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: **FAR 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems (Nov 2021)**
Focal Document URL: https://www.acquisition.gov/far/52.204-21
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-far-52-204-21.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
52.204-21(a)	N/A	Read FAR 52.204-21(a) for full text (https://www.acquisition.gov/far/52.204-21)	Functional	Intersects With	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	5	
52.204-21(b)	N/A	This is merely a section title without content.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
52.204-21(b)(1)	N/A	The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
52.204-21(b)(1)	N/A	The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:	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	
52.204-21(b)(1)	N/A	The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	8	
52.204-21(b)(1)	N/A	The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	8	
52.204-21(b)(1)	N/A	The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:	Functional	Subset Of	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.	10	
52.204-21(b)(1)	N/A	The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	8	
52.204-21(b)(1)	N/A	The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	8	
52.204-21(b)(1)(i)	Authorized Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
52.204-21(b)(1)(i)	Authorized Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
52.204-21(b)(1)(i)	Authorized Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
52.204-21(b)(1)(i)	Authorized Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Functional	Intersects With	Automated System Account Management (Directory Services)	IAC-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
52.204-21(b)(1)(i)	Authorized Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Functional	Equal	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	10	
52.204-21(b)(1)(i)	Authorized Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
52.204-21(b)(1)(i)	Authorized Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
52.204-21(b)(1)(i)	Authorized Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
52.204-21(b)(1)(ii)	Transaction & Function Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
52.204-21(b)(1)(ii)	Transaction & Function Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
52.204-21(b)(1)(iii)	External Connections	Verify and control/limit connections to and use of external information systems.	Functional	Equal	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	10	
52.204-21(b)(1)(iii)	External Connections	Verify and control/limit connections to and use of external information systems.	Functional	Intersects With	Ad-Hoc Transfers	DCH-17	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	3	
52.204-21(b)(1)(iii)	External Connections	Verify and control/limit connections to and use of external information systems.	Functional	Intersects With	Limits of Authorized Use	DCH-13.1	Mechanisms exist to prohibit external parties, including Technology Assets, Applications and/or Services (TAAS), from storing, processing and transmitting data unless authorized individuals first:(1) Verifying the implementation of required security, compliance and/or resilience controls; or(2) Retaining a processing agreement with the entity hosting the external TAAS.	5	
52.204-21(b)(1)(iv)	Control Public Information	Control information posted or processed on publicly accessible information systems.	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
52.204-21(b)(1)(iv)	Control Public Information	Control information posted or processed on publicly accessible information systems.	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	5	
52.204-21(b)(1)(iv)	Control Public Information	Control information posted or processed on publicly accessible information systems.	Functional	Intersects With	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5	
52.204-21(b)(1)(iv)	Control Public Information	Control information posted or processed on publicly accessible information systems.	Functional	Intersects With	Sensitive Data In Public Cloud Providers	CLD-10	Mechanisms exist to limit and manage the storage of sensitive/regulated data in public cloud providers.	5	
52.204-21(b)(1)(iv)	Control Public Information	Control information posted or processed on publicly accessible information systems.	Functional	Intersects With	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	8	
52.204-21(b)(1)(iv)	Control Public Information	Control information posted or processed on publicly accessible information systems.	Functional	Intersects With	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	8	
52.204-21(b)(1)(iv)	Control Public Information	Control information posted or processed on publicly accessible information systems.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	8	
52.204-21(b)(1)(iv)	Control Public Information	Control information posted or processed on publicly accessible information systems.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	8	
52.204-21(b)(1)(iv)	Control Public Information	Control information posted or processed on publicly accessible information systems.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	8	
52.204-21(b)(1)(iv)	Control Public Information	Control information posted or processed on publicly accessible information systems.	Functional	Intersects With	Web Security	WEB-01	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.	3	
52.204-21(b)(1)(iv)	Control Public Information	Control information posted or processed on publicly accessible information systems.	Functional	Intersects With	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized Technology Assets, Applications and/or Services (TAAS) on certain services, protocols and ports.	3	
52.204-21(b)(1)(iv)	Control Public Information	Control information posted or processed on publicly accessible information systems.	Functional	Intersects With	Client-Facing Web Services	WEB-04	Mechanisms exist to deploy reasonably-expected security, compliance and resilience controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	3	
52.204-21(b)(1)(v)	Identification	Identify information system users, processes acting on behalf of users, or devices.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	8	
52.204-21(b)(1)(v)	Identification	Identify information system users, processes acting on behalf of users, or devices.	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	8	
52.204-21(b)(1)(v)	Identification	Identify information system users, processes acting on behalf of users, or devices.	Functional	Intersects With	Automated System Account Management (Directory Services)	IAC-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	8	
52.204-21(b)(1)(vi)	Authentication	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
52.204-21(b)(1)(vi)	Authentication	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5	
52.204-21(b)(1)(vi)	Authentication	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Functional	Intersects With	Automated System Account Management (Directory Services)	IAC-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
52.204-21(b)(1)(vii)	Media Disposal	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
52.204-21(b)(1)(vii)	Media Disposal	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	8	
52.204-21(b)(1)(vii)	Media Disposal	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
52.204-21(b)(1)(vii)	Media Disposal	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	Functional	Equal	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	10	
52.204-21(b)(1)(vii)	Media Disposal	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	8	
52.204-21(b)(1)(viii)	Limit Physical Access	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Functional	Subset Of	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	10	
52.204-21(b)(1)(viii)	Limit Physical Access	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Functional	Intersects With	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	8	
52.204-21(b)(1)(viii)	Limit Physical Access	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Functional	Intersects With	Access To Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility.	8	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
52.204-21(b)(1)(viii)	Limit Physical Access	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	
52.204-21(b)(1)(viii)	Limit Physical Access	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	
52.204-21(b)(1)(viii)	Limit Physical Access	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
52.204-21(b)(1)(viii)	Limit Physical Access	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Functional	Intersects With	Access Control for Output Devices	PES-12.2	Physical security mechanisms exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output.	5	
52.204-21(b)(1)(ix)	Escort Visitors	Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	8	
52.204-21(b)(1)(ix)	Escort Visitors	Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
52.204-21(b)(1)(ix)	Escort Visitors	Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.	Functional	Intersects With	Distinguish Visitors from On-Site Personnel	PES-06.1	Physical access control mechanisms exist to easily distinguish between onsite personnel and visitors, especially in areas where sensitive/regulated data is accessible.	3	
52.204-21(b)(1)(ix)	Escort Visitors	Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.	Functional	Intersects With	Restrict Unescorted Access	PES-06.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.	5	
52.204-21(b)(1)(x)	Boundary Protection	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
52.204-21(b)(1)(x)	Boundary Protection	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	Functional	Intersects With	Guest Networks	NET-02.2	Mechanisms exist to implement and manage a secure guest network.	3	
52.204-21(b)(1)(x)	Boundary Protection	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	Functional	Equal	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
52.204-21(b)(1)(xi)	Public-Access System Separation	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	5	
52.204-21(b)(1)(xii)	Flaw Remediation	Identify, report, and correct information and information system flaws in a timely manner.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
52.204-21(b)(1)(xii)	Flaw Remediation	Identify, report, and correct information and information system flaws in a timely manner.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	8	
52.204-21(b)(1)(xii)	Flaw Remediation	Identify, report, and correct information and information system flaws in a timely manner.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
52.204-21(b)(1)(xiii)	Malicious Code Protection	Provide protection from malicious code at appropriate locations within organizational information systems.	Functional	Subset Of	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	10	
52.204-21(b)(1)(xiii)	Malicious Code Protection	Provide protection from malicious code at appropriate locations within organizational information systems.	Functional	Equal	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	
52.204-21(b)(1)(xiv)	Update Malicious Code Protection	Update malicious code protection mechanisms when new releases are available.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	8	
52.204-21(b)(1)(xv)	System & File Scanning	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	Functional	Subset Of	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	
52.204-21(b)(1)(xv)	System & File Scanning	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	Functional	Intersects With	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	8	