eligibility for access to classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (h)(1)(i)	Procedures.	(i) Review cycle. The CSA will determine the scope and frequency of security reviews, which may be increased or decreased consistent with risk management principles.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (h)(1)(ii)	Procedures.	(ii) Procedures.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (h)(1)(ii)(A)	Procedures.	(A) The CSA will generally provide notice to the contractor of a forthcoming review, but may also conduct unannounced reviews at its discretion. The CSA security review may subject contractor employees and all areas and receptacles under the control of the contractor to examination.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (h)(1)(ii)(B)	Procedures.	(B) The CSA will make every effort to avoid unnecessary intrusion into the personal effects of contractor personnel.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (h)(1)(ii)(C)	Procedures.	(C) The CSA may conduct physical examinations of the interior space of containers not authorized to secure classified material. Such examinations will always be accomplished in the presence of a representative of the contractor.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (h)(1)(iii)	Procedures.	(iii) Controlled unclassified information (CUI). 32 CFR part 2002 requires agencies to implement CUI requirements, but compliance with CUI requirements is outside the scope of the NISP and this part. However, CSAs may conduct CUI assessments in conjunction with NISP USG reviews when:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (h)(1)(iii)(A)	Procedures.	(A) The contractor is a participant in the NISP based on a requirement to access classified information;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (h)(1)(iii)(B)	Procedures.	(B) A classified contract under the CSA's cognizance includes provisions for access to, or protection or handling of, CUI; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (h)(1)(iii)(C)	Procedures.	(C) The CSA has provided the contractor with specific guidance regarding the assessment criteria and methodology it will use for overseeing protection of the CUI being accessed, stored or transmitted by the contractor as part of the classified contract.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (h)(2)	Procedures.	(2) Contractor reviews. Contractors will review their security programs on a continuing basis and conduct a formal self-inspection at least annually and at intervals consistent with risk management principles.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (h)(2)(i)	Procedures.	(i) Self-inspections will include the review of the classified activity, classified information, classified information systems, conditions of the overall security program, and the insider threat program. They will have sufficient scope, depth, and frequency, and will have management support during the self-inspection and during remedial actions taken as a result of the self-inspection. Self-inspections will include the review of samples representing the contractor's derivative classification actions, as applicable.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (h)(2)(ii)	Procedures.	(ii) The contractor will prepare a formal report describing the self-inspection, its findings, and its resolution of issues discovered during the self-inspection. The contractor will retain the formal report for CSA review until after the next CSA security review is completed.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (h)(2)(iii)	Procedures.	(iii) The SMO at the cleared facility will annually certify to the CSA, in writing, that a self-inspection has been conducted, that other KMP have been briefed on the results of the self-inspection, that appropriate corrective actions have been taken, and that management fully supports the security program at the cleared facility in the manner as described in the certification.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (i)	Procedures.	(i) Contractors working at USG locations. Contractor employees performing work within the confines of a USG facility will safeguard classified information according to the procedures of the host installation or agency.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (j)	Procedures.	(j) Hotlines. Federal agencies maintain hotlines to provide an unconstrained avenue for USG and contractor employees to report, without fear of reprisal, known or suspected instances of security irregularities and infractions concerning contracts, programs, or projects. These hotlines do not supplant the contractor's responsibility to facilitate reporting and timely investigations of security issues concerning its operations or personnel. Contractor personnel are encouraged to report information through established contractor channels. The hotline may be used as an alternate means to report this type of information. Contractors will inform all personnel that hotlines may be used for reporting issues of national security significance. Each CSA will post hotline information and telephone numbers on their websites for contractor access.	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
§117.7 (k)	Procedures.	(k) Agency agreements. 32 CFR part 2004 and E.O. 12829 require non-CSA agency heads to enter into agreements with the Secretary of Defense as the Executive Agent for the NISP to provide industrial security services. The Secretary of Defense may also enter into agreements to provide services for other CSA's in accordance with 32 CFR part 2004 and E.O. 12829. Agency agreements establish the terms of the Secretary of Defense's (or the Secretary of Defense's designee's) responsibilities when acting as the CSA on behalf of these agency heads. The list of agencies for which the Secretary of Defense has agreed to render industrial security services is on the DCSA website at https://www.dcsa.mil.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (l)	Procedures.	(l) Security cognizance. The CSA will inform contractors if oversight has been delegated to a CSO.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (m)	Procedures.	(m) Rule interpretations. Contractors will forward requests for interpretations of this rule to their CSA in accordance with their CSA-provided guidance to supplement unique CSA mission requirements.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (n)	Procedures.	(n) Waivers to this rule. Contractors will submit any requests to waive provisions of this rule in accordance with CSA procedures, which may include periodic review of approved waivers. When submitting a request for a waiver, the contractor will, in writing, explain why it is impractical or unreasonable for the contractor to comply with the requirement it is asking to waive, identify alternative measures as prescribed by this rule, and include a proposed duration for the waiver. The contractor cannot implement a waiver unless the waiver is approved by the applicable CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.7 (o)	Procedures.	(o) Complaints and suggestions. Contractors may forward NISP administration complaints and suggestions to the Director of ISOO. However, contractors are encouraged to forward NISP administration complaints and suggestions to their respective CSA prior to forwarding to the ISOO.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(a)	Reporting requirements.	(a) General. Pursuant to this part, Security Executive Agent Directive (SEAD) 3, (available at: https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf) and CSA-provided guidance, contractors are required to:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(a)(1)	Reporting requirements.	(1) Report certain events that impact the status of the entity's or an employee's eligibility for access to classified information; report events that indicate an insider threat to classified information or to employees with access to classified information; report events that affect proper safeguarding of classified information; and report events that indicate classified information has been, or is suspected to be, lost or compromised.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(a)(2)	Reporting requirements.	(2) Establish internal procedures to ensure employees with eligibility for access to classified information are aware of their responsibilities for reporting pertinent information to the FSO. The contractor will:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(a)(2)(i)	Reporting requirements.	(i) Provide reports to the FBI, or other Federal authorities as required by this part, the terms of a classified contract or other agreement, and by U.S. law.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(a)(2)(ii)	Reporting requirements.	(ii) Provide complete information to enable the CSA to ascertain whether classified information is adequately protected.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(a)(2)(iii)	Reporting requirements.	(iii) Submit reports to the FBI, the CSA, or ISOO as specified in paragraphs (b), (c), and (g) of this section.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(a)(3)	Reporting requirements.	(3) Appropriately mark reports containing classified information in accordance with §117.14.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(a)(4)	Reporting requirements.	(4) Clearly mark a report containing information submitted in confidence as containing that information. When reports contain information pertaining to an individual, 5 U.S.C. 552a (also known as and referred to in this part as "The Privacy Act of 1974, as amended,") permits the withholding of certain information from the individual in accordance with specific exemptions, which include authority to withhold release of information to the extent that the disclosure of the information would reveal the identity of a source who furnished the information to the USG under an express promise that the identity of the source would be held in confidence.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(b)	Reporting requirements.	(b) Reports to be submitted to the FBI. The contractor will promptly submit a written report to the nearest field office of the FBI regarding information coming to the contractor's attention concerning actual, probable, or possible espionage, sabotage, terrorism, or subversive activities at any of its locations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(b)(1)	Reporting requirements.	(1) An initial report may be made by phone, but it must be followed up in writing (e.g., email or formal correspondence), regardless of the FBI's disposition of the report.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(b)(2)	Reporting requirements.	(2) The contractor will promptly notify the CSA when they make a report to the FBI and provide the CSA a copy of the written report.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)	Reporting requirements.	(c) Reports to be submitted to the CSA. For the purpose of §117.8(c) and §117.8(d), each subcontractor will be considered as a prime contractor in relation to its own subcontractor(s).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(1)	Reporting requirements.	(1) Adverse information. Contractors are required to report adverse information coming to their attention concerning any of their employees determined to be eligible for access to classified information, in accordance with this part, SEAD 3, and CSA-provided guidance. Contractors will not make reports based on rumor or innuendo.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(1)(i)	Reporting requirements.	(i) The termination of employment of an employee does not negate the requirement to submit this report. If a contractor employee is assigned to a USG location, the contractor will furnish a copy of the report and its final disposition to the USG security point of contact for that location.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(1)(ii)	Reporting requirements.	(ii) Pursuant to Becker v. Philco, 372 F.2d 771 (4th Cir. 1967), cert. denied 389 U.S. 979 (1967), and subsequent cases, a contractor may not be liable for defamation of an employee because of communications that are required of and made by a contractor to an agency of the United States under the requirements of this part or under the terms of applicable contracts.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(2)	Reporting requirements.	(2) Suspicious contacts. Contractors will report information pertaining to suspicious contacts with employees determined to be eligible for access to classified information, and pertaining to efforts to obtain illegal or unauthorized access to the contractor's cleared facility by any means, including:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(2)(i)	Reporting requirements.	(i) Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(2)(ii)	Reporting requirements.	(ii) Efforts by any individual, regardless of nationality, to elicit information from an employee determined eligible for access to classified information, and any contact which suggests the employee may be the target of an attempted exploitation by an intelligence service of another country. See SEAD 3 for specific information to be reported.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(3)	Reporting requirements.	(3) Change in status of employees determined eligible for access to classified information. Contractors will report by means of the CSA-designated reporting mechanism information pertaining to changes in status of employees determined eligible for access to classified information such as:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(3)(i)	Reporting requirements.	(i) Death.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(3)(ii)	Reporting requirements.	(ii) Change in name.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(3)(iii)	Reporting requirements.	(iii) Termination of employment.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(3)(iv)	Reporting requirements.	(iv) Change in citizenship.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(4)	Reporting requirements.	(4) Citizenship by naturalization. Contractors will report if a non-U.S. citizen employee granted an LAA becomes a citizen through naturalization. The report will include:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(4)(i)	Reporting requirements.	(i) City, county, and state where naturalized.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(4)(ii)	Reporting requirements.	(ii) Date naturalized.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(4)(iii)	Reporting requirements.	(iii) Court.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(4)(iv)	Reporting requirements.	(iv) Certificate number.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(5)	Reporting requirements.	(5) Employees desiring not to be processed for a national security eligibility determination or not to perform classified work. Contractors will report instances when an employee no longer wishes to be processed for a determination of eligibility for access to classified information or to continue having access to classified information, and the reason for that request.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(6)	Reporting requirements.	(6) Classified information nondisclosure agreement (NDA). Contractors will report the refusal by an employee to sign the SF 312, "Classified Information Nondisclosure Agreement," (available at: https://www.gsa.gov/cdnstatic/SF312-13.pdf?forceDownload=1) or other approved NDA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(7)	Reporting requirements.	(7) Changed conditions affecting the contractor's eligibility for access to classified information. Contractors are required to report certain events that affect the status of the entity eligibility determination (e.g., FCL), affect the status of an employee's PCL, may indicate an employee poses an insider threat, affect the proper safeguarding of classified information, or indicate classified information has been lost or compromised, including:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(7)(i)	Reporting requirements.	(i) Change of ownership or control of the contractor, including stock transfers that affect control of the entity.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(7)(ii)	Reporting requirements.	(ii) Change of operating name or address of the entity or any of its locations determined eligible for access to classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(7)(iii)	Reporting requirements.	(iii) Any change to the information previously submitted for KMP including, as appropriate, the names of the individuals the contractor is replacing. A new complete KMP listing need be submitted only at the discretion of the contractor or when requested by the CSA. The contractor will provide a statement indicating:	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
§117.8(c)(7)(iii)(A)	Reporting requirements.	(A) Whether the new KMP are cleared for access to classified information, and if cleared, to what level they are cleared and when they were cleared, their dates and places of birth, social security numbers, and citizenship.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(7)(iii)(B)	Reporting requirements.	(B) Whether they have been excluded from access to classified information in accordance with §117.7(b)(5)(ii).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(7)(iii)(C)	Reporting requirements.	(C) Whether they have been temporarily excluded from access to classified information pending the determination of eligibility for access to classified information in accordance with §117.9(g).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(7)(iv)	Reporting requirements.	(iv) Any action to terminate business or operations for any reason, imminent adjudication or reorganization in bankruptcy, or any change that might affect the validity of the contractor's eligibility for access to classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(7)	Reporting requirements.	(v) Any material change concerning the information previously reported concerning foreign ownership, control, or influence (FOCI). This report will be made by the submission of an updated SF 328, "Certificate Pertaining to Foreign Interests," in accordance with CSA-provided guidance. When submitting this information, it is not necessary to repeat answers that have not changed. When entering into discussion, consultations, or agreements that may reasonably lead to effective ownership or control by a foreign interest, the contractor will report the details to the CSA in writing. If the contractor has received a Schedule 13D from the investor, the contractor will forward a copy with the report.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(8)	Reporting requirements.	(8) Changes in storage capability. The contractor will report any changes in their storage requirement or capability to safeguard classified material.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(9)	Reporting requirements.	(9) Inability to safeguard classified material. The contractor will report any emergency situation that renders their location incapable of safeguarding classified material as soon as possible.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(10)	Reporting requirements.	(10) Unsatisfactory conditions of a prime or subcontractors.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(10)(i)	Reporting requirements.	(i) Prime contractors will report any information coming to their attention that may indicate that classified information cannot be adequately protected by a subcontractor, or other circumstances that may impact the validity of the eligibility for access to classified information of any subcontractors.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(10)(ii)	Reporting requirements.	(ii) Subcontractors will report any information coming to their attention that may indicate that classified information cannot be adequately protected or other circumstances that may impact the validity of the eligibility for access to classified information of their prime contractor.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(11)	Reporting requirements.	(11) Dispositioned material previously terminated. The contractor will make a report when the location or disposition of material previously terminated from accountability is subsequently discovered and brought back into accountability.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(12)	Reporting requirements.	(12) Foreign classified contracts. Contractors will report any pre-contract negotiation or award not placed through a CSA or U.S. GCA that involves, or may involve:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(12)(i)	Reporting requirements.	(i) The release or disclosure of U.S. classified information to a foreign interest.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(12)(ii)	Reporting requirements.	(ii) Access to classified information furnished by a foreign interest.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(13)	Reporting requirements.	(13) Reporting of improper receipt of foreign government material. The contractor will report to the CSA the receipt of classified material from foreign interests that is not received through Government channels.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(c)(14)	Reporting requirements.	(14) Reporting by subcontractor. Subcontractors will also notify their prime contractors if they make any reports to their CSA in accordance with the provisions of paragraphs (c)(7) through (c)(10) of this section.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(d)	Reporting requirements.	(d) Reports of loss, compromise, or suspected compromise. The contractor will report any loss, compromise, or suspected compromise of classified information, U.S. or foreign, to the CSA in accordance with paragraph (d)(1) through (d)(3) of this section. Each CSA may provide additional guidance concerning the reporting time period. If the contractor is located on a USG facility, the contractor will submit the report to the CSA and to the head of the USG facility.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(d)(1)	Reporting requirements.	(1) Preliminary inquiry. Immediately upon receipt of a security violation report involving classified information, the contractor will initiate a preliminary inquiry to ascertain all of the circumstances surrounding the presumed loss, compromise, or suspected compromise, including validation of the classification of the information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(d)(2)	Reporting requirements.	(2) Initial report. If the contractor's preliminary inquiry confirms that a loss, compromise, or suspected compromise of any classified information occurred, the contractor will promptly submit an initial report of the incident unless otherwise notified by the CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(d)(3)	Reporting requirements.	(3) Final report. When the investigation has been completed, the contractor will submit a final report to the CSA which, in turn, will follow CSA procedures to notify the applicable GCA. The report will include:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(d)(3)(i)	Reporting requirements.	(i) Material and relevant information that was not included in the initial report.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(d)(3)(ii)	Reporting requirements.	(ii) The full name and social security number of the individual or individuals primarily responsible for the incident, including a record of prior loss, compromise, or suspected compromise for which the individual had been determined responsible.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(d)(3)(iii)	Reporting requirements.	(iii) A statement of the corrective action taken to preclude a recurrence.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(d)(3)(iv)	Reporting requirements.	(iv) Disciplinary action taken against the responsible individual or individuals, if any.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(d)(3)(v)	Reporting requirements.	(v) Specific reasons for reaching the conclusion that loss, compromise, or suspected compromise occurred or did not occur.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(d)(4)	Reporting requirements.	(4) Employee information in compromise cases. When requested by the CSA, the contractor will report information concerning an employee or other individual, determined to be responsible for the incident, when the information is needed by the CSA for the loss, compromise, or suspected compromise of classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(e)	Reporting requirements.	(e) Individual culpability reports. Contractors will establish and enforce policies that provide for appropriate administrative or disciplinary actions taken against employees who violate the requirements of this part.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(e)(1)	Reporting requirements.	(1) Contractors will establish a system to manage and track information regarding employees with eligibility for access to classified information who violate the requirements of this part in order to be able to identify patterns of negligence or carelessness, or to identify a potential insider threat.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(e)(2)	Reporting requirements.	(2) Contractors will establish and apply a graduated scale of administrative and disciplinary actions in the event of employee security violations or negligence in the handling of classified information. CSAs may provide guidance to contractors with examples of administrative or disciplinary actions that the contractor may consider implementing in the event of employee violations or negligence. Contractors are required to submit a final report to the CSA with the findings of an employee's culpability and what corrective actions were taken.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(e)(3)	Reporting requirements.	(3) Contractors will include a statement of the administrative or disciplinary actions taken against an employee in a final report to the CSA. A statement must be included when the individual responsible for a security violation can be determined. Contractors' final reports will indicate whether one or more of the following factors are evident:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(e)(3)(i)	Reporting requirements.	(i) Involved a deliberate disregard of security requirements.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(e)(3)(ii)	Reporting requirements.	(ii) Involved negligence in the handling of classified material.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(e)(3)(iii)	Reporting requirements.	(iii) Was not deliberate in nature but reflects a recent or recurring pattern of questionable judgment, irresponsibility, negligence, or carelessness.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(f)	Reporting requirements.	(f) CDC cyber incident reports. This paragraph applies only to CDCs and sets forth reporting requirements pursuant to 10 U.S.C. 391 and 393 and Defense Federal Acquisition Regulation Supplement Clause 252.204-7012. The reporting requirements of paragraph (f) of this section are in addition to the requirements in paragraphs (b) and (d) of this section, which can include certain activities occurring on unclassified information systems. DoD will provide detailed reporting instructions for contractors affected by these references via industrial security letter in accordance with DoDI 5220.22.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(f)(1)	Reporting requirements.	(1) Reports to be submitted to the designated DoD CSO. CDCs will immediately report to the DoD CSO, any cyber incident on a classified covered information system that has been approved by that CSO to process classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(f)(1)(i)	Reporting requirements.	(i) At a minimum, the report will include:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(f)(1)(i)(A)	Reporting requirements.	(A) A description of the technique or method used in the cyber incident.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(f)(1)(i)(B)	Reporting requirements.	(B) A sample of the malicious software involved in the cyber incident, if discovered and isolated by the CDC,	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(f)(1)(i)(C)	Reporting requirements.	(C) A summary of information in connection with any DoD program that has been potentially compromised due to the cyber incident.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(f)(1)(ii)	Reporting requirements.	(ii) Information that is reported by the CDC (or derived from information reported by the CDC) will be safeguarded, used, and disseminated in a manner consistent with DoD procedures governing the handling of such information pursuant to Pub. L. 112-239 and 10 U.S.C. 391.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(f)(1)(iii)	Reporting requirements.	(iii) Reports involving classified foreign government information will be reported to the Director, International Security Programs, Defense Technology Security Administration (DoD).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(f)(2)	Reporting requirements.	(2) Reports on non-Federal information systems not authorized to process classified information. CDCs will report cyber incidents on non-Federal, unclassified information systems in accordance with contract requirements.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(f)(3)	Reporting requirements.	(3) Access to equipment and information by DoD personnel.	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
§117.8(f)(3)(i)	Reporting requirements.	(i) The CDC will allow, upon request by DoD personnel, access by DoD personnel to additional equipment or information of the CDC that is necessary to conduct forensic analysis of reportable cyber incidents in addition to any analysis conducted by the CDC.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(f)(3)(ii)	Reporting requirements.	(ii) The CDC is only required to provide DoD access to equipment or information to determine whether information created by or for DoD in connection with any DoD program was successfully exfiltrated from a CDC's network or information system, and what information was exfiltrated from the CDC's network or information system.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(g)	Reporting requirements.	(g) Reports to ISOO.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(g)(1)	Reporting requirements.	(1) Contractors will report instances of redundant or duplicative security review and audit activity by the CSAs to the Director, ISOO, for resolution.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.8(g)(2)	Reporting requirements.	(2) Contractors will report instances of CSAs duplicating processing to determine an entity's eligibility for access to classified information when there is an existing determination of an entity's eligibility for access to classified information by another CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (a)	Entity eligibility determination for access to classified information.	(a) General. This section applies to all contractors with entity eligibility determinations, except as provided in §117.22 for entity eligibility determinations for participation in the CCIPP under the cognizance of DHS.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (a)(1)	Entity eligibility determination for access to classified information.	(1) Prior to the entity being granted an entity eligibility determination for access to classified information, the responsible CSA must have determined that:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (a)(1)(i)	Entity eligibility determination for access to classified information.	(i) The entity is eligible for access to classified information to meet a legitimate USG or foreign government need.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (a)(1)(ii)	Entity eligibility determination for access to classified information.	(ii) Access is consistent with national security interests.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (a)(2)	Entity eligibility determination for access to classified information.	(2) The CSA will provide guidance on processing entity eligibility determinations for entity access to classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (a)(3)	Entity eligibility determination for access to classified information.	(3) The determination of entity eligibility for access is separate from the determination of a classified information safeguarding capability (see §117.15).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (a)(4)	Entity eligibility determination for access to classified information.	(4) Neither the contractor nor its employees will be permitted access to classified information until the CSA has made an entity eligibility determination (e.g., issued an FCL).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (a)(5)	Entity eligibility determination for access to classified information.	(5) The requirement for a favorable entity eligibility determination (also referred to in some instances as an FCL) for a prime contractor includes instances where all access to classified information will be limited to subcontractors. A prime contractor must have a favorable entity eligibility determination at the same or higher classification level as its subcontractors.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (a)(6)	Entity eligibility determination for access to classified information.	(6) Contractors are eligible for storage of classified material in connection with a legitimate USG or foreign government requirement if they have a favorable entity eligibility determination and a classified information safeguarding capability approved by the CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (a)(7)	Entity eligibility determination for access to classified information.	(7) An entity eligibility determination is valid for access to classified information at the same or lower classification level.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (a)(8)	Entity eligibility determination for access to classified information.	(8) Each CSA will maintain a record of entity eligibility determinations made by that CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (a)(9)	Entity eligibility determination for access to classified information.	(9) A contractor will not use its favorable entity eligibility determination for advertising or promotional purposes. This does not prohibit the contractor from advertising employee positions that require a PCL in connection with the position.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (a)(10)	Entity eligibility determination for access to classified information.	(10) A contractor or prospective contractor cannot apply for its own entity eligibility determination. A GCA or a currently cleared contractor may sponsor an entity for an entity eligibility determination at any point during the contracting or agreement life cycle at which the entity must have access to classified information to participate (including the solicitation or competition phase).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (b)	Entity eligibility determination for access to classified information.	(b) Reciprocity. If an entity has an appropriate, final entity eligibility determination, a CSA will not duplicate the entity eligibility determination processes performed by another CSA. If a CSA cannot acknowledge an entity eligibility determination to another CSA, the involved entity may be subject to duplicate processing in accordance with 32 CFR part 2004.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (c)	Entity eligibility determination for access to classified information.	(c) Eligibility requirements. To be eligible for an initial entity eligibility determination or to maintain an existing entity eligibility determination, the entity must:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (c)(1)	Entity eligibility determination for access to classified information.	(1) Need access to classified information in connection with a legitimate USG or foreign government requirement, and access must be consistent with U.S. national security interests as determined by the CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (c)(2)	Entity eligibility determination for access to classified information.	(2) Be organized and existing:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (c)(2)(i)	Entity eligibility determination for access to classified information.	(i) Under the laws of the United States, one of the fifty States, the District of Columbia, or an organized U.S. territory (Guam, Commonwealth of the Northern Marianas Islands, Commonwealth of Puerto Rico, and the U.S. Virgin Islands); or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (c)(2)(ii)	Entity eligibility determination for access to classified information.	(ii) Under the laws of an American Indian/Alaska Native tribal entity if:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (c)(2)(ii)(A)	Entity eligibility determination for access to classified information.	(A) The American Indian or Alaska Native tribe under whose laws the entity is chartered has been formally acknowledged by the Assistant Secretary – Indian Affairs, of the U.S. Department of the Interior.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (c)(2)(ii)(B)	Entity eligibility determination for access to classified information.	(B) The contractor is organized and continues to exist, during the period of the eligibility under a tribal statue or code, or pursuant to a resolution of an authorized tribal legislative body.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (c)(2)(ii)(C)	Entity eligibility determination for access to classified information.	(C) The contractor has submitted or will submit records such as a charter, certificate of organization, or other applicable tribal documents and statute or code provisions governing the formation and continuation of the entity, for CSA determination that the entity is tribally chartered.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (c)(3)	Entity eligibility determination for access to classified information.	(3) Be located in the United States or its territorial areas.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (c)(4)	Entity eligibility determination for access to classified information.	(4) Have a record of integrity and lawful conduct in its business dealings.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (c)(5)	Entity eligibility determination for access to classified information.	(5) Have an SMO, FSO, and ITPSO who have and who maintain eligibility for access to classified information and are not excluded from participating in USG contracts or agreements in accordance with §117.7(b)(1) through §117.7(b)(3).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (c)(6)	Entity eligibility determination for access to classified information.	(6) Not be under FOCI to such a degree that a favorable entity eligibility determination for access to classified information would be inconsistent with the national interest, in the judgment of the CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (c)(7)	Entity eligibility determination for access to classified information.	(7) Maintain sufficient authorized and cleared employees to manage and implement the requirements of this part in accordance with CSA guidance.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (c)(8)	Entity eligibility determination for access to classified information.	(8) Not pose an unacceptable risk to national security interests, in the judgment of the CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (c)(9)	Entity eligibility determination for access to classified information.	(9) Meet all requirements governing access to classified information established by the CSA or the relevant authorizing law, regulation, or government-wide policy.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (d)	Entity eligibility determination for access to classified information.	(d) Processing the entity eligibility determination. The CSA will assess the entity's eligibility for access to classified information based on its business structure.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (d)(1)	Entity eligibility determination for access to classified information.	(1) At a minimum, the entity will:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (d)(1)(i)	Entity eligibility determination for access to classified information.	(i) Provide CSA-requested documentation within timelines established by the CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (d)(1)(ii)	Entity eligibility determination for access to classified information.	(ii) Have and identify the SMO.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (d)(1)(iii)	Entity eligibility determination for access to classified information.	(iii) Appoint a U.S. citizen employee as the FSO.	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
§117.9 (d)(1)(iv)	Entity eligibility determination for access to classified information.	(iv) Appoint a U.S. citizen employee as the ITPSO.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (d)(1)(v)	Entity eligibility determination for access to classified information.	(v) Submit requests for personnel security investigations for the SMO, FSO, ITPSO, and those other KMP identified by the CSA as requiring eligibility for access to classified information in connection with the entity eligibility.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (d)(2)	Entity eligibility determination for access to classified information.	(2) If the entity is under FOCI with a special security agreement (SSA) as the proposed method of FOCI mitigation, and the GCA requires the entity to have access to proscribed information, the CSA must consider the measures listed in §117.11(d) as part of the entity eligibility determination.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (e)	Entity eligibility determination for access to classified information.	(e) Other personnel eligibility determinations concurrent with the entity eligibility determination.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (e)(1)	Entity eligibility determination for access to classified information.	(1) Contractors may designate employees who require access to classified information during the negotiation of a contract or the preparation of a bid or quotation pertaining to a prime contract or a subcontract. These designated employees will be processed for a determination of eligibility for access to classified information (i.e., PCL eligibility) concurrent with entity's entity eligibility determination.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (e)(2)	Entity eligibility determination for access to classified information.	(2) The entity eligibility determination is not dependent on the PCL eligibility for access to classified information by such employees, provided none of these employees are among those listed in paragraph (c)(5) of this section. Even so, the employees will not be granted access to classified information until both a favorable entity eligibility determination and PCL eligibility has been granted.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (f)	Entity eligibility determination for access to classified information.	(f) Exclusion procedures. If a CSA determines that certain KMP can be excluded from access to classified information, the contractor will follow the procedures in accordance with §117.7(b)(5)(ii).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (g)	Entity eligibility determination for access to classified information.	(g) Temporary exclusions. As a result of a changed condition, the SMO or other KMP who require eligibility for access to classified information in connection with the facility entity eligibility determination may be temporarily excluded from access to classified information while in the process of a PCL eligibility determination provided:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (g)(1)	Entity eligibility determination for access to classified information.	(1) The SMO or other KMP are not appointed as the FSO or ITPSO. FSOs and ITPSOs may not be temporarily excluded. A cleared employee must always be appointed to fulfill the requirements of these positions in accordance with this part.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (g)(2)	Entity eligibility determination for access to classified information.	(2) An employee, cleared to the level of the entity eligibility determination, must be able to fulfill the NISP responsibilities of the temporarily excluded KMP in accordance with this part while the temporary exclusion is in effect.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (g)(3)	Entity eligibility determination for access to classified information.	(3) The applicable CSA may provide additional guidance on the duration of a temporary exclusion from access to classified information based on circumstances, business structure, and other relevant security information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (g)(4)	Entity eligibility determination for access to classified information.	(4) The contractor's governing board affirms the exclusion action, and provides a copy of the exclusion action to the CSA. This action will be made a matter of record by the organization's governing body. Table 1 to paragraph (g)(iv) Temporary Exclusion Resolutions	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (h)	Entity eligibility determination for access to classified information.	(h) Interim entity eligibility determinations. The CSA may make an interim entity eligibility determination for access to classified information, in the sole discretion of the CSA. See §117.10(l) for access limitations that also apply to interim entity eligibility determinations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (h)(1)	Entity eligibility determination for access to classified information.	(i) An interim entity eligibility determination is made on a temporary basis pending completion of the full investigative requirements.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (h)(2)	Entity eligibility determination for access to classified information.	(ii) If the contractor with an interim entity eligibility determination is unable or unwilling to comply with the requirements of this part and CSA-provided guidance regarding the process to obtain a final entity eligibility determination, the CSA will withdraw the interim entity eligibility.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (i)	Entity eligibility determination for access to classified information.	(i) Multiple facility organizations. The home office must have an entity eligibility determination at the same level as the highest entity eligibility determination of an entity within the MFO. The CSA will determine whether branch offices are eligible for access to classified information if the branch offices need access and meet all other requirements.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (j)	Entity eligibility determination for access to classified information.	(j) Parent-subsidiary relationships. When a parent-subsidiary relationship exists, the CSA will process the parent and the subsidiary separately for entity eligibility determinations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (j)(1)	Entity eligibility determination for access to classified information.	(1) If the CSA determines the parent must be processed for an entity eligibility determination, then the parent must have an entity eligibility determination at the same or higher level as the subsidiary.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (j)(2)	Entity eligibility determination for access to classified information.	(2) When a parent and subsidiary or multiple cleared subsidiaries are collocated, a formal written agreement to use common security services may be executed by the entities, subject to the approval of the CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (k)	Entity eligibility determination for access to classified information.	(k) Joint ventures. A joint venture may be granted eligibility for access to classified information if it meets the eligibility requirements in paragraph (c) of this section, including:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (k)(1)	Entity eligibility determination for access to classified information.	(1) The joint venture must be established as a legal business entity (e.g. limited liability entity, corporation, or partnership). A joint venture established by contract that is not also established as a legal business entity is not eligible for an entity eligibility determination.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (k)(2)	Entity eligibility determination for access to classified information.	(2) The business entity operating as a joint venture must have been awarded a classified contract or sponsored by a GCA or prime contractor for an entity eligibility determination in advance of a potential award for which the business entity has bid pursuant to paragraph (c) of this section.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (k)(3)	Entity eligibility determination for access to classified information.	(3) The business entity operating as a joint venture must have an employee or employees appointed as security officials or KMP pursuant to §117.7(b).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (l)	Entity eligibility determination for access to classified information.	(l) Consultants. The responsible CSA will determine when there is a need for self-employed consultants requiring access to classified information to be considered for an entity eligibility determination.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (m)	Entity eligibility determination for access to classified information.	(m) Limited entity eligibility determination (Non-FOCI).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (m)(1)	Entity eligibility determination for access to classified information.	(1) The applicable CSA may choose to allow a GCA to request limited entity eligibility determinations for a single, narrowly defined contract, agreement, or circumstance and specific to the requesting GCA's classified information. This is not the same as a limited entity eligibility determination in situations involving FOCI, when the FOCI is not mitigated or negated.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (m)(1)(i)	Entity eligibility determination for access to classified information.	(i) Limited entity eligibility determinations (or FCLs) involving FOCI will be processed in accordance with §117.11(e).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (m)(1)(ii)	Entity eligibility determination for access to classified information.	(ii) This paragraph (paragraph (m) of this section) applies to limited entity eligibility determinations for purposes other than FOCI mitigation in accordance with 32 CFR part 2004. Additional guidance may be provided by the responsible CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (m)(2)	Entity eligibility determination for access to classified information.	(2) An entity must be sponsored for a limited entity eligibility determination by a GCA in accordance with the sponsorship requirements contained in paragraph (c) of this section. The contractor should be aware that the sponsorship request from the GCA to the CSA must also include:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (m)(2)(i)	Entity eligibility determination for access to classified information.	(i) Description of the compelling need for the limited entity eligibility determination that is in accordance with U.S. national security interests.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (m)(2)(ii)	Entity eligibility determination for access to classified information.	(ii) Specific reason(s) or rationale for limiting the entity eligibility determination.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (m)(2)(iii)	Entity eligibility determination for access to classified information.	(iii) The GCA's formal acknowledgement and acceptance of the risk associated with this rationale.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (m)(3)	Entity eligibility determination for access to classified information.	(3) The entity must otherwise meet the entity eligibility determination requirements set out in this part.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (m)(4)	Entity eligibility determination for access to classified information.	(4) Access limitations are inherent with the limited entity eligibility determination and are imposed upon all of the entity's employees regardless of citizenship.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (m)(5)	Entity eligibility determination for access to classified information.	(5) Contractors should be aware that the CSA will document the requirements of each limited entity eligibility determination it makes, including the scope of, and any limitations on, access to classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (m)(6)	Entity eligibility determination for access to classified information.	(6) Contractors should be aware that the CSA will verify limited entity eligibility determinations only to the requesting GCA. In the case of multiple limited entity eligibility determinations for a single entity, the CSA verifies each one separately only to its requestor.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (m)(7)	Entity eligibility determination for access to classified information.	(7) The applicable CSA administratively terminates the limited entity eligibility determination when there is no longer a need for access to the classified information for which the CSA approved the limited entity eligibility determination.	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
§117.9 (n)	Entity eligibility determination for access to classified information.	(n) Termination of the entity eligibility determination. Once granted, a favorable entity eligibility determination remains in effect until terminated or revoked. If the entity eligibility determination is terminated or revoked, the contractor will return all classified material in its possession to the appropriate GCA or dispose of the material as instructed by the CSA. The contractor should be aware that it may request an administrative termination or the CSA may:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (n)(1)	Entity eligibility determination for access to classified information.	(1) After coordination with applicable GCAs, administratively terminate the entity eligibility determination because the contractor no longer has a need for access to classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (n)(2)	Entity eligibility determination for access to classified information.	(2) Revoke an entity eligibility determination if the contractor is unable or unwilling to protect classified information or is unable to comply with the security requirements of this part.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (o)	Entity eligibility determination for access to classified information.	(o) Invalidation of the entity eligibility determination. The CSA may invalidate an existing entity eligibility determination. While the entity eligibility determination is in an invalidated status, the contractor may not bid on or be awarded new classified contracts or solicitations. The contractor may continue to work on existing classified contracts if the GCA agrees.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.9 (p)	Entity eligibility determination for access to classified information.	(p) Records maintenance. Contractors will maintain the original CSA designated forms for the duration of the entity eligibility determination in accordance with CSA-provided guidance.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(a)	Determination of eligibility for access to classified information for contractor employees.	(a) General.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(a)(1)	Determination of eligibility for access to classified information for contractor employees.	(1) The CSA is responsible for determining an employee's eligibility for access to classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(a)(1)(i)	Determination of eligibility for access to classified information for contractor employees.	(i) The contractor must determine that access to classified information is essential in the performance of tasks or services related to the fulfillment of a classified contract.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(a)(1)(ii)	Determination of eligibility for access to classified information for contractor employees.	(ii) Access must be clearly consistent with U.S. national security interests as determined by the CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(a)(1)(iii)	Determination of eligibility for access to classified information for contractor employees.	(iii) A contractor may give an employee access to classified information at the same or lower level of classification as the level of the contractor's entity eligibility determination if the employee has:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(a)(1)(iii)(A)	Determination of eligibility for access to classified information for contractor employees.	(A) A valid need-to-know for the classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(a)(1)(iii)(B)	Determination of eligibility for access to classified information for contractor employees.	(B) A USG favorable eligibility determination for access to classified information at the appropriate level.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(a)(1)(iii)(C)	Determination of eligibility for access to classified information for contractor employees.	(C) A signed non-disclosure agreement.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(a)(2)	Determination of eligibility for access to classified information for contractor employees.	(2) The CSA will determine eligibility for access to classified information in accordance with SEAD 4 (available at: https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf) and notify the contractor when eligibility has been granted.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(a)(2)(i)	Determination of eligibility for access to classified information for contractor employees.	(i) The CSA will notify the contractor when an employee's eligibility has been denied, suspended, or revoked.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(a)(2)(ii)	Determination of eligibility for access to classified information for contractor employees.	(ii) The contractor will immediately deny access to classified information to any employee when notified of a denial, revocation, or suspension of eligibility regardless of the contractor employee's location.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(a)(2)(iii)	Determination of eligibility for access to classified information for contractor employees.	(iii) If the employee's performance is at a USG facility, the contractor will provide notification to the appropriate GCA of any denial, revocation, or suspension of eligibility for access to classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(a)(3)	Determination of eligibility for access to classified information for contractor employees.	(3) Contractors will annotate and maintain the accuracy of their employees' records in the system of record for contractor eligibility and access to classified information, when one has been designated by the CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(a)(4)	Determination of eligibility for access to classified information for contractor employees.	(4) Within an MFO or within the same business organization, contractors may centrally manage eligibility for access to classified information and access to classified information records.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(a)(5)	Determination of eligibility for access to classified information for contractor employees.	(5) The contractor will limit requests for determinations of eligibility for access to classified information to the minimum number of employees and consultants necessary for operational efficiency in accordance with contractual obligations and other requirements of this part. Requests for determinations of eligibility for access to classified information will not be used to establish a cache of cleared employees.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(a)(6)	Determination of eligibility for access to classified information for contractor employees.	(6) The contractor will not submit a request for an eligibility determination to one CSA if the employee applicant is known to be cleared or in process for eligibility for access to classified information by another CSA. In such cases, to permit verification of eligibility, the contractor will provide the new CSA with the full name, date and place of birth, social security number, clearing agency, and type of investigation.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(a)(7)	Determination of eligibility for access to classified information for contractor employees.	(7) Contractors will not submit requests for determination of eligibility for access to classified information for individuals who are not their employees or consultants; nor will they submit requests for employees of subcontractors.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(a)(8)	Determination of eligibility for access to classified information for contractor employees.	(8) Access to SCI, SAP, FRD, and RD information is a determination made by the granting authority by the applicable USG granting authority for each category of information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(b)	Determination of eligibility for access to classified information for contractor employees.	(b) Investigative requirements. E.O. 13467, as amended, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information," designates the Security and Suitability Executive Agents responsible for establishing the standards for investigative requirements that apply to contractors.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(b)(1)	Determination of eligibility for access to classified information for contractor employees.	(1) Investigative tiers. The standards established in accordance with E.O. 13467, as amended, designate specific investigative tiers that are acceptable for access to classified information. An investigative tier is for positions designated as moderate risk, non-critical sensitive, and allow access to information classified at the L, CONFIDENTIAL, and SECRET levels. Another investigative tier is for positions designated as high risk, critical sensitive, special sensitive, and allow access to information classified at the Q, TOP SECRET, and SCI levels.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(b)(2)	Determination of eligibility for access to classified information for contractor employees.	(2) Investigative coverage.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(b)(2)(i)	Determination of eligibility for access to classified information for contractor employees.	(i) Automated sources. Investigative providers will use automation whenever possible to collect, verify, corroborate, or discover information about an individual, as documented on the request for investigation or developed from other sources, i.e., automated record checks and inquiries.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(b)(2)(ii)	Determination of eligibility for access to classified information for contractor employees.	(ii) Interviews. Interviews, if required, will cover areas of adjudicative concern.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(b)(2)(iii)	Determination of eligibility for access to classified information for contractor employees.	(iii) Information Covered in Previous Investigations. Information validated in a prior investigation, the results of which are not expected to change (e.g., verification of education degree), will not be repeated as part of subsequent investigations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(b)(3)	Determination of eligibility for access to classified information for contractor employees.	(3) Polygraph. Agencies with policies authorizing the use of the polygraph for purposes of determining eligibility for access to classified information may require polygraph examinations when necessary. If adjudicatively relevant information arises during the investigation or the polygraph examination, the investigation may be expanded to resolve the adjudicative concerns.	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
§117.10(b)(4)	Determination of eligibility for access to classified information for contractor employees.	(4) Financial disclosure. When a GCA requires that a contractor employee complete a financial disclosure form, the contractor will ensure that the employee has the opportunity to complete and submit the form in accordance with the Privacy Act of 1974, as amended, and other applicable provisions of law.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(b)(5)	Determination of eligibility for access to classified information for contractor employees.	(5) Reinvestigation and Continuous Evaluation. Contractor employees determined eligible for access to classified information will follow CSA guidance to complete reinvestigation and continuous evaluation or continuous vetting requirements. The contractor will validate that the employee requires continued eligibility for access to classified information before initiating the reinvestigation.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(c)	Determination of eligibility for access to classified information for contractor employees.	(c) Verification of U.S. citizenship. A contractor will require each applicant for determination of eligibility for access to classified information who claims U.S. citizenship to provide evidence of citizenship to the FSO or other authorized representative of the contractor. All documentation must be the original or certified copies of the original documents.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(c)(1)	Determination of eligibility for access to classified information for contractor employees.	(1) Any document, or its successor, listed in this paragraph is an acceptable document to corroborate U.S. citizenship by birth, including by birth abroad to a U.S. citizen.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(c)(1)(i)	Determination of eligibility for access to classified information for contractor employees.	(i) A birth certificate certified with the registrar's signature, which bears the raised, embossed, impressed, or multicolored seal of the registrar's office.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(c)(1)(ii)	Determination of eligibility for access to classified information for contractor employees.	(ii) A current or expired U.S. passport or passport card that is unaltered and undamaged and was originally issued to the individual.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(c)(1)(iii)	Determination of eligibility for access to classified information for contractor employees.	(iii) A Department of State Form FS-240, "Consular Report of Birth Abroad of a Citizen of the United States of America."	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(c)(1)(iv)	Determination of eligibility for access to classified information for contractor employees.	(iv) A Department of State Form FS-545 or DS-1350, "Certification of Report of Birth."	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(c)(2)	Determination of eligibility for access to classified information for contractor employees.	(2) Any document, or its successor, listed in this paragraph is an acceptable document to corroborate U.S. citizenship by certification, naturalization, or birth abroad to a U.S. citizen.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(c)(2)(i)	Determination of eligibility for access to classified information for contractor employees.	(i) A U.S. Citizenship and Immigration Services Form N-560 or N-561, "Certification of U.S. Citizenship."	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(c)(2)(ii)	Determination of eligibility for access to classified information for contractor employees.	(ii) A U.S. Citizenship and Immigration Services Form 550, 551, or 570, "Naturalization Certificate."	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(c)(2)(iii)	Determination of eligibility for access to classified information for contractor employees.	(iii) A valid or expired U.S. passport or passport card that is unaltered and undamaged and was originally issued to the individual.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(d)	Determination of eligibility for access to classified information for contractor employees.	(d) Procedures for completing the electronic version of the SF 86, "Questionnaire for National Security Positions." The electronic version of the SF 86 (available at: https://www.opm.gov/forms/pdf_fill/sf86.pdf) must be completed in e-QIP or its successor system by the contractor employee and reviewed by the FSO or other contractor employee(s) who has (have) been specifically designated by the contractor to review an employee's SF 86. The FSO or designee will:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(d)(1)	Determination of eligibility for access to classified information for contractor employees.	(1) Provide the employee with written notification that review of the SF 86 by the FSO or other contractor employee is for adequacy and completeness, information will be used for no other purpose within the entity, that the information provided by the employee is protected by the "Privacy Act of 1974, as amended" and that the Privacy Act notice included in the SF 86, including the routine uses for which this information can be disclosed, applies to this information collection.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(d)(2)	Determination of eligibility for access to classified information for contractor employees.	(2) Not share information from the employee's SF 86 within the entity and will not use the information for any purpose other than determining the adequacy and completeness of the SF 86.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(e)	Determination of eligibility for access to classified information for contractor employees.	(e) Fingerprint collection. The contractor will submit fingerprints in accordance with CSA guidance. Contractors will use digital fingerprints whenever possible.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(f)	Determination of eligibility for access to classified information for contractor employees.	(f) Pre-employment eligibility determination action.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(f)(1)	Determination of eligibility for access to classified information for contractor employees.	(1) If a potential employee requires access to classified information immediately upon commencement of employment, the contractor may submit a request for investigation prior to the date of employment, provided:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(f)(1)(i)	Determination of eligibility for access to classified information for contractor employees.	(i) A written commitment for employment has been made by the contractor.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(f)(1)(ii)	Determination of eligibility for access to classified information for contractor employees.	(ii) The candidate has accepted the offer in writing.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(f)(2)	Determination of eligibility for access to classified information for contractor employees.	(2) The commitment for employment must indicate employment will commence within 45 days of the employee being granted eligibility for access to classified information at a level that allows them to perform the tasks or services associated with the contract or Government requirement for which they were hired.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(f)(3)	Determination of eligibility for access to classified information for contractor employees.	(3) Contractors will comply with the requirements pursuant to paragraph (a) (5) of this section.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(g)	Determination of eligibility for access to classified information for contractor employees.	(g) Classified information NDA. The NDA designated by the CSA (e.g., SF 312), is an agreement between the USG and an individual who is determined eligible for access to classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(g)(1)	Determination of eligibility for access to classified information for contractor employees.	(1) An employee determined eligible for access to classified information must execute an NDA prior to being granted access to classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(g)(2)	Determination of eligibility for access to classified information for contractor employees.	(2) The employee must sign and date the NDA in the presence of a witness. The employee's and witness' signatures must bear the same date.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(g)(3)	Determination of eligibility for access to classified information for contractor employees.	(3) The contractor will forward the executed NDA to the CSA for retention. The CSA may authorize the contractor to retain a copy of the form for administrative purposes, if appropriate.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(g)(4)	Determination of eligibility for access to classified information for contractor employees.	(4) If the employee refuses to execute the NDA, the contractor will deny the employee access to classified information and submit a report to the CSA in accordance with §117.8(c)(6).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(h)	Determination of eligibility for access to classified information for contractor employees.	(h) Reciprocity. The applicable CSA is responsible for determining whether contractor employees have been previously determined eligible for access to classified information or investigated by an authorized investigative activity in accordance with SEAD 7 (available at: https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-7_BI_ReciprocityU.pdf).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(h)(1)	Determination of eligibility for access to classified information for contractor employees.	(1) Any current eligibility determination for access to classified information that is based on an investigation of a scope that meets or exceeds that necessary for the required level of access will provide the basis for a new eligibility determination.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(h)(2)	Determination of eligibility for access to classified information for contractor employees.	(2) The prior investigation will be used without further investigation or adjudication unless the CSA becomes aware of significant derogatory information that was not previously adjudicated.	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
§117.10(i)	Determination of eligibility for access to classified information for contractor employees.	(i) Break in access. There are circumstances when a contractor administratively terminates an employee's access to classified information solely because of no current requirement for such access. If the employee again requires access to classified information and has been in the contractor's continuous employment, and the employee again requires access to classified information, the contractor may provide access to classified information without further investigation, based on CSA guidance, so long as the employee remains eligible for access to classified information and has a current investigation of a scope that meets or exceeds that necessary for the access required and no new derogatory information is known. Any adverse information from or about the employee must continue to be reported while the employee maintains eligibility for access to classified information, even when access to classified information has been administratively terminated.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(j)	Determination of eligibility for access to classified information for contractor employees.	(j) Break in employment.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(j)(1)	Determination of eligibility for access to classified information for contractor employees.	(1) When an employee had a break in employment and now requires access to classified information, the contractor may provide access to classified information based on CSA guidance provided the employee remains eligible for access to classified information and has a current investigation of a scope that meets or exceeds that necessary for the access required.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(j)(2)	Determination of eligibility for access to classified information for contractor employees.	(2) The contractor may not provide access to classified information to an employee who previously was eligible for access to classified information, but has had a break in employment that resulted in a loss of eligibility without a new eligibility determination by the CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(k)	Determination of eligibility for access to classified information for contractor employees.	(k) Non-U.S. citizens.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(k)(1)	Determination of eligibility for access to classified information for contractor employees.	(1) Contractors must make every effort to ensure that non-U.S. citizens are not employed in duties that may require access to classified information. However, compelling reasons may exist to grant access to classified information to a non-U.S. citizen. The CSA may grant such individuals a LAA in those rare circumstances where a non-U.S. citizen possesses unique or unusual skills or expertise that is urgently needed to support a specific USG contract involving access to specified classified information, and a cleared or clearable U.S. citizen is not readily available. The CSA will provide specific procedures for requesting an LAA, to include the need for approval by a GCA senior official.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(k)(2)	Determination of eligibility for access to classified information for contractor employees.	(2) An LAA granted under the provisions of this part is not valid for access to:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(k)(2)(i)	Determination of eligibility for access to classified information for contractor employees.	(i) TOP SECRET information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(k)(2)(ii)	Determination of eligibility for access to classified information for contractor employees.	(ii) RD or FRD.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(k)(2)(iii)	Determination of eligibility for access to classified information for contractor employees.	(iii) Information that has not been determined releasable by a USG designated disclosure authority to the country of which the individual is a citizen.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(k)(2)(iv)	Determination of eligibility for access to classified information for contractor employees.	(iv) Communications security (COMSEC) information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(k)(2)(v)	Determination of eligibility for access to classified information for contractor employees.	(v) Intelligence information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(k)(2)(vi)	Determination of eligibility for access to classified information for contractor employees.	(vi) NATO information. Foreign nationals of a NATO member nation may be authorized access to NATO information provided:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(k)(2)(vi)(A)	Determination of eligibility for access to classified information for contractor employees.	(A) The CSA obtains a NATO security clearance certificate from the individual's country of citizenship.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(k)(2)(vi)(B)	Determination of eligibility for access to classified information for contractor employees.	(B) NATO access is limited to performance on a specific NATO contract.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(k)(2)(vii)	Determination of eligibility for access to classified information for contractor employees.	(vii) Information for which foreign disclosure has been prohibited in whole or in part.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(k)(2)(viii)	Determination of eligibility for access to classified information for contractor employees.	(viii) Information provided to the USG in confidence by a third-party government.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(k)(2)(ix)	Determination of eligibility for access to classified information for contractor employees.	(ix) Classified information furnished by a third-party government.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(l)	Determination of eligibility for access to classified information for contractor employees.	(l) Temporary eligibility for access to classified information. In accordance with SEAD 8 (available at: https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-8_Temporary_Eligibility_U.pdf), the CSA may grant temporary (previously called interim) eligibility for access to classified information, as appropriate, to applicants for access to TOP SECRET, SECRET, and CONFIDENTIAL information. This eligibility may only be granted if there is no evidence of adverse information that calls into question an individual's eligibility for access to classified information. If results are favorable following completion of full investigative requirements, the CSA will update the temporary eligibility determination for access to classified information to be final. In any case, a temporary eligibility determination shall not exceed one year unless approved by the applicable CSA in the system of record. Non-U.S. citizens are not eligible for access to classified information on a temporary basis.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(l)(1)	Determination of eligibility for access to classified information for contractor employees.	(1) A temporary SECRET or CONFIDENTIAL eligibility determination is valid for access to classified information at the level of the eligibility granted. Access to RD, COMSEC information, and NATO information requires a final SECRET eligibility determination.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(l)(2)	Determination of eligibility for access to classified information for contractor employees.	(2) A temporary TOP SECRET eligibility determination is valid for access to TOP SECRET information. If an individual has a temporary Top Secret eligibility determination and has a final Secret eligibility determination based on a previously completed investigation, the temporary Top Secret eligibility determination is valid for access to RD, NATO, and COMSEC information at the Secret or Confidential level. (3) Access to SCI and SAP information based on a temporary eligibility determination is a determination made by the granting authority.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(l)(4)	Determination of eligibility for access to classified information for contractor employees.	(4) When a temporary eligibility determination has been made and derogatory information is subsequently developed, the CSA may withdraw the temporary eligibility pending completion of the processing that is a prerequisite to the final eligibility determination.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(l)(5)	Determination of eligibility for access to classified information for contractor employees.	(5) When a temporary eligibility determination is withdrawn for an individual who is required to be eligible for access to classified information in connection with the entity eligibility determination for access to classified information, the contractor must remove the individual from access to classified information and any KMP position requiring PCL eligibility or the temporary entity eligibility determination will also be withdrawn.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(l)(6)	Determination of eligibility for access to classified information for contractor employees.	(6) Withdrawal of a temporary eligibility determination is not a denial, termination, or revocation of eligibility under this part and may not be appealed.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(m)	Determination of eligibility for access to classified information for contractor employees.	(m) Consultants.	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
§117.10(m)(1)	Determination of eligibility for access to classified information for contractor employees.	(1) A consultant will not access classified information off the premises of the using (hiring) contractor except in connection with authorized classified visits.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(m)(2)	Determination of eligibility for access to classified information for contractor employees.	(2) A contractor may only assign a consultant outside the United States with responsibilities requiring access to classified information when:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(m)(2)(i)	Determination of eligibility for access to classified information for contractor employees.	(i) The consultant agreement between the contractor and consultant includes:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(m)(2)(i)(A)	Determination of eligibility for access to classified information for contractor employees.	(A) Identification of the contract, license, or agreement that requires access to classified information, the level of classified information that is required, and access to FGI by the consultant while assigned outside the United States.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(m)(2)(i)(B)	Determination of eligibility for access to classified information for contractor employees.	(B) A formal agreement that prohibits the consultant from disclosing any classified information related to the contract, license, or agreement as required in paragraph (m)(i)(A) of this section to any party other than the USG or foreign government with which the consultant is meeting, and who possesses the requisite clearance and need to know.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(m)(2)(ii)	Determination of eligibility for access to classified information for contractor employees.	(ii) The consultant and the using contractor will jointly execute the consultant agreement setting forth respective security responsibilities. The contractor will retain an original signed copy of the agreement and will ensure its availability if requested by the CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(m)(2)(iii)	Determination of eligibility for access to classified information for contractor employees.	(iii) The contractor, in consultation with the applicable CSA as appropriate, will determine what threat briefing(s) the consultant should receive before the assignment, and conduct those briefings as part of the consultant's pre-assignment and recurring security training.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(m)(2)(iv)	Determination of eligibility for access to classified information for contractor employees.	(iv) The contractor provides notice of any changes to the consultant agreement to the applicable CSA during assessments or upon CSA request.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(m)(3)	Determination of eligibility for access to classified information for contractor employees.	(3) The using contractor will be the consumer of the consultant services as set forth in the consultant agreement.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(m)(4)	Determination of eligibility for access to classified information for contractor employees.	(4) For security administration purposes, a consultant will be considered an employee of the using contractor for compliance with this part.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.10(m)(5)	Determination of eligibility for access to classified information for contractor employees.	(5) Consultants to GCAs are not under the purview of the NISP and will be processed for determination of eligibility by the GCA in accordance with GCA procedures.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(a)	Foreign Ownership, Control, or Influence (FOCI).	(a) General. Foreign investment can play an important role in maintaining the vitality of the U.S. industrial base. Therefore, it is the intent of the USG to allow foreign investment consistent with the national security interests of the United States. The following FOCI procedures for cleared U.S. entities are intended to mitigate the risks associated with FOCI by ensuring that foreign firms cannot undermine U.S. security to gain unauthorized access to classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(a)(1)	Foreign Ownership, Control, or Influence (FOCI).	(1) The CSA will consider a U.S. entity to be under FOCI when:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(a)(1)(i)	Foreign Ownership, Control, or Influence (FOCI).	(i) A foreign interest has the power to direct or decide matters affecting the entity's management or operations in a manner that could either:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(a)(1)(i)(A)	Foreign Ownership, Control, or Influence (FOCI).	(A) Result in unauthorized access to classified information; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(a)(1)(i)(B)	Foreign Ownership, Control, or Influence (FOCI).	(B) Adversely affect performance of a classified contract or agreement.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(a)(1)(ii)	Foreign Ownership, Control, or Influence (FOCI).	(ii) The foreign government is currently exercising, or could prospectively exercise, that power, whether directly or indirectly, such as::	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(a)(1)(ii)(A)	Foreign Ownership, Control, or Influence (FOCI).	(A) Through ownership of the U.S. entity's securities, by contractual arrangements, or other means, or;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(a)(1)(ii)(B)	Foreign Ownership, Control, or Influence (FOCI).	(B) By the ability to control or influence the election or appointment of one or more members to the entity's governing board.;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(a)(2)	Foreign Ownership, Control, or Influence (FOCI).	(2) When the CSA has determined that an entity is under FOCI, the primary consideration will be the protection of classified information. The CSA will take whatever action is necessary to protect classified information, in coordination with other affected agencies as appropriate.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(a)(3)	Foreign Ownership, Control, or Influence (FOCI).	(3) A U.S. entity that is in process for an entity eligibility determination for access to classified information and subsequently determined to be under FOCI is ineligible for access to classified information unless and until effective security measures have been put in place to negate or mitigate FOCI to the satisfaction of the CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(a)(4)	Foreign Ownership, Control, or Influence (FOCI).	(4) When a contractor determined to be under FOCI is negotiating an acceptable FOCI mitigation or negation measure in good faith, an existing entity eligibility determination may continue in effect so long as there is no indication that classified information is at risk of compromise in consultation with the applicable GCA. The applicable CSA may decide that circumstances involving the FOCI are such that the entity eligibility determination will be invalidated until implementation of an acceptable FOCI mitigation plan.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(a)(5)	Foreign Ownership, Control, or Influence (FOCI).	(5) An existing entity eligibility determination will be invalidated if the contractor is unable or unwilling to negotiate and implement an acceptable FOCI mitigation or negation measure. An existing entity eligibility determination will be revoked if security measures cannot be taken to remove the possibility of unauthorized access to classified information or adverse effect on performance of classified contracts.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(a)(6)	Foreign Ownership, Control, or Influence (FOCI).	(6) Changed conditions, such as a change in ownership, indebtedness, or a foreign intelligence threat, may justify certain adjustments to the security terms under which an entity is operating or, alternatively, that a different FOCI mitigation or negation method be employed. If a changed condition is of sufficient significance, it might also result in a determination that a contractor is no longer considered to be under FOCI, or, conversely, that a contractor is no longer eligible for access to classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(a)(7)	Foreign Ownership, Control, or Influence (FOCI).	(7) The USG reserves the right, and has the obligation, to impose any security method, safeguard, or restriction (including denial, termination or revocation of an entity eligibility determination) it believes necessary to ensure that unauthorized access to classified information is effectively precluded and performance of classified contracts is not adversely affected.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(a)(8)	Foreign Ownership, Control, or Influence (FOCI).	(8) Nothing contained in this section affects the authority of a Federal agency head to limit, deny, or revoke access to classified information under its statutory, regulatory, or contract jurisdiction.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(b)	Foreign Ownership, Control, or Influence (FOCI).	(b) Factors. Factors relating to the entity, relevant foreign interests, and the government of such foreign interests, as appropriate, will be considered in the aggregate to determine whether an applicant entity is under FOCI, its eligibility for access to classified information, and the protective measures required. These factors include:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(b)(1)	Foreign Ownership, Control, or Influence (FOCI).	(1) Record of espionage against U.S. targets, either economic or government.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(b)(2)	Foreign Ownership, Control, or Influence (FOCI).	(2) Record of enforcement actions against the entity for transferring technology without authorization.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(b)(3)	Foreign Ownership, Control, or Influence (FOCI).	(3) Record of compliance with pertinent U.S. laws, regulations, and contracts or agreements.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(b)(4)	Foreign Ownership, Control, or Influence (FOCI).	(4) Type and sensitivity of the information the entity would access.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(b)(5)	Foreign Ownership, Control, or Influence (FOCI).	(5) Source, nature, and extent of FOCI, including whether foreign interests hold a majority or minority position in the entity, taking into consideration the immediate, intermediate, and ultimate parent entities.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(b)(6)	Foreign Ownership, Control, or Influence (FOCI).	(6) Nature of any relevant bilateral and multilateral security and information exchange agreements.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(b)(7)	Foreign Ownership, Control, or Influence (FOCI).	(7) Ownership or control, directly or indirectly, in whole or in part, by a foreign government.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(b)(8)	Foreign Ownership, Control, or Influence (FOCI).	(8) Any other factor that indicates or demonstrates capability of foreign interests to control or influence the entity's operations or management.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(c)	Foreign Ownership, Control, or Influence (FOCI).	(c) Procedures. An entity is required to complete an SF 328 during the process for an entity eligibility determination or when significant changes occur to information previously submitted. In the case of a corporate family, the form may be a consolidated response rather than separate submissions from individual members of the corporate family based on CSA guidance.	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
§117.11(c)(1)	Foreign Ownership, Control, or Influence (FOCI).	(1) If an entity provides any affirmative answers on the SF 328, or the CSA receives other information which indicates that the applicant entity may be under FOCI, the CSA will make a risk-based determination regarding the relative significance of the information in regard to:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(c)(1)(i)	Foreign Ownership, Control, or Influence (FOCI).	(i) Whether the applicant is under FOCI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(c)(1)(ii)	Foreign Ownership, Control, or Influence (FOCI).	(ii) The extent and manner to which the FOCI represents a risk to the national security or may adversely impact classified contract performance.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(c)(1)(iii)	Foreign Ownership, Control, or Influence (FOCI).	(iii) The type of actions, if any, that would be necessary to mitigate or negate the effects of FOCI to a level deemed acceptable to the USG. The CSA will advise entities on the CSA's appeal channels for disputing CSA FOCI determinations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(c)(2)	Foreign Ownership, Control, or Influence (FOCI).	(2) When an entity with a favorable eligibility determination enters into negotiations for the proposed merger, acquisition, or takeover by a foreign interest, the entity will submit notification to the CSA of the commencement of such negotiations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(c)(2)(i)	Foreign Ownership, Control, or Influence (FOCI).	(i) The submission will include the type of transaction under negotiation (e.g., stock purchase, asset purchase), the identity of the potential foreign interest investor, and a plan to negate or mitigate the FOCI by a method outlined in paragraph (d) of this section.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(c)(2)(ii)	Foreign Ownership, Control, or Influence (FOCI).	(ii) The entity will submit copies of loan, purchase, and shareholder agreements, annual reports, bylaws, articles of incorporation, partnership agreements, other organizational documents, and reports filed with other Federal agencies to the CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)	Foreign Ownership, Control, or Influence (FOCI).	(d) FOCI action plans.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(1)	Foreign Ownership, Control, or Influence (FOCI).	(1) When FOCI factors not related to ownership are present, the CSA will determine if positive measures will assure the CSA that the foreign interest can be effectively mitigated and cannot otherwise adversely affect performance on classified contracts. Examples of such measures include:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(1)(i)	Foreign Ownership, Control, or Influence (FOCI).	(i) Modification or termination of loan agreements, contracts, and other understandings with foreign interests.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(1)(ii)	Foreign Ownership, Control, or Influence (FOCI).	(ii) Diversification or reduction of foreign-source income.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(1)(iii)	Foreign Ownership, Control, or Influence (FOCI).	(iii) Demonstration of financial viability independent of foreign interests.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(1)(iv)	Foreign Ownership, Control, or Influence (FOCI).	(iv) Elimination or resolution of problem debt.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(1)(v)	Foreign Ownership, Control, or Influence (FOCI).	(v) Assignment of specific oversight duties and responsibilities to board members.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(1)(vi)	Foreign Ownership, Control, or Influence (FOCI).	(vi) Formulation of special executive-level security committees to consider and oversee matters that affect the performance of classified contracts.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(1)(vii)	Foreign Ownership, Control, or Influence (FOCI).	(vii) Physical or organizational separation of the contractor component performing on classified contracts.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(1)(viii)	Foreign Ownership, Control, or Influence (FOCI).	(viii) Adoption of special board resolutions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(1)(ix)	Foreign Ownership, Control, or Influence (FOCI).	(ix) Other actions that negate or mitigate foreign control or influence.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(1)(x)	Foreign Ownership, Control, or Influence (FOCI).	(x) A combination of these methods, as determined by the CSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)	Foreign Ownership, Control, or Influence (FOCI).	(2) When FOCI factors related to ownership are present, methods the CSA may apply to negate or mitigate the risk of foreign ownership include, but are not limited to:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(i)	Foreign Ownership, Control, or Influence (FOCI).	(i) Board resolution.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(i)(A)	Foreign Ownership, Control, or Influence (FOCI).	(A) When a foreign interest does not possess voting interests sufficient to elect, or otherwise is not entitled to representation on the entity's governing board, a resolution(s) by the governing board may be adequate. In the resolution, the governing board will:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(i)(A)(1)	Foreign Ownership, Control, or Influence (FOCI).	(1) Identify the foreign shareholder.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(i)(A)(2)	Foreign Ownership, Control, or Influence (FOCI).	(2) Describe the type and number of foreign-owned shares.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(i)(A)(3)	Foreign Ownership, Control, or Influence (FOCI).	(3) Acknowledge the entity's obligation to comply with all industrial security program requirements.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(i)(A)(4)	Foreign Ownership, Control, or Influence (FOCI).	(4) Certify that the foreign owner does not require, will not have, and can be effectively precluded from unauthorized access to all classified information entrusted to or held by the entity.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(i)(B)	Foreign Ownership, Control, or Influence (FOCI).	(B) The governing board will provide for annual certifications to the CSA acknowledging the continued effectiveness of the resolution.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(i)(C)	Foreign Ownership, Control, or Influence (FOCI).	(C) The entity will distribute to members of its governing board and to its KMP copies of such resolutions, and report in the entity's corporate records the completion of such distribution.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(ii)	Foreign Ownership, Control, or Influence (FOCI).	(ii) Security control agreement (SCA). When a foreign interest does not effectively own or control an entity (i.e., the entity is under U.S. control), but the foreign interest is entitled to representation on the entity's governing board, an SCA may be adequate. At least one cleared U.S. citizen must serve as an outside director on the entity's governing board. There are no access limitations under an SCA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iii)	Foreign Ownership, Control, or Influence (FOCI).	(iii) SSA. When a foreign interest effectively owns or controls an entity, an SSA may be adequate. An SSA is an arrangement that, based upon an assessment of the source and nature of FOCI and FOCI factors, imposes various industrial security measures within an institutionalized set of entity practices and procedures. The SSA preserves the foreign owner's right to be represented on the entity's board or governing body with a direct voice in the entity's business management, while denying the foreign owner majority representation and unauthorized access to classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iii)(A)	Foreign Ownership, Control, or Influence (FOCI).	(A) Requirement for a National Interest Determination (NID). Unless otherwise prohibited by law or regulation, the applicable CSA must determine whether allowing an entity access to proscribed information under an SSA is consistent with national security interests of the U.S. with concurrence from controlling agencies, as applicable. Such NIDs will be made as part of an entity eligibility determination or because of a changed condition when a GCA requires an entity to have access to proscribed information and the CSA proposes an SSA as the mitigation measure. The NID can be program, project, or contract specific.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iii)(B)	Foreign Ownership, Control, or Influence (FOCI).	(B) NID process:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iii)(B)(1)	Foreign Ownership, Control, or Influence (FOCI).	(1) The CSA makes a NID for TOP SECRET or SAP information to which the entity requires access. Contractors should be aware that DOE Order 470.4B provides additional information and requirements for processing NID requests for access to RD.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iii)(B)(2)	Foreign Ownership, Control, or Influence (FOCI).	(2) In cases in which any category of the proscribed information is controlled by another agency (ODNI for SCI, DOE for RD, the National Security Agency (NSA) for COMSEC), the CSA asks that controlling agency to concur or non-concur on the NID for that category of information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iii)(B)(3)	Foreign Ownership, Control, or Influence (FOCI).	(3) The CSA informs the GCA and the entity when the NID is complete. In cases involving SCI, RD, or COMSEC, the CSA also informs the GCA and the entity when a controlling agency concurs or non-concurs on that agency's category of proscribed information. The entity may begin accessing a category of proscribed information once the CSA informs the GCA and the	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11	Foreign Ownership, Control, or Influence (FOCI).	entity that the controlling agency concurs, even if other categories of proscribed information are pending concurrence.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iii)(B)(4)	Foreign Ownership, Control, or Influence (FOCI).	(4) An entity's access to SCI, RD, or COMSEC remains in effect so long as the entity remains eligible for access to classified information and the contract or agreement (or program or project) which imposes the requirement for access to those categories of proscribed information remains in effect, except under any of the following circumstances:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iii)(B)(4)(i)	Foreign Ownership, Control, or Influence (FOCI).	(i) The CSA, GCA, or controlling agency becomes aware of adverse information that impacts the entity eligibility determination.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iii)(B)(4)(ii)	Foreign Ownership, Control, or Influence (FOCI).	(ii) The CSA's threat assessment pertaining to the entity indicates a risk to one of the categories of proscribed information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iii)(B)(4)(iii)	Foreign Ownership, Control, or Influence (FOCI).	(iii) The CSA becomes aware of any material change regarding the source, nature, and extent of FOCI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iii)(B)(4)(iv)	Foreign Ownership, Control, or Influence (FOCI).	(iv) The entity's record of NISP compliance, based on CSA reviews, becomes less than satisfactory. Consult DOE Order 470.4B for additional information and requirements for processing NID requests for access to RD.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iii)(B)(5)	Foreign Ownership, Control, or Influence (FOCI).	(5) Under any of the circumstances in paragraphs (d)(2)(iii)(B)(4)(i) through (d)(2)(iii)(B)(4)(iv) in this section, the CSA determines whether the entity remains eligible for access to classified information, it must change the FOCI mitigation measure in order to remain eligible for access to classified information, or the CSA must terminate or revoke the access to classified information.	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
§117.11(d)(2)(iii)(B)(6)	Foreign Ownership, Control, or Influence (FOCI).	(6) When an entity is eligible for access to classified information that includes a favorable NID for SCI, RD, or COMSEC, the CSA does not have to request a new NID concurrence for the same entity if the access to classified information requirements for the relevant category of proscribed information and terms remain unchanged for:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iii)(B)(6)(i)	Foreign Ownership, Control, or Influence (FOCI).	(i) Renewing the contract or agreement.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iii)(B)(6)(ii)	Foreign Ownership, Control, or Influence (FOCI).	(ii) New task orders issued under the contract or agreement.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iii)(B)(6)(iii)	Foreign Ownership, Control, or Influence (FOCI).	(iii) A new contract or agreement that contains the same provisions as the previous one (this usually applies when the contract or agreement is for a program or project.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iii)(B)(6)(iv)	Foreign Ownership, Control, or Influence (FOCI).	(iv) Renewing the SSA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iii)(B)(7)	Foreign Ownership, Control, or Influence (FOCI).	(7) Under certain conditions, entities under an SSA may not require a NID for one or more categories of proscribed information in accordance with CSA-provided guidance. Categories of proscribed information for entities under SSAs not requiring a NID will be recorded in the CSA's system of record for entity eligibility determinations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iv)	Foreign Ownership, Control, or Influence (FOCI).	(iv) Voting Trust (VT) or Proxy Agreement (PA). The VT and the PA are arrangements that vest the voting rights of the foreign-owned stock in cleared U.S. citizens approved by the USG. Under a VT, the foreign owner transfers legal title its ownership interests in the entity to the trustees. Under a PA, the foreign owner's voting rights are conveyed to the proxy holders. Neither arrangement imposes any restrictions on the entity's eligibility to have access to classified information or to compete for classified contracts.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iv)(A)	Foreign Ownership, Control, or Influence (FOCI).	(A) Establishment of a VT or PA involves the selection of trustees or proxy holders, all of whom must become members of the entity's governing board. Both arrangements must provide for the	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11	Foreign Ownership, Control, or Influence (FOCI).	exercise of all prerogatives of ownership by the trustees or proxy holders with complete freedom to act independently from the foreign owners, except as provided in the VT or PA. The arrangements may limit the authority of the trustees or proxy holders by requiring approval be obtained from the foreign owner with respect to matters such as:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iv)(A)(1)	Foreign Ownership, Control, or Influence (FOCI).	(1) The sale or disposal of the entity's assets or a substantial part thereof.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iv)(A)(2)	Foreign Ownership, Control, or Influence (FOCI).	(2) Pledges, mortgages, or other encumbrances on the entity's assets, capital stock, or ownership interests.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iv)(A)(3)	Foreign Ownership, Control, or Influence (FOCI).	(3) Mergers, consolidations, or reorganizations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iv)(A)(4)	Foreign Ownership, Control, or Influence (FOCI).	(4) Dissolution.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iv)(A)(5)	Foreign Ownership, Control, or Influence (FOCI).	(5) Filing of a bankruptcy petition.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iv)(B)	Foreign Ownership, Control, or Influence (FOCI).	(B) The trustees or proxy holders may consult with the foreign owner, or vice versa, where otherwise consistent with U.S. laws, regulations, and the terms of the VT or PA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(iv)(C)	Foreign Ownership, Control, or Influence (FOCI).	(C) The trustees or proxy holders assume full responsibility for the foreign owner's voting interests and for exercising all governance and management prerogatives relating thereto to ensure the foreign owner will be insulated from the entity, thereby solely retaining the status of a beneficiary. The entity must be organized, structured, and financed to be capable of operating as a viable business entity and independent from the foreign owners' interests that required FOCI mitigation or negation.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(d)(2)(v)	Foreign Ownership, Control, or Influence (FOCI).	(v) Combination measures. The CSA may apply combinations of the measures in paragraphs (d)(2)(i) through (d)(2)(iv) in this section or other similar measures that effectively mitigate or negate the risks involved with foreign ownership.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(e)	Foreign Ownership, Control, or Influence (FOCI).	(e) Limited entity eligibility determination due to FOCI. In accordance with the provisions of this section and CSA-provided guidance, a limited entity eligibility determination may be an option for a single, narrowly defined contract, agreement, or circumstance for entities under FOCI without mitigation or negation. Limitations on access to classified information are inherent with the granting of limited entity eligibility determinations and are imposed upon all of the entity's employees regardless of citizenship.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(e)(1)	Foreign Ownership, Control, or Influence (FOCI).	(1) In exceptional circumstances, when a entity is under FOCI, the CSA may decide that a limited entity eligibility determination is appropriate when the entity is unable or unwilling to implement FOCI mitigation or negation measures, and the conditions in paragraphs (e)(1)(i) through (iii) of this section are met. This is not the same as a limited entity eligibility determination for purposes not related to FOCI. Information on limited entity eligibility determinations for purposes other than FOCI can be found in §117.9(m). A CSA may decide that a limited entity eligibility is appropriate for a entity under FOCI if:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(e)(1)(i)	Foreign Ownership, Control, or Influence (FOCI).	(i) The limited entity eligibility determination is in accordance with national security interests and a GCA has informed the CSA that access to classified information by the contractor is essential to contract or agreement performance.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(e)(1)(ii)	Foreign Ownership, Control, or Influence (FOCI).	(ii) There is an industrial security agreement with the foreign government of the country from which the FOCI is derived.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(e)(1)(iii)	Foreign Ownership, Control, or Influence (FOCI).	(iii) The contractor meets all other entity eligibility requirements outlined in §117.9(c) except that KMP, other than the FSO, may be citizens of the country from which the FOCI derives and the United States has obtained security assurances at the appropriate level from that country.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(e)(2)	Foreign Ownership, Control, or Influence (FOCI).	(2) A U.S. subsidiary of a foreign entity may be sponsored for a limited entity eligibility determination by a foreign government when the foreign government desires to award a contract or agreement to the U.S. subsidiary that involves access to only that classified information for which the foreign government is the OCA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(e)(3)	Foreign Ownership, Control, or Influence (FOCI).	(3) Limited entity eligibility determinations are specific to the classified information for the requesting GCA or foreign government and the single narrowly defined contract, agreement, or circumstance the request was based on. The limited entity eligibility determination will only be verified to that GCA or foreign government for the authorized level of access to classified information and any limitations to that access to classified information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(e)(4)	Foreign Ownership, Control, or Influence (FOCI).	(4) A limited entity eligibility determination is not an option for contractors that require access to proscribed information when a foreign government has ownership or control over the entity.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(e)(5)	Foreign Ownership, Control, or Influence (FOCI).	(5) Release of classified information must be in conformity with the U.S. National Disclosure Policy-1 (provided to designated disclosure authorities on a need-to-know basis from the Office of the Under Secretary of Defense for Policy, Defense Technology Security Administration).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(e)(6)	Foreign Ownership, Control, or Influence (FOCI).	(6) A limited entity eligibility determination will be administratively terminated when there is no longer a need for the contractor to access the classified information for which it was sponsored. Administrative termination of one limited entity eligibility determination does not impact a contractor's other limited entity eligibility determinations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(e)(7)	Foreign Ownership, Control, or Influence (FOCI).	(7) If there is no industrial security agreement with the foreign government of the country from which the FOCI is derived, in extraordinary circumstances, a limited entity eligibility determination may also be granted if there is a compelling need to do so consistent with U.S. national security interests and the GCA has informed the applicable CSA that access to classified information by the contractor is essential to contract or agreement performance. Under this circumstance, the entity must follow all provisions of this rule.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(f)	Foreign Ownership, Control, or Influence (FOCI).	(f) Qualifications of trustees, proxy holders, and outside directors. Individuals who serve as trustees, proxy holders, or outside directors must meet the following criteria:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(f)(1)	Foreign Ownership, Control, or Influence (FOCI).	(1) Trustees and proxy holders must be resident U.S. citizens who can exercise governance and management prerogatives relating to their position in a way that ensures that the foreign owner can be effectively insulated from the entity.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(f)(2)	Foreign Ownership, Control, or Influence (FOCI).	(2) Outside directors must be resident U.S. citizens who can exercise governance and management prerogatives relating to their position in a way that ensures that the foreign owner can be effectively separated from the entity's classified work.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(f)(3)	Foreign Ownership, Control, or Influence (FOCI).	(3) New trustees, proxy holders, and outside directors must be completely disinterested individuals with no prior involvement with the entity, the entities with which it is affiliated, or the foreign owner.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(f)(4)	Foreign Ownership, Control, or Influence (FOCI).	(4) The CSA may consider other circumstances that may affect an individual's eligibility to serve effectively including the number of boards on which the individual serves, the length of time serving on any other governance boards, and other factors in accordance with CSA-provided guidance.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(f)(5)	Foreign Ownership, Control, or Influence (FOCI).	(5) Trustees, proxy holders, and outside directors must be determined eligible for access to classified information at the level of the entity eligibility determination for access to classified information. Individuals who are serving as trustees, proxy holders, or outside directors as part of a mitigation measure for the entity are not considered to have prior involvement solely by performing that role for purposes of paragraph (f)(3) of this section.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(g)	Foreign Ownership, Control, or Influence (FOCI).	(g) Government security committee (GSC). Under a VT, PA, SSA, or SCA, the contractor is required to establish a permanent committee of its board of directors, known as the GSC.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(g)(1)	Foreign Ownership, Control, or Influence (FOCI).	(1) Unless otherwise approved by the CSA, the GSC consists of trustees, proxy holders, or outside directors and those officer directors who have been determined to be eligible for access to classified information.	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
§117.11(g)(2)	Foreign Ownership, Control, or Influence (FOCI).	(2) The members of the GSC are required to ensure that the contractor adheres to laws and regulations and maintains internal entity policies and procedures to safeguard classified information entrusted to it. The GSC ensures that violations of those policies and procedures are promptly investigated and reported to the appropriate authority when it has been determined that a violation has occurred.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(g)(3)	Foreign Ownership, Control, or Influence (FOCI).	(3) The contractor's FSO will be the principal advisor to the GSC and attend GSC meetings. The chairman of the GSC must concur with the appointment and replacement of FSOs selected by management. The FSO functions will be carried out under the authority of the GSC.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(h)	Foreign Ownership, Control, or Influence (FOCI).	(h) Additional procedures for FOCI mitigation or negation measures. In addition to the basic requirements of the FOCI mitigation or negation agreement, the entity may be required to document and implement additional procedures based upon the circumstances of an entity's operations. Those additional procedures will be established in supplements to the FOCI mitigation agreement to allow for flexibility as circumstances change without having to renegotiate the entire agreement. When making use of supplements, the CSA does not consider the FOCI mitigation measure final until the CSA has approved the required supplements. These supplements may include:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(h)(1)	Foreign Ownership, Control, or Influence (FOCI).	(1) Technology control plan (TCP). A TCP approved by the CSA will be developed and implemented by those entities cleared under a VT, PA, SSA and SCA and when otherwise deemed appropriate by the CSA. The TCP will prescribe all security measures determined necessary to reasonably prevent the possibility of access by non-U.S. citizen employees and visitors to information for which they are not authorized. The TCP will also prescribe measures designed to assure that access by non-U.S. citizens is strictly limited to only that specific information for which appropriate USG disclosure authorization has been obtained, e.g., an approved export license or technical assistance agreement. Unique badging, escort, segregated work area, security indoctrination schemes, and other measures will be included, as appropriate.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(h)(2)	Foreign Ownership, Control, or Influence (FOCI).	(2) Electronic communications plan (ECP). The contractor will develop and implement an ECP, subject to CSA approval, tailored to the contractor's operations to verify that electronic controls are in place for clear technical and logical separation of electronic communications and networks between the contractor, the foreign interest, and its affiliates. The purpose is to prevent the unauthorized disclosure of classified information to the foreign parent or its affiliates. The contractor will include in the ECP a detailed network description and configuration diagram that clearly delineates which networks will be shared and which will be protected from access by the foreign parent or its affiliates. The network description will address firewalls, remote administration, monitoring, maintenance, and separate email servers, as appropriate.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(h)(3)	Foreign Ownership, Control, or Influence (FOCI).	(3) Affiliated operations plan. There may be circumstances when the parties to a transaction propose in the FOCI action plan that the U.S. contractor provides certain services for the foreign interest or enters into arrangements with the foreign interest, or the foreign interest provides services for or enters into arrangements with the U.S. contractor. In such circumstances, the contractor will document a plan, subject to CSA approval, outlining the entity's consolidated policies and procedures regarding the control of affiliated operations, regardless of whether such endeavors are administrative, operational, or commercial, performed directly or through third-party service providers, within the entity or among any of the enitity's controlled entities, or the foreign interest and its affiliates.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(h)(4)	Foreign Ownership, Control, or Influence (FOCI).	(4) Facilities location plan. When a contractor is potentially collocated with or in close proximity to its foreign parent or an affiliate, the contractor will prepare a facilities location plan to assist the CSA in determining if the contractor is collocated or if the close proximity can be allowed under the FOCI mitigation plan. A U.S. entity generally cannot be collocated with the foreign parent or affiliate, i.e., at the same address or in the same location.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(i)	Foreign Ownership, Control, or Influence (FOCI).	(i) Annual review and certification.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(i)(1)	Foreign Ownership, Control, or Influence (FOCI).	(1) Annual review. The CSA will meet at least annually, and otherwise as required by circumstances, with the GSCs of contractors operating under a VT, PA, SSA, or SCA to review the purpose and effectiveness of the clearance arrangement and to establish a common understanding of the operating requirements and their implementation. These reviews will include an examination of:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(i)(1)(i)	Foreign Ownership, Control, or Influence (FOCI).	(i) Acts of compliance or noncompliance with the approved security arrangement, standard rules, and applicable laws and regulations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(i)(1)(ii)	Foreign Ownership, Control, or Influence (FOCI).	(ii) Problems or impediments associated with the practical application or utility of the security arrangement.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(i)(1)(iii)	Foreign Ownership, Control, or Influence (FOCI).	(iii) Whether security controls, practices, or procedures warrant adjustment.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(i)(2)	Foreign Ownership, Control, or Influence (FOCI).	(2) Annual certification. For contractors operating under a VT, PA, SSA, or SCA, the chairman of the GSC will submit to the CSA one year from the effective date of the agreement and annually thereafter, an implementation and compliance report. Such reports will include:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(i)(2)(i)	Foreign Ownership, Control, or Influence (FOCI).	(i) A detailed description of the manner in which the contractor is carrying out its obligations under the agreement.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(i)(2)(ii)	Foreign Ownership, Control, or Influence (FOCI).	(ii) Changes to security procedures, implemented or proposed, and the reasons for those changes.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(i)(2)(iii)	Foreign Ownership, Control, or Influence (FOCI).	(iii) A detailed description of any acts of noncompliance, whether inadvertent or intentional, with a discussion of remedial measures, including steps taken to prevent such acts from recurring.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(i)(2)(iv)	Foreign Ownership, Control, or Influence (FOCI).	(iv) Any changes, or impending changes, of KMP or key board members, including the reasons therefore.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(i)(2)(v)	Foreign Ownership, Control, or Influence (FOCI).	(v) Any changes or impending changes in the organizational structure or ownership, including any reorganizations, acquisitions, mergers, or divestitures.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(i)(2)(vi)	Foreign Ownership, Control, or Influence (FOCI).	(vi) Any other issues that could have a bearing on the effectiveness of the applicable agreement.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(j)	Foreign Ownership, Control, or Influence (FOCI).	(j) Transactions involving foreign persons, and the Committee on Foreign Investment in the United States (CFIUS).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(j)(1)	Foreign Ownership, Control, or Influence (FOCI).	(1). The CFIUS is a USG interagency committee chaired by the Treasury Department that conducts assessments, reviews and investigations of transactions that could result in foreign control of a U.S. business, and certain non-controlling investments and certain real estate transactions involving foreign persons under 50 U.S.C. 4565.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(j)(2)	Foreign Ownership, Control, or Influence (FOCI).	(2) In CFIUS cases where the acquired U.S. person requires access to classified information, the CFIUS assessment, review or investigation, as applicable, and the CSA industrial security FOCI review are carried out in parallel, but are separate processes with different time constraints and considerations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.11(j)(3)	Foreign Ownership, Control, or Influence (FOCI).	(3) The CSA will promptly advise the parties in a transaction under CFIUS review that would require FOCI negation or mitigation measures if consummated, to submit to the CSA a plan to negate or mitigate FOCI. If it appears that an agreement cannot be reached on material terms of a FOCI action plan, or if the U.S. person that is a party, or in applicable cases, a subject of the proposed transaction fails to comply with the FOCI reporting requirements of this part, the CSA may recommend a full investigation of the transaction by the CFIUS to determine the effects on national security.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
§117.12(a)	Security training and briefings.	(a) General. Contractors will provide all cleared employees with security training and briefings commensurate with their involvement with classified information.	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	
§117.12(a)	Security training and briefings.	(a) General. Contractors will provide all cleared employees with security training and briefings commensurate with their involvement with classified information.	Functional	Intersects With	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.	5	