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: **Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012**
Focal Document URL: https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-dow-dfars-252-204-7012.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
252.204-7012	Safeguarding Covered Defense Information and Cyber Incident Reporting	As prescribed in 204.7304(c), use the following clause:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
252.204-7012(a)	Definitions	See fDE for details	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
252.204-7012(b)	Adequate security	The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
252.204-7012(b)	Adequate security	The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
252.204-7012(b)	Adequate security	The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
252.204-7012(b)	Adequate security	The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
252.204-7012(b)	Adequate security	The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
252.204-7012(b)	Adequate security	The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:	Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are:(1) Implemented correctly; and(2) Operating as intended.	5	
252.204-7012(b)	Adequate security	The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:	Functional	Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.	5	
252.204-7012(b)	Adequate security	The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:	Functional	Intersects With	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications, Services and/or Data (TAASD) under their control on an ongoing basis for applicable threats and risks, as well as to ensure security, compliance and resilience controls are operating as intended.	5	
252.204-7012(b)	Adequate security	The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
252.204-7012(b)	Adequate security	The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	8	
252.204-7012(b)(1)	Adequate security	For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
252.204-7012(b)(1)(i)	Adequate security	Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
252.204-7012(b)(1)(ii)	Adequate security	Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
252.204-7012(b)(2)	Adequate security	For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
252.204-7012(b)(2)(i)	Adequate security	Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at https://csrc.nist.gov/publications/sp800) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
252.204-7012(b)(2)(ii)(A)	Adequate security	The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
252.204-7012(b)(2)(ii)(B)	Adequate security	The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5	
252.204-7012(b)(2)(ii)(B)	Adequate security	The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	milestones (POA&M) or similar methodology, that formally documents, at a minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable;(7) Point of Contact (POC) (e.g., asset/process owner);(8) Resources required to conduct remediation actions;(9) Planned remedial actions to the deficiency(ies);(10) Proposed remediation timelines; and(11) Disposition	8	
252.204-7012(b)(2)(ii)(B)	Adequate security	The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
252.204-7012(b)(2)(ii)(C)	Adequate security	If the DoD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	8	
252.204-7012(b)(2)(ii)(D)	Adequate security	If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/documents-templates/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
252.204-7012(b)(3)	Adequate security	Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
252.204-7012(c)	Cyber incident reporting requirement	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
252.204-7012(c)(1)	Cyber incident reporting requirement	When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
252.204-7012(c)(1)(i)	Cyber incident reporting requirement	Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	8	
252.204-7012(c)(1)(ii)	Cyber incident reporting requirement	Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.	Functional	Subset Of	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	10	
252.204-7012(c)(2)	Cyber incident report	The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at https://dibnet.dod.mil.	Functional	Subset Of	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	10	
252.204-7012(c)(3)	Medium assurance certificate requirement	In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/.	Functional	Subset Of	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	10	
252.204-7012(d)	Malicious software	When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.	Functional	Subset Of	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	10	
252.204-7012(e)	Media preservation and protection	When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.	Functional	Subset Of	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	10	
252.204-7012(f)	Access to additional information or equipment necessary for forensic analysis	Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.	Functional	Intersects With	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
252.204-7012(g)	Cyber incident damage assessment activities	If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.	Functional	Intersects With	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	5	
252.204-7012(h)	DoD safeguarding and use of contractor attributional/proprietary information	The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
252.204-7012(i)	Use and release of contractor attributional/proprietary information not created by or for DoD	Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD—-	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
252.204-7012(i)(1)	Use and release of contractor attributional/proprietary information not created by or for DoD	To entities with missions that may be affected by such information;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
252.204-7012(i)(2)	Use and release of contractor attributional/proprietary information not created by or for DoD	To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
252.204-7012(i)(3)	Use and release of contractor attributional/proprietary information not created by or for DoD	To Government entities that conduct counterintelligence or law enforcement investigations;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
252.204-7012(i)(4)	Use and release of contractor attributional/proprietary information not created by or for DoD	For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
252.204-7012(i)(5)	Use and release of contractor attributional/proprietary information not created by or for DoD	To a support services contractor ("recipient") that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
252.204-7012(j)	Use and release of contractor attributional/proprietary information created by or for DoD	Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
252.204-7012(k)	N/A	The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
252.204-7012(l)	Other safeguarding or reporting requirements	The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
252.204-7012(m)	Subcontracts	The Contractor shall—	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
252.204-7012(m)(1)	Subcontracts	Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial products or commercial services, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
252.204-7012(m)(2)	Subcontracts	Require subcontractors to—	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
252.204-7012(m)(2)(i)	Subcontracts	Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and	Functional	Subset Of	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	10	