Control ID	Control/Activity Description	Capability	ISO 27002	ISO 27002 Control Name	NIST 800-53	NIST Control Name
					AC-1	ACCESS CONTROL POLICY AND PROCEDURES
					AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
					AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES
					CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES
					CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES
					CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES
					IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES
					IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES
JNCSF-1	Develop and document control policies	Security in Architecture and Portfolio	5.1.1	POLICIES FOR INFORMATION SECURITY	MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES
			9.1.1	ACCESS CONTROL POLICY	MP-1	MEDIA PROTECTION POLICY AND PROCEDURES
					PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES
					PL-1	SECURITY PLANNING POLICY AND PROCEDURES
					PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES
					RA-1	RISK ASSESSMENT POLICY AND PROCEDURES
					SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES
					SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES
					SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES
					AC-1	ACCESS CONTROL POLICY AND PROCEDURES
					AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
					AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES
					CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES
					CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES
					CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES
					IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES
					IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES
JNCSF-2	Work with information owners to set appropriate control policies	Security in Architecture and Portfolio	5.1.1	POLICIES FOR INFORMATION SECURITY	MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES
					MP-1	MEDIA PROTECTION POLICY AND PROCEDURES
					PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES
					PL-1	SECURITY PLANNING POLICY AND PROCEDURES
					PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES
					RA-1	RISK ASSESSMENT POLICY AND PROCEDURES
					SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES
					SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES
					SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES
			6.1.5	INFORMATION SECURITY IN PROJECT MANAGEMENT		
JNCSF-3	Address information security requirements and risks in all project management	Security in Architecture and Portfolio	14.1.1	INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION		
JNCSF-4	Address information security in all project management	Security in Architecture and Portfolio	6.1.5	INFORMATION SECURITY IN PROJECT MANAGEMENT		
JNCSF-5	Ensure management agrees with audit requirements for access to information systems and data, as appropriate	Security in Architecture and Portfolio	12.7.1	INFORMATION SYSTEMS AUDIT CONTROLS		
JNCSF-6	Assign a senior-level executive as the authorizing official for information systems	Security in Architecture and Portfolio			CA-6	SECURITY AUTHORIZATION
JNCSF-7	Develop and document a granular inventory of current, authorized information system components on all information systems	Security in Architecture and Portfolio	18.1.2	INTELLECTUAL PROPERTY RIGHTS	CM-8	INFORMATION SYSTEM COMPONENT INVENTORY
			8.1.1	INVENTORY OF ASSETS		
JNCSF-8	Review and update the inventory of system components on all information systems	Security in Architecture and Portfolio	8.1.1	INVENTORY OF ASSETS	CM-8	INFORMATION SYSTEM COMPONENT INVENTORY
JNCSF-9	Develop a security plan for maintaining information system security that describes security requirements, authorization boundaries, and the system's operational environment	Security in Architecture and Portfolio			PL-2	SYSTEM SECURITY PLAN
JNCSF-10	Update security plans for maintaining information system security to address changes/problems encountered	Security in Architecture and Portfolio			PL-2	SYSTEM SECURITY PLAN
JNCSF-11	Approve, control, and monitor information system maintenance tools	Security in Architecture and Portfolio			MA-3	MAINTENANCE TOOLS
JNCSF-12	Develop a security plan governing information systems that includes security categorization, security requirements. and any security controls in place	Security in Architecture and Portfolio	5.1.1	POLICIES FOR INFORMATION SECURITY	PL-2	SYSTEM SECURITY PLAN
JNCSF-13	Develop a security plan that describes information systems' operational environments and connections with other systems	Security in Architecture and Portfolio			PL-2	SYSTEM SECURITY PLAN
JNCSF-14	Develop an information security architecture that describes the philosophy, requirements, and approach to managing and protecting information	Security in Architecture and Portfolio			PL-8	INFORMATION SECURITY ARCHITECTURE
JNCSF-15	Develop an information security architecture that describes how the architecture is integrated into and supports enterprise architecture	Security in Architecture and Portfolio			PL-8	INFORMATION SECURITY ARCHITECTURE
JNCSF-16	Develop an information security architecture that describes any information security assumptions about, and/or dependencies on. external services	Security in Architecture and Portfolio			PL-8	INFORMATION SECURITY ARCHITECTURE
JNCSF-17	Review and update the information security architecture at appropriate intervals, ensuring any changes are reflected in the security plan and CONOPS	Security in Architecture and Portfolio			PL-8	INFORMATION SECURITY ARCHITECTURE
JNCSF-18	Review and update the information security architecture, ensuring any changes are reflected in the security plan and CONOPS	Security in Architecture and Portfolio				
JNCSF-19	Manage organizational security controls and related processes centrally	Security in Architecture and Portfolio			PL-9	CENTRAL MANAGEMENT
JNCSF-20	Establish a line item for information security in budgeting documentation	Security in Architecture and Portfolio			SA-2	ALLOCATION OF RESOURCES
JNCSF-21	Describe the trustworthiness required in information systems supporting critical business functions	Security in Architecture and Portfolio			SA-13	TRUSTWORTHINESS
JNCSF-22	Ensure outsourced developer security architecture and design is consistent with the organization's security and enterprise architecture	Security in Architecture and Portfolio	14.2.7	OUTSOURCED DEVELOPMENT	SA-17	DEVELOPER SECURITY ARCHITECTURE AND DESIGN
JNCSF-23	Distribute processing and storage across multiple physical locations	Security in Architecture and Portfolio			SC-36	DISTRIBUTED PROCESSING AND STORAGE
JNCSF-24	Configure information systems to implement fail-safe procedures upon organization-defined conditions	Security in Architecture and Portfolio			SI-17	FAIL-SAFE PROCEDURES
JNCSF-25	Develop and implement procedures for maintaining privacy and protection of personally identifiable information	Security in Architecture and Portfolio	18.1.4	PRIVACY AND PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION		
JNCSF-26	Configure information systems to require re-authentication after defined circumstances (e.g., period of inactivity)	Development			IA-11	RE-AUTHENTICATION
					AC-11	SESSION LOCK
JNCSF-27	Configure information systems to terminate user sessions after defined conditions or trigger events are met	Development			AC-12	SESSION TERMINATION
JNCSF-28	Configure information systems to terminate user sessions after defined conditions or triggers are met	Development	9.4.2	SECURE LOG-ON PROCEDURES		
JNCSF-29	Designate individuals authorized to post information onto publicly accessible information systems	Development	14.1.2	SECURING APPLICATION SERVICES ON PUBLIC NETWORKS	AC-22	PUBLICLY ACCESSIBLE CONTENT
			12.4.1	EVENT LOGGING		
JNCSF-30	Configure information systems to generate audit records of all relevant information about every auditable event	Development	12.5.1	INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS	AU-3	CONTENT OF AUDIT RECORDS
			14.2.2	SYSTEM CHANGE CONTROL PROCEDURES	AU-12	AUDIT GENERATION
			12.7.1	INFORMATION SYSTEMS AUDIT CONTROLS	CM-3	CONFIGURATION CHANGE CONTROL
			12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES		
JNCSF-31	Document interface characteristics, security requirements, and the nature of information for each internal connection between information systems	Development			CA-9	INTERNAL SYSTEM CONNECTIONS
JNCSF-32	Develop, document, and maintain a baseline configuration of all information systems	Development	12.5.1	INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS	CM-2	BASELINE CONFIGURATION
			12.1.1	DOCUMENTED OPERATING PROCEDURES		
JNCSF-33	Determine the types of changes to information systems that are configuration-controlled	Development	12.1.2	CHANGE MANAGEMENT	CM-3	CONFIGURATION CHANGE CONTROL
			14.2.2	SYSTEM CHANGE CONTROL PROCEDURES		
JNCSF-34	Document, implement, and review configuration-controlled changes to information systems	Development	12.5.1	INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS	CM-3	CONFIGURATION CHANGE CONTROL
			12.1.2	CHANGE MANAGEMENT		
			14.2.2	SYSTEM CHANGE CONTROL PROCEDURES		
JNCSF-35	Establish, document, and implement restrictive configuration settings for IT components within information systems	Development			CM-6	CONFIGURATION SETTINGS
JNCSF-36	Identify, document, and approve any deviations from configuration settings	Development			CM-6	CONFIGURATION SETTINGS
JNCSF-37	Develop, document, and implement a configuration management plan for information systems that establishes roles and responsibilities	Development			CM-9	CONFIGURATION MANAGEMENT PLAN
JNCSF-38	Protect the configuration management plan from unauthorized disclosure/modification	Development	14.2.6	SECURE DEVELOPMENT ENVIRONMENT	CM-9	CONFIGURATION MANAGEMENT PLAN
			12.5.1	INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS		
JNCSF-39	Establish and enforce policies governing the installation of software installation by users	Development	12.6.2	RESTRICTIONS ON SOFTWARE INSTALLATIONS	CM-11	USER-INSTALLED SOFTWARE
			18.1.2	INTELLECTUAL PROPERTY RIGHTS		
JNCSF-40	Ensure changes to operational systems are tested in a different environment requiring different user profiles than that of operational systems	Development	12.1.4	SEPARATION OF DEVELOPMENT, TESTING AND OPERATIONAL ENVIRONMENTS		
JNCSF-41	Establish a system to test the effectiveness of the contingency plan, review the results, and initiate necessary corrective actions	Development	17.1.3	VERIFY, REVIEW AND EVALUATE INFORMATION SECURITY CONTINUITY	CP-4	CONTINGENCY PLAN TESTING
JNCSF-42	Review the information security continuity plan when there are any changes information systems or management	Development	17.1.3	VERIFY, REVIEW AND EVALUATE INFORMATION SECURITY CONTINUITY		
JNCSF-43	Establish a system to regular test backup media to ensure the integrity of the information	Development	12.3.1	INFORMATION BACKUP		
JNCSF-44	Configure information systems to identify and authenticate devices before establishing a network connection	Development	9.1.2	ACCESS TO NETWORKS AND NETWORK SERVICES	IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION
JNCSF-45	Ensure authenticators are high-quality and sufficiently secure	Development	9.4.3	PASSWORD MANAGEMENT SYSTEM	IA-5	AUTHENTICATOR MANAGEMENT
JNCSF-46	Change default authenticators prior to information system installation	Development	9.2.4	MANAGEMENT OF SECRET AUTHENTICATION INFORMATION OF USERS	IA-5	AUTHENTICATOR MANAGEMENT
JNCSF-47	Configure information systems to obscure authentication information during authentication processes	Development	9.4.2	SECURE LOG-ON PROCEDURES	IA-6	AUTHENTICATOR FEEDBACK
			9.4.3	PASSWORD MANAGEMENT SYSTEM		
JNCSF-48	Configure information systems to have federally regulated authentication mechanisms for cryptographic modules. where applicable	Development			IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION
JNCSF-49	Configure information systems to identify and authenticate non-organizational users, as appropriate	Development			IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)
JNCSF-50	Ensure access to program source code is restricted and enforced with strict authorization procedures and policies.	Development	9.4.5	ACCESS CONTROL TO PROGRAM SOURCE CODE		
JNCSF-51	Ensure program source libraries are not held in operational systems	Development	9.4.5	ACCESS CONTROL TO PROGRAM SOURCE CODE		
JNCSF-52	Test supporting utilities regularly to ensure functionality	Development	11.2.2	SUPPORTING UTILITIES		
JNCSF-53	Manage information systems using a well-defined system development lifecycle that incorporates information security considerations	Development	14.2.6	SECURE DEVELOPMENT ENVIRONMENT	SA-3	SYSTEM DEVELOPMENT LIFE CYCLE
JNCSF-54	Define and document information security roles and responsibilities of specific individuals throughout the system development life cycle	Development	14.1.1	INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION	SA-3	SYSTEM DEVELOPMENT LIFE CYCLE
JNCSF-55	Integrate information security risk management processes into system development life cycle activities	Development	14.1.1	INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION	SA-3	SYSTEM DEVELOPMENT LIFE CYCLE
JNCSF-56	Ensure developers have the necessary security expertise to design, code, and implement new software securely	Development	14.2.1	SECURE DEVELOPMENT POLICY	SA-3	SYSTEM DEVELOPMENT LIFE CYCLE
JNCSF-57	Provide guidance for ensuring secure software development and use of programming languages	Development	14.2.1	SECURE DEVELOPMENT POLICY		
JNCSF-58	Ensure developers are capable of avoiding, finding, and fixing information system vulnerabilities	Development	14.2.1	SECURE DEVELOPMENT POLICY		
JNCSF-59	Establish administrator documentation that describes configuration, installation, and operation procedures	Development			SA-5	INFORMATION SYSTEM DOCUMENTATION
JNCSF-60	Update information system documentation after any system change	Development	14.2.2	SYSTEM CHANGE CONTROL PROCEDURES		
JNCSF-61	Apply information system security engineering principles in the development of information systems	Development	14.2.5	SECURE SYSTEM ENGINEERING PRINCIPLES	SA-8	SECURITY ENGINEERING PRINCIPLES
JNCSF-62	Review security engineering procedures to ensure their effectiveness	Development	14.2.5	SECURE SYSTEM ENGINEERING PRINCIPLES		
JNCSF-63	Require information system developers to perform configuration management during system development	Development	14.2.2	SYSTEM CHANGE CONTROL PROCEDURES	SA-10	DEVELOPER CONFIGURATION MANAGEMENT
					CM-3	CONFIGURATION CHANGE CONTROL
JNCSF-64	Implement and document only approved changes to information systems	Development	14.2.2	SYSTEM CHANGE CONTROL PROCEDURES	SA-10	DEVELOPER CONFIGURATION MANAGEMENT
JNCSF-65	Review and test application control and integrity procedures after making operating platform changes	Development	14.2.3	TECHNICAL REVIEW OF APPLICATIONS AFTER OPERATING PLATFORM CHANGES		
JNCSF-66	Require the information system developers to test and evaluate whether newly implemented security controls are implemented correctly and operating as intended	Development	14.2.8	SYSTEM SECURITY TESTING	SA-11	DEVELOPER SECURITY TESTING AND EVALUATION
JNCSF-67	Require independent system acceptance testing for new information systems and changes to existing ones	Development	14.2.9	SYSTEM ACCEPTANCE TESTING		
JNCSF-68	Employ access control procedures for test application systems to protect confidentiality of test data	Development	14.3.1	PROTECTION OF TEST DATA		
JNCSF-69	Require separate authorization each time operational information is copied to a test environment	Development	14.3.1	PROTECTION OF TEST DATA		
JNCSF-70	Erase operational information from test environments immediately upon completion of testing	Development	14.3.1	PROTECTION OF TEST DATA		
JNCSF-71	Perform criticality analyses throughout the system development life cycle to identify critical information system components	Development			SA-14	CRITICALITY ANALYSIS
JNCSF-72	Require use of a development process that identifies and documents tools used in the development process	Development			SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS
JNCSF-73	Require use of a development process that documents and ensures the integrity of changes to the development process and associated tools	Development	14.2.2	SYSTEM CHANGE CONTROL PROCEDURES	SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS
JNCSF-74	Review the development process to ensure that the process, standards, and tools satisfy security requirements	Development			SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS
JNCSF-75	Require training for developers on the correct use of security functions and controls	Development	14.2.1	SECURE DEVELOPMENT POLICY	SA-16	DEVELOPER-PROVIDED TRAINING
JNCSF-76	Ensure outsourced developer security architecture and design accurately describes the required security functionality	Development			SA-17	DEVELOPER SECURITY ARCHITECTURE AND DESIGN
JNCSF-77	Ensure outsourced developer security architecture and design accurately allocates security controls among physical and logical components	Development			SA-17	DEVELOPER SECURITY ARCHITECTURE AND DESIGN
JNCSF-78	Ensure outsourced developer security architecture and design expresses how security functions and services work together to provide security capabilities	Development			SA-17	DEVELOPER SECURITY ARCHITECTURE AND DESIGN
JNCSF-79	Employ licensing arrangements, code ownership, and intellectual property rights for outsourced system development	Development	14.2.7	OUTSOURCED DEVELOPMENT		
JNCSF-80	Perform acceptance testing for outsourced system development deliverables	Development	14.2.7	OUTSOURCED DEVELOPMENT		
JNCSF-81	Require information system developers to have appropriate access authorizations	Development	14.2.6	SECURE DEVELOPMENT ENVIRONMENT	SA-21	DEVELOPER SCREENING
JNCSF-82	Establish a secure development environment that considers the sensitivity of data being processed	Development	14.2.6	SECURE DEVELOPMENT ENVIRONMENT		
JNCSF-83	Discourage modification to software packages and limit changes to necessary and strictly controlled changes	Development	14.2.4	RESTRICTIONS ON CHANGES TO SOFTWARE PACKAGES		
JNCSF-84	Ensure information system components have the minimal required level of functionality and information storage	Development			SC-25	THIN NODES
JNCSF-85	Segregate development environments throughout the system development lifecycle	Development	14.2.6	SECURE DEVELOPMENT ENVIRONMENT		
JNCSF-86	Test software and firmware updates for effectiveness and side effects before installation	Development	12.5.1	INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS	SI-2	FLAW REMEDIATION
JNCSF-87	Employ malicious code protection mechanisms at information system entry and exit points	Development			SI-3	MALICIOUS CODE PROTECTION
JNCSF-88	Update malicious code protection mechanisms when new releases are available and/or in accordance with organizational policy	Development			SI-3	MALICIOUS CODE PROTECTION
JNCSF-89	Configure malicious code protections to periodically scan information systems and external files as files are downloaded or opened	Development	13.2.1	INFORMATION TRANSFER POLICIES AND PROCEDURES	SI-3	MALICIOUS CODE PROTECTION

JNCSF-90	Configure malicious code protections to perform defined actions in response to malicious code detection (e.g., block code. send alert to administrator)	Development				SI-3	MALICIOUS CODE PROTECTION
JNCSF-91	Address any false positives during malicious code detection and their impact on the availability of information systems	Development				SI-3	MALICIOUS CODE PROTECTION
JNCSF-92	Notify appropriate personnel of any failed security verification tests and take appropriate actions upon failure	Development				SI-6	SECURITY FUNCTION VERIFICATION
JNCSF-93	Configure information systems to validate that information output from software programs is consistent with its expected content	Development				SI-15	INFORMATION OUTPUT FILTERING
JNCSF-94	Configure information systems to implement security safeguards to protect its memory from unauthorized code execution	Development				SI-16	MEMORY PROTECTION
JNCSF-95	Define and distribute user account types for information systems and networks where applicable	Delivery	9.2.2 9.2.3 9.2.1 9.1.2	USER ACCESS PROVISIONING MANAGEMENT OF PRIVILEGED ACCESS RIGHTS USER REGISTRATION AND DE-REGISTRATION ACCESS TO NETWORKS AND NETWORK SERVICES		PR	ACCESS CONTROL
JNCSF-96	Assign access rights to all user accounts, consistent with control policies	Delivery	9.2.2 9.2.3	USER ACCESS PROVISIONING MANAGEMENT OF PRIVILEGED ACCESS RIGHTS		AC-2	ACCOUNT MANAGEMENT
JNCSF-97	Assign account managers for all information system accounts	Delivery				AC-2	ACCOUNT MANAGEMENT
JNCSF-98	Employ physical or logical access controls to restrict users' access rights to sensitive applications or data	Delivery	9.4.1	INFORMATION ACCESS RESTRICTION			
JNCSF-99	Ensure all information systems manage the flow of information within and between connected systems, consistent with control policies	Delivery				AC-4	INFORMATION FLOW ENFORCEMENT
JNCSF-100	Formally separate sensitive duties among multiple individuals to prevent access rights abuses or conflicts of interest	Delivery	6.1.2	SEGREGATION OF DUTIES		AC-5	SEPARATION OF DUTIES
JNCSF-101	Define information system access authorizations that enforce separation of duties for sensitive activities	Delivery				AC-5	SEPARATION OF DUTIES
JNCSF-102	Manage access rights to be consistent with the principle of least privilege	Delivery	9.4.4 9.2.3	USE OF PRIVILEGED UTILITY PROGRAMS MANAGEMENT OF PRIVILEGED ACCESS RIGHTS		AC-6	LEAST PRIVILEGE
JNCSF-103	Identify and document which user actions are permitted on information systems without user identification or authentication	Delivery				AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
JNCSF-104	Define and allocate all information security responsibilities, stating specific assets and processes for which individuals are responsible	Delivery	6.1.1	INFORMATION SECURITY ROLES AND RESPONSIBILITIES			
JNCSF-105	Prevent unauthorized access to mobile devices by using physical protection against theft, cryptographic techniques, and secret authentication information	Delivery	6.2.1	MOBILE DEVICE POLICY		AC-19	ACCESS CONTROL FOR MOBILE DEVICES
JNCSF-106	Establish procedures to ensure access control decisions are applied consistently with control policies	Delivery				AC-24	ACCESS CONTROL DECISIONS
JNCSF-107	Assign different user IDs to be used only for privileged access rights, separate from regular business activities	Delivery	9.2.3	MANAGEMENT OF PRIVILEGED ACCESS RIGHTS			
JNCSF-108	Allow authorized personnel to select how and which auditable events will be audited by specific components of information systems	Delivery				AU-12	AUDIT GENERATION
JNCSF-109	Ensure the authorizing official authorizes information systems for processing before commencing operations	Delivery				CA-6	SECURITY AUTHORIZATION
JNCSF-110	Establish an emergency change process to quickly implement changes to processes and information systems needed to resolve an incident	Delivery	12.1.2	CHANGE MANAGEMENT			
JNCSF-111	Establish a committee to periodically coordinate and provide oversight for configuration-controlled changes	Delivery				CM-3	CONFIGURATION CHANGE CONTROL
JNCSF-112	Define, document, approve, and enforce access restrictions associated with information system changes	Delivery	12.5.1 14.2.6 14.2.2	INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS SECURE DEVELOPMENT ENVIRONMENT SYSTEM CHANGE CONTROL PROCEDURES		CM-5	ACCESS RESTRICTIONS FOR CHANGE
JNCSF-113	Establish a rollback strategy before implementing system changes	Delivery	12.5.1 12.1.2	INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS CHANGE MANAGEMENT			
JNCSF-114	Establish a formal approval for information system changes from authorized users	Delivery	14.2.2	SYSTEM CHANGE CONTROL PROCEDURES		CM-3	CONFIGURATION CHANGE CONTROL
JNCSF-115	Document rules for transferring software from development to operational, and ensure they are run on different systems	Delivery	12.1.4	SEPARATION OF DEVELOPMENT, TESTING AND OPERATIONAL ENVIRONMENTS			
JNCSF-116	Configure information systems to identify and authenticate organizational users	Delivery	9.4.1	INFORMATION ACCESS RESTRICTION		IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
JNCSF-117	Establish an information system and user identifier management system to select and assign identifiers to individuals or groups	Delivery				IA-4	IDENTIFIER MANAGEMENT
JNCSF-118	Prevent the reuse of information system and user identifiers for a defined time period	Delivery	9.4.3 9.2.1	PASSWORD MANAGEMENT SYSTEM USER REGISTRATION AND DE-REGISTRATION		IA-4	IDENTIFIER MANAGEMENT
JNCSF-119	Establish procedures to verify the identity of a user prior to providing new secret authentication information	Delivery	9.2.4	MANAGEMENT OF SECRET AUTHENTICATION INFORMATION OF USERS		IA-5	AUTHENTICATOR MANAGEMENT
JNCSF-120	Provide temporary, secure, and unique authentication information upon initial user registration	Delivery	9.2.4	MANAGEMENT OF SECRET AUTHENTICATION INFORMATION OF USERS		IA-5	AUTHENTICATOR MANAGEMENT
JNCSF-121	Establish lifetime restrictions and conditions on reusing and changing authenticators	Delivery	9.4.3	PASSWORD MANAGEMENT SYSTEM		IA-5	AUTHENTICATOR MANAGEMENT
JNCSF-122	Change authenticators for group or role accounts when membership changes	Delivery	9.2.6	REMOVAL OR ADJUSTMENT OF ACCESS RIGHTS		IA-5	AUTHENTICATOR MANAGEMENT
JNCSF-123	Identify and authenticate information system services using approved safeguard measures	Delivery				IA-9	SERVICE IDENTIFICATION AND AUTHENTICATION
JNCSF-124	Restrict use, authorization, and availability of utility programs that can override system and application controls	Delivery	9.4.4	USE OF PRIVILEGED UTILITY PROGRAMS			
JNCSF-125	Establish a process for granting and documenting maintenance personnel authorization	Delivery	11.2.4	EQUIPMENT MAINTENANCE		MA-5	MAINTENANCE PERSONNEL
JNCSF-126	Ensure non-escorted maintenance personnel have required access authorizations	Delivery				MA-5	MAINTENANCE PERSONNEL
JNCSF-127	Designate competent and authorized personnel to supervise maintenance activities of un-authorized personnel	Delivery				MA-5	MAINTENANCE PERSONNEL
JNCSF-128	Establish a media downgrading process using mechanisms commensurate with the media's level of security and access authorization	Delivery				MP-8	MEDIA DOWNGRADING
JNCSF-129	Require authorization for media removal where necessary	Delivery	8.3.1	MANAGEMENT OF REMOVABLE MEDIA			
JNCSF-130	Grant restricted physical access to external support service personnel only when required	Delivery	11.1.2	PHYSICAL ENTRY CONTROLS			
JNCSF-131	Review and update user access agreements as needed	Delivery	13.2.4	CONFIDENTIALITY OR NONDISCLOSURE AGREEMENTS		PS-6	ACCESS AGREEMENTS
JNCSF-132	Ensure that individuals sign appropriate access agreements prior to receiving access and after access agreements have been updated	Delivery	7.1.2	TERMS AND CONDITIONS OF EMPLOYMENT		PS-6	ACCESS AGREEMENTS
JNCSF-133	Ensure an authorized individual reviews and approves security categorization decisions associated with information and information systems	Delivery				RA-2	SECURITY CATEGORIZATION
JNCSF-134	Establish user documentation that describes how to effectively use user-accessible security functions of information systems	Delivery				SA-5	INFORMATION SYSTEM DOCUMENTATION
JNCSF-135	Ensure security and protection of information systems and system components throughout their delivery in the supply chain process	Delivery	15.1.3	INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAIN		SA-12	SUPPLY CHAIN PROTECTION
JNCSF-136	Configure information systems to verify the correct operation of security functions (e.g., authentication)	Delivery				SI-6	SECURITY FUNCTION VERIFICATION
JNCSF-137	Establish a process to assign information ownership to appropriate individuals in a timely fashion	Delivery	8.1.2	OWNERSHIP OF ASSETS			
JNCSF-138	Require information owners to define and review access restrictions to important information	Delivery	8.1.2 8.1.2	OWNERSHIP OF ASSETS OWNERSHIP OF ASSETS			
JNCSF-139	Establish a process to routinely review that user access rights align with control policies	Operation	9.2.5 9.2.2 9.2.3	REVIEW OF USER ACCESS RIGHTS USER ACCESS PROVISIONING MANAGEMENT OF PRIVILEGED ACCESS RIGHTS		AC-2	ACCOUNT MANAGEMENT
JNCSF-140	Establish a process to evaluate and approve or reject access right requests consistent with control policies	Operation	9.2.2 9.2.3	USER ACCESS PROVISIONING MANAGEMENT OF PRIVILEGED ACCESS RIGHTS		AC-2	ACCOUNT MANAGEMENT
JNCSF-141	Establish a process to appropriately remove or adjust access rights from users as specified in control policies	Operation	9.2.6 9.2.2 9.2.5	REMOVAL OR ADJUSTMENT OF ACCESS RIGHTS USER ACCESS PROVISIONING REVIEW OF USER ACCESS RIGHTS		AC-2 PS-4 PS-5	ACCOUNT MANAGEMENT PERSONNEL TERMINATION PERSONNEL TRANSFER
JNCSF-142	Configure information systems to limit the number of unsuccessful logon attempts within a defined time period	Operation				AC-7	UNSUCCESSFUL LOGON ATTEMPTS
JNCSF-143	Configure information systems to lock user accounts after the maximum number of permitted unsuccessful logon attempts is exceeded	Operation				AC-7	UNSUCCESSFUL LOGON ATTEMPTS
JNCSF-144	Log unsuccessful and successful logon attempts and display this information upon a successful login	Operation	9.4.2	SECURE LOG-ON PROCEDURES			
JNCSF-145	Configure information systems to limit the number of concurrent user sessions for account types, as appropriate.	Operation				AC-10	CONCURRENT SESSION CONTROL
JNCSF-146	Configure information systems to prevent further user access (e.g., a session lock) after a defined period of user inactivity	Operation				AC-11	SESSION LOCK
JNCSF-147	Provide the ability to tag information based on sensitivity.	Operation	8.2.1	CLASSIFICATION OF INFORMATION			
JNCSF-148	Ensure information is appropriately tagged and that tags remain associated with information at rest and in transit	Operation				AC-16	SECURITY ATTRIBUTES
JNCSF-149	Establish capabilities to ensure information is appropriately tagged and that tags remain associated with information at rest and in transit	Operation	8.2.2	LABELLING OF INFORMATION			
JNCSF-150	Define the range of appropriate information tags for each information system	Operation	8.2.1	CLASSIFICATION OF INFORMATION		AC-16	SECURITY ATTRIBUTES
JNCSF-151	Establish clear procedures, guidelines, and requirements for all allowed types of remote user access	Operation	6.2.2	TELEWORKING		AC-17	REMOTE ACCESS
JNCSF-152	Maintain appropriate contacts with relevant authorities especially in the event of a security incident	Operation	6.1.3	CONTACT WITH AUTHORITIES			
JNCSF-153	Maintain appropriate contacts with professional special interest groups	Operation	6.1.4	CONTACT WITH SPECIAL INTEREST GROUPS			
JNCSF-154	Address communication security requirements for teleworking activities and provide suitable communication equipment	Operation	6.2.2	TELEWORKING			
JNCSF-155	Ensure teleworking sites are secure, both physically and from unauthorized access	Operation	6.2.2	TELEWORKING			
JNCSF-156	Establish requirements and restrictions on the configuration of wireless network services and the use of home networks	Operation	6.2.2 13.1.1	TELEWORKING NETWORK CONTROLS			
JNCSF-157	Establish policies on the use of malware protection for teleworking equipment	Operation	6.2.2	TELEWORKING			
JNCSF-158	Configure information systems to require appropriate authorization procedures before allowing remote user access	Operation				AC-17	REMOTE ACCESS
JNCSF-159	Establish usage restrictions (by establishing authentication or encryption protocols), configuration/connection requirements. and implementation guidance for wireless access	Operation				AC-18	WIRELESS ACCESS
JNCSF-160	Configure wireless networks to require appropriate authorization procedures before allowing wireless access	Operation	9.1.2 13.1.1	ACCESS TO NETWORKS AND NETWORK SERVICES NETWORK CONTROLS		AC-18	WIRELESS ACCESS
JNCSF-161	Ensure users can only access networks and network services they are authorized to use	Operation	9.1.2 13.1.1	ACCESS TO NETWORKS AND NETWORK SERVICES NETWORK CONTROLS			
JNCSF-162	Establish usage restrictions, configuration/connection requirements, and implementation guidance for organization-controlled mobile devices	Operation	6.2.1	MOBILE DEVICE POLICY		AC-19	ACCESS CONTROL FOR MOBILE DEVICES
JNCSF-163	Configure information systems to require authorization procedures before connecting mobile devices	Operation	6.2.1	MOBILE DEVICE POLICY		AC-19	ACCESS CONTROL FOR MOBILE DEVICES
JNCSF-164	Take appropriate verification and protection measures to protect payment methods on public networks from fraud	Operation	14.1.2	SECURING APPLICATION SERVICES ON PUBLIC NETWORKS			
JNCSF-165	Employ data-mining prevention and detection techniques to prevent unapproved data mining activity.	Operation				AC-23	DATA MINING PROTECTION
JNCSF-166	Configure information systems to implement tamperproof reference monitors for access control policies that are small enough to be analyzed and tested	Operation				AC-25	REFERENCE MONITOR
JNCSF-167	Ensure information systems are capable of logging events deemed auditable	Operation				AU-2	AUDIT EVENTS
JNCSF-168	Coordinate with other organizational functions to guide the selection of auditable events	Operation				AU-2	AUDIT EVENTS
JNCSF-169	Configure event logs to record alarms raised by the access control system	Operation	12.4.1	EVENT LOGGING			
JNCSF-170	Establish and maintain audit record storage requirements	Operation	12.4.2	PROTECTION OF LOG INFORMATION		AU-4	AUDIT STORAGE CAPACITY
JNCSF-171	Configure information systems to alert appropriate personnel after an audit-processing failure	Operation				AU-5	RESPONSE TO AUDIT PROCESSING FAILURES
JNCSF-172	Configure information systems to take specified actions after an audit processing failure (e.g., shut down information system, stop generating audit records, etc.)	Operation				AU-5	RESPONSE TO AUDIT PROCESSING FAILURES
JNCSF-173	Establish cadence to review information system audit records and report any unusual activity to appropriate personnel	Operation	12.4.1 12.4.3	EVENT LOGGING ADMINISTRATOR AND OPERATOR LOGS		AU-6 CM-3	AUDIT REVIEW, ANALYSIS, AND REPORTING CONFIGURATION CHANGE CONTROL
JNCSF-174	Log all system administrator and system operator activities and protect these logs	Operation	12.4.3	ADMINISTRATOR AND OPERATOR LOGS			
JNCSF-175	Configure information systems to provide on-demand audit reviews and after-the-fact security incident investigations	Operation				AU-7	AUDIT REDUCTION AND REPORT GENERATION
JNCSF-176	Configure information systems to ensure the generation of audit reports and reductions do not alter any original log data	Operation				AU-7	AUDIT REDUCTION AND REPORT GENERATION
JNCSF-177	Configure information systems to use internal system clocks to record time stamps for all audit records	Operation	12.4.4	CLOCK SYNCHRONISATION		AU-8	TIME STAMPS
JNCSF-178	Configure information systems to protect against individuals falsely denying having performed auditable events	Operation	14.1.1	INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION		AU-10	NON-REPUDIATION
JNCSF-179	Retain audit records for a defined time period consistent with the organization's records retention policy, with regulatory requirements, and for after-the-fact security incident investigations	Operation	18.1.3	PROTECTION OF RECORDS		AU-11	AUDIT RECORD RETENTION
JNCSF-180	Monitor open source information sources for evidence of unauthorized disclosure of organizational information	Operation				AU-13	MONITORING FOR INFORMATION DISCLOSURE
JNCSF-181	Configure information systems to provide the capability for authorized users to select a user session to record or view	Operation				AU-14	SESSION AUDIT
JNCSF-182	Provide a backup audit capability in case of a failure in the primary audit capability	Operation				AU-15	ALTERNATE AUDIT CAPABILITY
JNCSF-183	Document and implement approaches to establish a single reference time across all information systems and synchronize internal clocks	Operation	12.4.4	CLOCK SYNCHRONISATION		AU-8	TIME STAMPS
JNCSF-184	Ensure audit requirements and activities on operational systems are carefully planned and defined to minimize disruptions to organizational processes	Operation	12.7.1	INFORMATION SYSTEMS AUDIT CONTROLS			
JNCSF-185	Control the scope of technical audit tests, and limit them to read-only access to software and data	Operation	12.7.1	INFORMATION SYSTEMS AUDIT CONTROLS			
JNCSF-186	Develop and document a plan to remediate weaknesses or vulnerabilities discovered during security controls assessments	Operation	CA-5 SA-11	PLAN OF ACTION AND MILESTONES DEVELOPER SECURITY TESTING AND EVALUATION			
JNCSF-187	Conduct periodic independent reviews of the organization's approach to managing and implementation of information security	Operation	18.2.1	INDEPENDENT REVIEW OF INFORMATION SECURITY			
JNCSF-188	Ensure managers review that information security requirements defined in policies are met in their area of responsibility	Operation	18.2.2	COMPLIANCE WITH SECURITY POLICIES AND STANDARDS			
JNCSF-189	Establish cadence to review and update the security authorization of information systems	Operation				CA-6	SECURITY AUTHORIZATION
JNCSF-190	Implement a continuous monitoring program with security control assessments, security status monitoring, analysis of information, and established response actions	Operation				CA-7	CONTINUOUS MONITORING
JNCSF-191	Conduct frequent penetration testing on information systems and system components	Operation	18.2.3	TECHNICAL COMPLIANCE REVIEW		CA-8	PENETRATION TESTING
JNCSF-192	Ensure all penetration tests are conducted by trained specialists under supervision and are conducted in a way that minimizes unintended, adverse impacts on the organization	Operation	18.2.3	TECHNICAL COMPLIANCE REVIEW			
JNCSF-193	Ensure all internal connections of information system components to information systems are appropriately authorized	Operation				CA-9	INTERNAL SYSTEM CONNECTIONS

JNCSF-194	Conduct security impact analyses of changes to information systems prior to implementing changes	Operation	12.5.1 12.1.2 12.6.1 14.2.2	INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS CHANGE MANAGEMENT MANAGEMENT OF TECHNICAL VULNERABILITIES SYSTEM CHANGE CONTROL PROCEDURES	CM-4	SECURITY IMPACT ANALYSIS
JNCSF-195	Monitor and control changes to the configuration settings in accordance with organization policies	Operation			CM-6	CONFIGURATION SETTINGS
JNCSF-196	Prohibit functions, ports, protocols, and/or services on information systems as appropriate	Operation	12.5.1	INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS	CM-7	LEAST FUNCTIONALITY
JNCSF-197	Track software usage to ensure compliance with contract agreements and copyright laws	Operation	18.1.2	INTELLECTUAL PROPERTY RIGHTS	CM-10	SOFTWARE USAGE RESTRICTIONS
JNCSF-198	Document the use of peer-to-peer file sharing technology to ensure there is no unauthorized use of copyrighted work	Operation	18.1.2	INTELLECTUAL PROPERTY RIGHTS	CM-10	SOFTWARE USAGE RESTRICTIONS
JNCSF-199	Monitor software installation policy compliance at frequent intervals	Operation			CM-11	USER-INSTALLED SOFTWARE
JNCSF-200	Archive old versions of software, with all required information, procedures and configuration details	Operation	12.5.1	INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS		
JNCSF-201	Monitor the use of resources to make projections of future capacity requirements to ensure efficiency of system performance	Operation	12.1.3	CAPACITY MANAGEMENT		
JNCSF-202	Develop a contingency plan for all information systems that provides recovery objectives, restoration priorities, and metrics	Operation	17.1.2	IMPLEMENTING INFORMATION SECURITY CONTINUITY	CP-2	CONTINGENCY PLAN
JNCSF-203	Determine if information security continuity is captured in the business continuity or disaster recovery management process	Operation	17.1.1	PLANNING INFORMATION SECURITY CONTINUITY		
JNCSF-204	Determine requirements for the continuity of information security management during a crisis and implement such management	Operation	17.1.1 17.1.2	PLANNING INFORMATION SECURITY CONTINUITY IMPLEMENTING INFORMATION SECURITY CONTINUITY		
JNCSF-205	Develop a contingency plan that addresses contingency roles and responsibilities	Operation	17.1.2	IMPLEMENTING INFORMATION SECURITY CONTINUITY	CP-2	CONTINGENCY PLAN
JNCSF-206	Develop a contingency plan that addresses full information system restoration without compromising original security safeguards	Operation	17.1.2	IMPLEMENTING INFORMATION SECURITY CONTINUITY	CP-2	CONTINGENCY PLAN
JNCSF-207	Ensure that third-parties are aware of business continuity procedures and are able to implement such procedures if needed	Operation	15.2.1	MONITORING AND REVIEW OF SUPPLIER SERVICES		
JNCSF-208	Develop incident response and contingency security plans and/or documented processes that meet mission, size, structure, and functions requirements of organization	Operation	17.1.2 16.1.1	IMPLEMENTING INFORMATION SECURITY CONTINUITY RESPONSIBILITIES AND PROCEDURES	CP-2 IR-8	CONTINGENCY PLAN INCIDENT RESPONSE PLAN
JNCSF-209	Ensure security plans for maintaining information system security are reviewed frequently and are approved by appropriate personnel	Operation			PL-2	SYSTEM SECURITY PLAN
JNCSF-210	Ensure incident response and contingency security plans and/or documented processes are reviewed frequently and are approved by appropriate personnel	Operation	17.1.3 16.1.1	VERIFY, REVIEW AND EVALUATE INFORMATION SECURITY CONTINUITY RESPONSIBILITIES AND PROCEDURES	CP-2 IR-8	CONTINGENCY PLAN INCIDENT RESPONSE PLAN
JNCSF-211	Distribute copies of security plans for maintaining information system security to identified key personnel	Operation			PL-2	SYSTEM SECURITY PLAN
JNCSF-212	Distribute copies of incident response and contingency security plans and documented processes to identified key personnel	Operation			IR-8 CP-2 CP-2 IR-4	INCIDENT RESPONSE PLAN CONTINGENCY PLAN CONTINGENCY PLAN INCIDENT HANDLING
JNCSF-213	Coordinate contingency planning activities with incident handling activities	Operation				
JNCSF-214	Ensure contingency planning and incident response procedures are updated to address gaps as they are discovered	Operation	17.1.3 16.1.6	VERIFY, REVIEW AND EVALUATE INFORMATION SECURITY CONTINUITY LEARNING FROM INFORMATION SECURITY INCIDENTS	CP-2 IR-8	CONTINGENCY PLAN INCIDENT RESPONSE PLAN
JNCSF-215	Communicate changes in security plans for maintaining information system security to appropriate personnel	Operation			PL-2	SYSTEM SECURITY PLAN
JNCSF-216	Protect security plans for maintaining information system security from unauthorized disclosure and modification	Operation			PL-2	SYSTEM SECURITY PLAN
JNCSF-217	Protect incident response and contingency security plans and documented processes from unauthorized disclosure and modification	Operation			CP-2 IR-8	CONTINGENCY PLAN INCIDENT RESPONSE PLAN
JNCSF-218	Establish an alternate storage site with agreements to permit the storage and retrieval of system backup information	Operation	17.2.1	AVAILABILITY OF INFORMATION PROCESSING FACILITIES	CP-6	ALTERNATE STORAGE SITE
JNCSF-219	Ensure that the information security safeguards are equivalent at both primary and alternate storage sites	Operation	17.2.1	AVAILABILITY OF INFORMATION PROCESSING FACILITIES	CP-6	ALTERNATE STORAGE SITE
JNCSF-220	Establish alternate processing sites with agreements permitting the transfer and resumption of operations	Operation	17.2.1	AVAILABILITY OF INFORMATION PROCESSING FACILITIES	CP-7	ALTERNATE PROCESSING SITE
JNCSF-221	Ensure that the necessary equipment and support is available for transfer/resumption at alternate processing sites	Operation			CP-7	ALTERNATE PROCESSING SITE
JNCSF-222	Ensure that the information security safeguards are equivalent at the primary and alternate processing sites	Operation	17.2.1	AVAILABILITY OF INFORMATION PROCESSING FACILITIES	CP-7	ALTERNATE PROCESSING SITE
JNCSF-223	Establish alternate telecommunications services that permits the resumption of operations	Operation			CP-8	TELECOMMUNICATIONS SERVICES
JNCSF-224	Establish alternate telecommunications services that permits the resumption of critical operations during disruptions	Operation	17.2.1	AVAILABILITY OF INFORMATION PROCESSING FACILITIES		
JNCSF-225	Conduct frequent backups of user- and system-level information in all information systems	Operation	12.3.1	INFORMATION BACKUP	CP-9	INFORMATION SYSTEM BACKUP
JNCSF-226	Conduct frequent backups of information system documentation including security-related documentation	Operation	12.3.1	INFORMATION BACKUP	CP-9	INFORMATION SYSTEM BACKUP
JNCSF-227	Protect confidentiality, integrity, and availability of backup information at storage locations	Operation	12.3.1	INFORMATION BACKUP	CP-9	INFORMATION SYSTEM BACKUP
JNCSF-228	Protect backup information by means of encryption in situations where confidentiality is important	Operation	12.3.1	INFORMATION BACKUP		
JNCSF-229	Establish capabilities to recover and reconstitute information systems to a known state after a disruption, compromise, or failure	Operation			CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION
JNCSF-230	Configure information systems to be able to employ alternative communications protocols to maintain continuity of operations during disruptions	Operation			CP-11	ALTERNATE COMMUNICATIONS PROTOCOLS
JNCSF-231	Configure information systems to enter a safe mode of operation under organization-defined conditions, such as during an incident	Operation	12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES	CP-12	SAFE MODE
JNCSF-232	Identify technical vulnerabilities and their associated risks using information resources and develop appropriate actions to be taken	Operation	12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES	SC-38	OPERATIONS SECURITY
JNCSF-233	Align technical vulnerability management with incident management activities to communicate data on vulnerabilities	Operation	12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES		
JNCSF-234	Employ alternative controls, where appropriate, when the primary means of implementing controls is compromised (e.g., providing senior leaders with one-time pads if encryption is compromised)	Operation	17.1.2	IMPLEMENTING INFORMATION SECURITY CONTINUITY	CP-13	ALTERNATIVE SECURITY MECHANISMS
JNCSF-235	Disable information system and user identifiers after a defined period of activity or as needed	Operation	9.4.3	PASSWORD MANAGEMENT SYSTEM	IA-4	IDENTIFIER MANAGEMENT
JNCSF-236	Require users to change their passwords at their first log-on	Operation	9.2.4 9.4.3	MANAGEMENT OF SECRET AUTHENTICATION INFORMATION OF USERS PASSWORD MANAGEMENT SYSTEM		
JNCSF-237	Require individuals to use safeguards to protect authenticators from unauthorized use	Operation	9.3.1	USE OF SECRET AUTHENTICATION INFORMATION	IA-5	AUTHENTICATOR MANAGEMENT
JNCSF-238	Advise users to avoid keeping a record of secret authentication unless it can be stored in a secure and approved manner	Operation	9.3.1 9.4.3	USE OF SECRET AUTHENTICATION INFORMATION PASSWORD MANAGEMENT SYSTEM		
JNCSF-239	Advise users to change secret authentication information after any indication of its possible compromise	Operation	9.3.1	USE OF SECRET AUTHENTICATION INFORMATION		
JNCSF-240	Require electronic signatures for electronic messaging and/or application service transactions to ensure authenticity of users and to protect information transfers	Operation	14.1.3 13.2.3	PROTECTING APPLICATION SERVICES TRANSACTIONS ELECTRONIC MESSAGING		
JNCSF-241	Require users to obtain approval prior to using external public messaging services such as instant messaging	Operation	13.2.3	ELECTRONIC MESSAGING		
JNCSF-242	Require stronger levels of authentication controlling access from publicly accessible networks to electronic messaging services	Operation	13.2.3	ELECTRONIC MESSAGING		
JNCSF-243	Store application service transaction details outside of any publicly accessible environment (e.g., on a storage platform on the organizational intranet)	Operation	14.1.3	PROTECTING APPLICATION SERVICES TRANSACTIONS		
JNCSF-244	Ensure that all information and secret authentication involved with application service transactions remain confidential and protected	Operation	14.1.3	PROTECTING APPLICATION SERVICES TRANSACTIONS		
JNCSF-245	Require additional authentication information to access information systems under conditions deemed high-risk	Operation			IA-10	ADAPTIVE IDENTIFICATION AND AUTHENTICATION
JNCSF-246	Ensure users only have access to networks and network services they are authorized to use	Operation	9.1.2	ACCESS TO NETWORKS AND NETWORK SERVICES		
JNCSF-247	Maintain a record of access rights granted to users to access information systems and services	Operation	9.2.2	USER ACCESS PROVISIONING		
JNCSF-248	Segregate utility programs from applications software on all information systems where applicable	Operation	9.4.4	USE OF PRIVILEGED UTILITY PROGRAMS		
JNCSF-249	Provide frequent incident response training to users upon assuming an IR role or after a system change, as appropriate	Operation			IR-2	INCIDENT RESPONSE TRAINING
JNCSF-250	Conduct and document results of frequent incident response testing to determine incident response effectiveness	Operation			IR-3	INCIDENT RESPONSE TESTING
JNCSF-251	Conduct and document results of frequent incident response testing to determine its effectiveness	Operation				
JNCSF-252	Implement an incident handling capability for security incidents including preparation, detection and analysis, containment, eradication, and recovery	Operation	16.1.1	RESPONSIBILITIES AND PROCEDURES	IR-4	INCIDENT HANDLING
JNCSF-253	Implement incident response procedures for escalation, controlled recovery, and necessary communication	Operation	16.1.1 16.1.1	RESPONSIBILITIES AND PROCEDURES RESPONSIBILITIES AND PROCEDURES		
JNCSF-254	Establish reporting procedures for incidence response that ensure accurate, immediate, and detailed reporting of information security events	Operation	16.1.1	RESPONSIBILITIES AND PROCEDURES		
JNCSF-255	Update incident response capabilities based on results from incident handling activities	Operation	16.1.6 16.1.6	LEARNING FROM INFORMATION SECURITY INCIDENTS LEARNING FROM INFORMATION SECURITY INCIDENTS	IR-4	INCIDENT HANDLING
JNCSF-256	Track and document information system security incidents	Operation	16.1.5	RESPONSE TO INFORMATION SECURITY INCIDENTS	IR-5	INCIDENT MONITORING
JNCSF-257	Require users to report suspected security incidents to the incident response capability within a specified time period	Operation	16.1.2 16.1.1	REPORTING INFORMATION SECURITY EVENTS RESPONSIBILITIES AND PROCEDURES	IR-6	INCIDENT REPORTING
JNCSF-258	Define procedures to report security incident information to external authorities as appropriate	Operation	16.1.2 16.1.1	REPORTING INFORMATION SECURITY EVENTS RESPONSIBILITIES AND PROCEDURES	IR-6	INCIDENT REPORTING
JNCSF-259	Provide the ability for users to report potential security incidents to the appropriate personnel	Operation	16.1.2	REPORTING INFORMATION SECURITY EVENTS	IR-7	INCIDENT RESPONSE ASSISTANCE
JNCSF-260	Develop an incident response plan, including a roadmap for implementing incident response capabilities	Operation			IR-8	INCIDENT RESPONSE PLAN
JNCSF-261	Develop an incident response plan that describes the structure and organization of the incident response capability	Operation			IR-8	INCIDENT RESPONSE PLAN
JNCSF-262	Develop an incident response plan that describes the structure and organization of incident response capabilities	Operation				
JNCSF-263	Develop an incident response plan that provides metrics for measuring the performance of incident response capabilities	Operation			IR-8	INCIDENT RESPONSE PLAN
JNCSF-264	Develop an incident response plan that defines the necessary resources and management support for maintaining an incident response capability	Operation			IR-8	INCIDENT RESPONSE PLAN
JNCSF-265	Develop an incident response plan that defines the necessary resources and management support for maintaining incident response capabilities	Operation	16.1.1	RESPONSIBILITIES AND PROCEDURES		
JNCSF-266	Develop an incident response plan that defines what events constitute reportable incidents	Operation	16.1.4	ASSESSMENT OF AND DECISION ON INFORMATION SECURITY EVENTS	IR-8	INCIDENT RESPONSE PLAN
JNCSF-267	Develop an ability to identify any specific information involved in information spills or contamination	Operation	16.1.5	RESPONSE TO INFORMATION SECURITY INCIDENTS	IR-9	INFORMATION SPILLAGE RESPONSE
JNCSF-268	Develop the capability to isolate contaminated information or information systems during an information spill	Operation			IR-9	INFORMATION SPILLAGE RESPONSE
JNCSF-269	Develop the ability to identify other information systems and components subsequently contaminated after an information spill	Operation			IR-9	INFORMATION SPILLAGE RESPONSE
JNCSF-270	Establish a formal process for identifying, collecting, acquiring, and preserving evidence from an information security event	Operation	16.1.7 16.1.5	COLLECTION OF EVIDENCE RESPONSE TO INFORMATION SECURITY INCIDENTS		
JNCSF-271	Require users to report suspected security weaknesses to the appropriate security personnel within specified time period	Operation	16.1.3	REPORTING INFORMATION SECURITY WEAKNESSES		
JNCSF-272	Establish a team of forensic/malicious code analysts, tool developers, and real-time operations personnel	Operation			IR-10	INTEGRATED INFORMATION SECURITY ANALYSIS TEAM
JNCSF-273	Perform, document, and review maintenance repairs on information systems in accordance with supplier/organization requirements	Operation	11.2.4	EQUIPMENT MAINTENANCE	MA-2	CONTROLLED MAINTENANCE
JNCSF-274	Approve and monitor all information system and network maintenance activities, regardless of whether equipment and maintenance is on/off site	Operation	11.2.4	EQUIPMENT MAINTENANCE	MA-2	CONTROLLED MAINTENANCE
JNCSF-275	Require explicit approval before removing information system components from facilities for off-site maintenance and/or repairs	Operation	11.2.5	REMOVAL OF ASSETS	MA-2	CONTROLLED MAINTENANCE
JNCSF-276	Remove all information from associated media prior to off-site maintenance and/or repairs as appropriate	Operation	11.2.4	EQUIPMENT MAINTENANCE	MA-2	CONTROLLED MAINTENANCE
JNCSF-277	Verify that potentially impacted security controls are functioning as intended after information system and network maintenance repairs	Operation	11.2.4	EQUIPMENT MAINTENANCE	MA-2	CONTROLLED MAINTENANCE
JNCSF-278	Include all information system and network maintenance-related information in maintenance records	Operation	11.2.4	EQUIPMENT MAINTENANCE	MA-2	CONTROLLED MAINTENANCE
JNCSF-279	Approve, monitor, and record all nonlocal maintenance	Operation			MA-4	NONLOCAL MAINTENANCE
JNCSF-280	Ensure use of nonlocal maintenance is consistent with security policies and is documented in the security plan	Operation			MA-4	NONLOCAL MAINTENANCE
JNCSF-281	Employ strong authenticators for all sessions related to nonlocal maintenance	Operation			MA-4	NONLOCAL MAINTENANCE
JNCSF-282	Employ strong authenticators and authorization measures for those involved in the off-site removal and use of assets	Operation	11.2.5	REMOVAL OF ASSETS		
JNCSF-283	Ensure user sessions and network connections are terminated after the completion of nonlocal maintenance	Operation			MA-4	NONLOCAL MAINTENANCE
JNCSF-284	Obtain maintenance support for system failures in a timely fashion	Operation			MA-6	TIMELY MAINTENANCE
JNCSF-285	Restrict access to media to organization-specified personnel	Operation	8.3.1	MANAGEMENT OF REMOVABLE MEDIA	MP-2	MEDIA ACCESS
JNCSF-286	Indicate distribution limitations, handling caveats, and any security markings on system media as appropriate	Operation			MP-3	MEDIA MARKING
JNCSF-287	Exempt system media from marking if the media remain within defined and controlled areas	Operation			MP-3	MEDIA MARKING
JNCSF-288	Employ safeguards to protect media during transport outside of controlled areas	Operation	8.3.3	PHYSICAL MEDIA TRANSFER	MP-5	MEDIA TRANSPORT
JNCSF-289	Maintain accountability for media during transport outside of controlled areas	Operation	8.3.3	PHYSICAL MEDIA TRANSFER	MP-5	MEDIA TRANSPORT
JNCSF-290	Document activities associated with the transport of media	Operation	8.3.3	PHYSICAL MEDIA TRANSFER	MP-5	MEDIA TRANSPORT
JNCSF-291	Restrict media transport activities to authorized personnel	Operation	8.3.3	PHYSICAL MEDIA TRANSFER	MP-5	MEDIA TRANSPORT
JNCSF-292	Employ sanitization mechanisms at a level in line with the media's security classification	Operation	8.3.2	DISPOSAL OF MEDIA	MP-6	MEDIA SANITIZATION
JNCSF-293	Restrict and prohibit the use of certain types of media on information systems as appropriate	Operation			MP-7	MEDIA USE
JNCSF-294	Identify media requiring downgrading and employ the established downgrading process	Operation			MP-8	MEDIA DOWNGRADING
JNCSF-295	Store multiple copies of valuable information on separate media to reduce risk of damage/loss	Operation	8.3.1	MANAGEMENT OF REMOVABLE MEDIA		
JNCSF-296	Monitor all transfers of information to removable media	Operation	8.3.1	MANAGEMENT OF REMOVABLE MEDIA		
JNCSF-297	Coordinate results of reviews and investigations of physical security controls with the organization incident response capability	Operation			PE-6	MONITORING PHYSICAL ACCESS
JNCSF-298	Enable employees to communicate with information security personnel in case of security incidents at alternate work sites	Operation			PE-17	ALTERNATE WORK SITE
JNCSF-299	Store information system components in locations within facilities that are safe from physical hazards and unauthorized access	Operation	11.2.1	EQUIPMENT SITING AND PROTECTION	PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS
JNCSF-300	Employ regulated asset location technologies to monitor the location of assets within controlled areas	Operation			PE-20	ASSET MONITORING AND TRACKING
JNCSF-301	Discourage unsupervised work in secure areas	Operation	11.1.5	WORKING IN SECURE AREAS		

JNCSF-302	Advise users to terminate or lock information system settings when systems are unattended	Operation	11.2.8	UNATTENDED USER EQUIPMENT			
JNCSF-303	Establish a clear desk and clear screen policy to protect any sensitive information	Operation	11.2.9	CLEAR DESK AND CLEAR SCREEN POLICY			
JNCSF-304	Ensure media and equipment taken off-site has appropriate protections commiserate with sensitivity levels	Operation	11.2.6	SECURITY OF EQUIPMENT AND ASSETS OFF-PREMISES			
JNCSF-305	Maintain a log of all media and equipment taken off-site, including responsible parties for its care and protection	Operation	11.2.6	SECURITY OF EQUIPMENT AND ASSETS OFF-PREMISES			
JNCSF-306	Develop, review, and update a security Concept of Operations (CONOPS) for information systems, as appropriate	Operation			PL-7	SECURITY CONCEPT OF OPERATIONS	
JNCSF-307	Scan for vulnerabilities in information systems and hosted applications	Operation	12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES	RA-5	VULNERABILITY SCANNING	
JNCSF-308	Automate the vulnerability management process by using vulnerability scanning tools that have standards for enumerating platforms, formatting checklists, and measuring vulnerability impact	Operation			RA-5	VULNERABILITY SCANNING	
JNCSF-309	Analyze vulnerability scan reports and results from security control assessments	Operation			RA-5	VULNERABILITY SCANNING	
JNCSF-310	Remediate vulnerabilities in accordance with a risk assessment	Operation	12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES	RA-5	VULNERABILITY SCANNING	
JNCSF-311	Share information from vulnerability scanning processes with appropriate personnel to prevent future similar vulnerabilities	Operation			RA-5	VULNERABILITY SCANNING	
JNCSF-312	Create a timeline for remediating vulnerabilities after receiving notice of such vulnerabilities	Operation	12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES	RA-5	VULNERABILITY SCANNING	
JNCSF-313	Establish roles and responsibilities associated with technical vulnerability management	Operation	12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES			
JNCSF-314	Establish a procedure for what actions to carry out when there is no suitable countermeasure to a vulnerability	Operation	12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES			
JNCSF-315	Employ technical surveillance countermeasures to detect the presence of malicious or unintended surveillance activity	Operation			RA-6	TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY	
JNCSF-316	Determine information security requirements for information systems as part of business process planning	Operation	14.1.1	INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION	SA-2	ALLOCATION OF RESOURCES	
JNCSF-317	Determine, document and allocate necessary resources to protect information services	Operation	14.1.1	INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION	SA-2	ALLOCATION OF RESOURCES	
JNCSF-318	Establish and utilize secure repositories for storing development code	Operation	14.2.1	SECURE DEVELOPMENT POLICY			
JNCSF-319	Establish administrator documentation that describes effective use and maintenance of security functions and mechanisms	Operation			SA-5	INFORMATION SYSTEM DOCUMENTATION	
JNCSF-320	Establish administrator documentation that describes known information system vulnerabilities	Operation			SA-5	INFORMATION SYSTEM DOCUMENTATION	
JNCSF-321	Establish user documentation that describes user responsibilities and methods for maintaining the security of information systems	Operation			SA-5	INFORMATION SYSTEM DOCUMENTATION	
JNCSF-322	Protect and distribute administrator and user information system documentation to appropriate personnel	Operation			SA-5	INFORMATION SYSTEM DOCUMENTATION	
JNCSF-323	Monitor third-parties to ensure compliance with organizational information security requirements and controls	Operation	14.2.6 15.1.2	SECURE DEVELOPMENT ENVIRONMENT ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS	SA-9	EXTERNAL INFORMATION SYSTEM SERVICES	
JNCSF-324	Document, manage, and control the integrity of changes to configuration items	Operation	14.2.2	SYSTEM CHANGE CONTROL PROCEDURES	SA-10	DEVELOPER CONFIGURATION MANAGEMENT	
JNCSF-325	Track security flaws and flaw resolution of information systems and report findings to appropriate personnel	Operation	14.2.3	TECHNICAL REVIEW OF APPLICATIONS AFTER OPERATING PLATFORM CHANGES	SA-10	DEVELOPER CONFIGURATION MANAGEMENT	
JNCSF-326	Change business continuity plans appropriately after making operating platform changes	Operation	14.2.3	TECHNICAL REVIEW OF APPLICATIONS AFTER OPERATING PLATFORM CHANGES			
JNCSF-327	Log the copying and use of operational information for testing	Operation	14.3.1	PROTECTION OF TEST DATA			
JNCSF-328	Employ security safeguards to protect against third-party supply chain threats to information systems	Operation	15.1.1 15.1.3	INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAIN	SA-12	SUPPLY CHAIN PROTECTION	
JNCSF-329	Ensure that third parties follow organizational security requirements throughout the supply chain if they involve other suppliers	Operation	15.1.3	INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAIN			
JNCSF-330	Monitor information system components throughout the supply chain to ensure there are no unauthorized or unwanted modifications	Operation	15.1.3	INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAIN	SA-12	SUPPLY CHAIN PROTECTION	
JNCSF-331	Identify and document the types of third parties allowed access to the organization's information	Operation	15.1.1 15.1.1	INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS			
JNCSF-332	Define, monitor, and control the types of information access that third parties will be allowed	Operation	13.2.2 15.1.2	AGREEMENTS ON INFORMATION TRANSFER ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS			
JNCSF-333	Establish procedures for monitoring third parties' adherence to information security requirements and control effectiveness	Operation	15.1.1 15.2.1	INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS MONITORING AND REVIEW OF SUPPLIER SERVICES	SA-4	ACQUISITION PROCESS	
JNCSF-334	Establish accuracy and completeness controls to ensure the integrity of provided information to/from third parties	Operation	15.1.1	INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS			
JNCSF-335	Establish resilience, recovery and contingency arrangements to ensure the availability of third party and organizational information	Operation	15.1.1	INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS			
JNCSF-336	Require third parties to deliver periodic independent reports on controls' effectiveness and establish an agreed timeline for correcting any issues that arise in the report	Operation	15.1.2 15.2.1	ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS MONITORING AND REVIEW OF SUPPLIER SERVICES			
JNCSF-337	Review third-party audit trails of information security events, operational problems, and failures	Operation	15.2.1	MONITORING AND REVIEW OF SUPPLIER SERVICES			
JNCSF-338	Require the use of development processes that explicitly address security requirements	Operation	14.1.1	INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION	SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS	
JNCSF-339	Require evidence from outsourced developers of acceptable levels of privacy and security quality	Operation	14.2.7	OUTSOURCED DEVELOPMENT			
JNCSF-340	Require evidence from outsourced developers of sufficient testing to guard against malicious content and/or vulnerabilities	Operation	14.2.7	OUTSOURCED DEVELOPMENT			
JNCSF-341	Implement a tamper protection program for all information systems as appropriate	Operation			SA-18	TAMPER RESISTANCE AND DETECTION	
JNCSF-342	Develop and implement anti-counterfeit procedures to prevent counterfeit components from entering information systems	Operation			SA-19	COMPONENT AUTHENTICITY	
JNCSF-343	Report counterfeit information system components to the counterfeit source and appropriate organizational personnel	Operation			SA-19	COMPONENT AUTHENTICITY	
JNCSF-344	Re-implement or custom develop critical information system components that cannot be trusted	Operation			SA-20	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS	
JNCSF-345	Replace information system components no longer supported by developers	Operation			SA-22	UNSUPPORTED SYSTEM COMPONENTS	
JNCSF-346	Configure information systems to separate user functionality from information system management functionality (e.g., using different computers or network addresses for each functionality)	Operation			SC-2	APPLICATION PARTITIONING	
JNCSF-347	Configure information systems to isolate security functions from nonsecurity functions via partitions and domains	Operation			SC-3	SECURITY FUNCTION ISOLATION	
JNCSF-348	Configure information systems to prevent unauthorized and unintended information transfer via shared system resources	Operation			SC-4	INFORMATION IN SHARED RESOURCES	
JNCSF-349	Configure information systems to employ safeguards to protect against denial of service attacks	Operation	13.2.3	ELECTRONIC MESSAGING	SC-5	DENIAL OF SERVICE PROTECTION	
JNCSF-350	Configure information systems to protect the availability of resources using quotas (e.g., priority protection)	Operation			SC-6	RESOURCE AVAILABILITY	
JNCSF-351	Configure information systems to implement subnetworks for publicly accessible system components that are separated from internal networks	Operation	13.1.3	SEGREGATION IN NETWORKS	SC-7	BOUNDARY PROTECTION	
JNCSF-352	Ensure that individual network domains have defined boundaries with appropriate gateway communication protection	Operation	13.1.3	SEGREGATION IN NETWORKS	SC-7 SC-39	BOUNDARY PROTECTION PROCESS ISOLATION	
JNCSF-353	Ensure network segregation assessments are in accordance with access control policies	Operation	13.1.3 13.2.3	SEGREGATION IN NETWORKS ELECTRONIC MESSAGING	SC-39	PROCESS ISOLATION	
JNCSF-354	Configure information systems to protect the confidentiality and integrity of transmitted information	Operation	13.2.1 14.1.3	INFORMATION TRANSFER POLICIES AND PROCEDURES PROTECTING APPLICATION SERVICES TRANSACTIONS	SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	
JNCSF-355	Establish procedures for protecting communicated sensitive electronic information in the form of an attachment	Operation	13.2.1	INFORMATION TRANSFER POLICIES AND PROCEDURES			
JNCSF-356	Establish retention and disposal guidelines for all business correspondence, including messages	Operation	13.2.1	INFORMATION TRANSFER POLICIES AND PROCEDURES			
JNCSF-357	Discourage users from leaving messages containing confidential information on answering machines	Operation	13.2.1	INFORMATION TRANSFER POLICIES AND PROCEDURES			
JNCSF-358	Configure information systems to terminate network connections after a session or after a period of inactivity	Operation			SC-10	NETWORK DISCONNECT	
JNCSF-359	Configure information systems to establish trusted communication paths between users and defined security functions, such as authentication prompts	Operation			SC-11	TRUSTED PATH	
JNCSF-360	Establish a cryptographic key management policy that generates keys for cryptography within information systems	Operation	10.1.2	KEY MANAGEMENT	SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	
JNCSF-361	Establish a cryptographic key management policy that issues and obtains public key certificates for cryptography	Operation	10.1.2	KEY MANAGEMENT	SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	
JNCSF-362	Establish a cryptographic key management policy that distributes keys with instructions of how keys should be activated	Operation	10.1.2	KEY MANAGEMENT	SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	
JNCSF-363	Establish an approach to store cryptographic keys within information systems	Operation	10.1.2	KEY MANAGEMENT	SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	
JNCSF-364	Establish an approach to access cryptographic keys	Operation	10.1.2	KEY MANAGEMENT	SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	
JNCSF-365	Establish procedures for revoking or destroying cryptographic keys when necessary (i.e., when a key is compromised	Operation	10.1.2	KEY MANAGEMENT	SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	
JNCSF-366	Establish procedures for backing up or archiving cryptographic keys	Operation	10.1.2	KEY MANAGEMENT			
JNCSF-367	Establish procedures to appropriately enforce the use of encryption for information transported by mobile or removable media devices or across communication lines	Operation	10.1.1	POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS			
JNCSF-368	Configure information systems to prohibit remote activation of collaborative computing devices unless explicitly noted otherwise	Operation			SC-15	COLLABORATIVE COMPUTING DEVICES	
JNCSF-369	Configure information systems to associate security attributes with information contained in organizational information systems	Operation			SC-16	TRANSMISSION OF SECURITY ATTRIBUTES	
JNCSF-370	Define acceptable and unacceptable mobile code and mobile code technologies	Operation			SC-18	MOBILE CODE	
JNCSF-371	Establish usage restrictions and implementation guidance for mobile code and mobile code technologies	Operation			SC-18	MOBILE CODE	
JNCSF-372	Authorize, monitor, and control the use of mobile code within the information system	Operation			SC-18	MOBILE CODE	
JNCSF-373	Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on their potential damage to information systems if used maliciously	Operation			SC-19	VOICE OVER INTERNET PROTOCOL	
JNCSF-374	Configure information systems to provide additional data origin authentication and integrity verification artifacts, as appropriate	Operation			SC-20	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	
JNCSF-375	Configure information systems to be able to indicate the security status of child zones to enable verification of a chain of trust among parent and child domains	Operation			SC-20	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	
JNCSF-376	Configure information systems to request and perform data origin authentication and data integrity verification on the responses the system receives from authoritative sources	Operation	13.1.1	NETWORK CONTROLS	SC-21	SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	
JNCSF-377	Ensure information systems that provide address resolution services are fault tolerant and implement internal/external role separation	Operation			SC-22	ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE	
JNCSF-378	Configure information systems to protect the authenticity of communication sessions	Operation	14.1.3	PROTECTING APPLICATION SERVICES TRANSACTIONS	SC-23	SESSION AUTHENTICITY	
JNCSF-379	Configure information systems to fail to a known state in the event of a system failure to preserve information	Operation			SC-24	FAIL IN KNOWN STATE	
JNCSF-380	Include information system components to attract malicious attacks to detect, deflect, and analyze attacks (i.e., honeypots)	Operation			SC-26	HONEYPOTS	
JNCSF-381	Configure information systems to include platform-independent applications as appropriate	Operation			SC-27	PLATFORM-INDEPENDENT APPLICATIONS	
JNCSF-382	Configure information systems to protect the confidentiality and integrity of information at rest	Operation			SC-28	PROTECTION OF INFORMATION AT REST	
JNCSF-383	Employ a diverse set of information technologies for information system components to reduce the impact of technology-specific vulnerabilities	Operation			SC-29	HETEROGENEITY	
JNCSF-384	Employ concealment and misdirection techniques for information systems to confuse and mislead adversaries	Operation			SC-30	CONCEALMENT AND MISDIRECTION	
JNCSF-385	Perform a covert channel analysis of information system communications to identify potential avenues for covert channels	Operation			SC-31	COVERT CHANNEL ANALYSIS	
JNCSF-386	Estimate the maximum bandwidth of potential covert channels	Operation			SC-31	COVERT CHANNEL ANALYSIS	
JNCSF-387	Partition information systems into components residing in separate environments or physical domains	Operation			SC-32	INFORMATION SYSTEM PARTITIONING	
JNCSF-388	Configure information systems to load and execute the operating environment from hardware-enforced, read-only media	Operation			SC-34	NON-MODIFIABLE EXECUTABLE PROGRAMS	
JNCSF-389	Configure information systems to load and execute applications from hardware-enforced, read-only media as appropriate	Operation			SC-34	NON-MODIFIABLE EXECUTABLE PROGRAMS	
JNCSF-390	Configure information systems to include components that proactively seek to identify malicious activity (i.e., honeyclients)	Operation			SC-35	HONEYCLIENTS	
JNCSF-391	Implement controls that prevent or detect the use of known or suspected malicious websites (e.g., blacklisting)	Operation	12.2.1	CONTROLS AGAINST MALWARE			
JNCSF-392	Implement controls that prevent or detect the use of unauthorized software on information systems	Operation	12.2.1	CONTROLS AGAINST MALWARE			
JNCSF-393	Conduct regular reviews of software and data content supporting critical business processes and investigate unapproved or unauthorized amendments	Operation	12.2.1	CONTROLS AGAINST MALWARE			
JNCSF-394	Install and regularly update malware detection and repair software to scan computers and media	Operation	12.2.1	CONTROLS AGAINST MALWARE			
JNCSF-395	Scan files received over networks, electronic mail downloads, and web pages for malware	Operation	12.2.1 13.2.1	CONTROLS AGAINST MALWARE INFORMATION TRANSFER POLICIES AND PROCEDURES			
JNCSF-396	Implement procedures to regularly collect information about new malware, ensuring the source is qualified and reputable	Operation	12.2.1	CONTROLS AGAINST MALWARE			
JNCSF-397	Define procedures and responsibilities for dealing with malware protection and recovering from malware attacks	Operation	12.2.1	CONTROLS AGAINST MALWARE			
JNCSF-398	Use technical vulnerability management to reduce vulnerabilities that could be exploited by malware	Operation	12.2.1 12.6.1	CONTROLS AGAINST MALWARE MANAGEMENT OF TECHNICAL VULNERABILITIES			
JNCSF-399	Employ out-of-band channels for the physical or electronic transmission of information to individuals	Operation			SC-37	OUT-OF-BAND CHANNELS	
JNCSF-400	Configure information systems to protect external and internal wireless links from signal parameter attacks	Operation	13.1.1	NETWORK CONTROLS	SC-40	WIRELESS LINK PROTECTION	
JNCSF-401	Physically disable or remove connection ports or input/output devices on information systems AS APPROPRIATE	Operation			SC-41	PORT AND I/O DEVICE ACCESS	
JNCSF-402	Configure information systems to prohibit the remote activation of environmental sensing capabilities unless an exception is noted	Operation			SC-42	SENSOR CAPABILITY AND DATA	
JNCSF-403	Configure information systems to provide an explicit indication of sensor use to defined classes of users	Operation			SC-42	SENSOR CAPABILITY AND DATA	
JNCSF-404	Establish usage restrictions and implementation guidance for information system components based on their potential damage to information systems if used maliciously	Operation			SC-43	USAGE RESTRICTIONS	
JNCSF-405	Authorize, monitor, and control the use of information system components	Operation			SC-43	USAGE RESTRICTIONS	
JNCSF-406	Establish a detonation chamber capability to investigate suspicious applications, files, and other potential payloads	Operation			SC-44	DETONATION CHAMBERS	
JNCSF-407	Identify, report, and correct information system flaws	Operation			SI-2	FLAW REMEDIATION	
JNCSF-408	Install security-relevant software and firmware updates within a defined period after the release of updates	Operation			SI-2	FLAW REMEDIATION	
JNCSF-409	Monitor information systems to detect current and possible future attacks	Operation	16.1.1	RESPONSIBILITIES AND PROCEDURES	SI-4	INFORMATION SYSTEM MONITORING	
JNCSF-410	Monitor information systems to detect unauthorized local, network, and remote connections	Operation	16.1.1	RESPONSIBILITIES AND PROCEDURES	SI-4	INFORMATION SYSTEM MONITORING	
JNCSF-411	Identify unauthorized use of information systems through defined monitoring techniques	Operation			SI-4	INFORMATION SYSTEM MONITORING	
JNCSF-412	Deploy monitoring devices within information systems to collect essential monitoring information	Operation			SI-4	INFORMATION SYSTEM MONITORING	

JNCSF-413	Deploy monitoring devices at ad hoc locations within systems to track specific types of transactions as necessary	Operation			SI-4	INFORMATION SYSTEM MONITORING
JNCSF-414	Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion	Operation			SI-4	INFORMATION SYSTEM MONITORING
JNCSF-415	Establish procedures to appropriately increase monitoring upon indication of increased risk to operations, assets, or individuals	Operation			SI-4	INFORMATION SYSTEM MONITORING
JNCSF-416	Receive information system security alerts, advisories, and directives from external organizations	Operation	6.1.4	CONTACT WITH SPECIAL INTEREST GROUPS	SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
JNCSF-417	Disseminate security alerts, advisories, and directives to appropriate personnel	Operation			SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
JNCSF-418	Implement external security directives in a timely fashion, as defined by security policies	Operation			SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
JNCSF-419	Employ integrity verification tools to detect unauthorized changes to software, firmware, and/or information	Operation	13.2.1	INFORMATION TRANSFER POLICIES AND PROCEDURES	SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY
JNCSF-420	Employ spam protecting mechanisms at information system entry and exit points	Operation			SI-8	SPAM PROTECTION
JNCSF-421	Update spam protection mechanisms when new releases are available	Operation			SI-8	SPAM PROTECTION
JNCSF-422	Configure information systems to check the validity of information inputs	Operation			SI-10	INFORMATION INPUT VALIDATION
JNCSF-423	Configure information systems to generate error messages providing necessary corrective actions without revealing exploitable information	Operation	9.4.2	SECURE LOG-ON PROCEDURES	SI-11	ERROR HANDLING
JNCSF-424	Configure information systems to only reveal error messages to appropriate personnel	Operation			SI-11	ERROR HANDLING
JNCSF-425	Handle and retain information and output from information systems over its full life cycle in accordance with policies	Operation			SI-12	INFORMATION HANDLING AND RETENTION
JNCSF-426	Determine mean time to failure (MTTF) for information system components in specific operation environments	Operation			SI-13	PREDICTABLE FAILURE PREVENTION
JNCSF-427	Create substitute information system components and a means to exchange active and standby components within a defined time period during a failure	Operation			SI-13	PREDICTABLE FAILURE PREVENTION
JNCSF-428	Implement non-persistent information system components with known initiation states and periodic terminations	Operation			SI-14	NON-PERSISTENCE
JNCSF-429	Require information owners to ensure that information is appropriately inventoried, classified, and protected	Operation	8.1.2 14.1.1	OWNERSHIP OF ASSETS INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION		
JNCSF-430	Separate operational responsibility for networks from computer operations where appropriate	Operation	13.1.1	NETWORK CONTROLS		
JNCSF-431	Identify and include security mechanisms, service levels, and management requirements of all network services in network services agreements	Operation	13.1.2	SECURITY OF NETWORK SERVICES		
JNCSF-432	Protect all types of records from destruction, unauthorized access, and falsification	Operation	18.1.3 12.4.2	PROTECTION OF RECORDS PROTECTION OF LOG INFORMATION	AU-9	PROTECTION OF AUDIT INFORMATION
JNCSF-433	Issue guidelines on the retention, storage, handling and disposal of records and information	Operation	18.1.3	PROTECTION OF RECORDS		
JNCSF-434	Place restrictions on the import or export of computer hardware and software used for cryptographic functions	Operation	18.1.5	REGULATION OF CRYPTOGRAPHIC CONTROLS		
JNCSF-435	Establish multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts	Operation				
JNCSF-436	Establish replay-resistant authentication mechanisms for network access to appropriate accounts or functions. (for example - privileged accounts)	Operation				
JNCSF-437	Establish minimum password complexity, password change, and reuse restriction protocols	Operation				
JNCSF-438	Establish cadence to review and update control policies	Foundational	5.1.2	REVIEW OF THE POLICIES FOR INFORMATION SECURITY	AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1 PS-1 RA-1 SA-1 SC-1 SI-1	ACCESS CONTROL POLICY AND PROCEDURES SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES CONFIGURATION MANAGEMENT POLICY AND PROCEDURES CONTINGENCY PLANNING POLICY AND PROCEDURES IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES INCIDENT RESPONSE POLICY AND PROCEDURES SYSTEM MAINTENANCE POLICY AND PROCEDURES MEDIA PROTECTION POLICY AND PROCEDURES PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES SECURITY PLANNING POLICY AND PROCEDURES PERSONNEL SECURITY POLICY AND PROCEDURES RISK ASSESSMENT POLICY AND PROCEDURES SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES
JNCSF-439	Establish, document, and maintain procedures to facilitate the implementation of control policies	Foundational	5.1.1 12.1.1	POLICIES FOR INFORMATION SECURITY DOCUMENTED OPERATING PROCEDURES	AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1 PS-1 RA-1 SA-1 SC-1 SI-1	ACCESS CONTROL POLICY AND PROCEDURES SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES CONFIGURATION MANAGEMENT POLICY AND PROCEDURES CONTINGENCY PLANNING POLICY AND PROCEDURES IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES INCIDENT RESPONSE POLICY AND PROCEDURES SYSTEM MAINTENANCE POLICY AND PROCEDURES MEDIA PROTECTION POLICY AND PROCEDURES PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES SECURITY PLANNING POLICY AND PROCEDURES PERSONNEL SECURITY POLICY AND PROCEDURES RISK ASSESSMENT POLICY AND PROCEDURES SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES
JNCSF-440	Ensure all information systems enforce access rights restrictions consistent with control policies	Foundational	9.4.1	INFORMATION ACCESS RESTRICTION	AC-3	ACCESS ENFORCEMENT
JNCSF-441	Display security notices to users before granting access to information systems stating that users are accessing a U.S. Government information system, if applicable	Foundational			AC-8	SYSTEM USE NOTIFICATION
JNCSF-442	Display security notices to users before granting access to information systems stating that unauthorized use is prohibited and subject to penalties	Foundational	9.4.2	SECURE LOG-ON PROCEDURES	AC-8	SYSTEM USE NOTIFICATION
JNCSF-443	Display security notices to users stating that using information systems implies consent to being monitored and recorded	Foundational			AC-8	SYSTEM USE NOTIFICATION
JNCSF-444	Require users to acknowledge security notices before attempting to access information systems	Foundational			AC-8	SYSTEM USE NOTIFICATION
JNCSF-445	Configure publicly accessible information systems to display appropriate security notices before granting access to users	Foundational			AC-8	SYSTEM USE NOTIFICATION
JNCSF-446	Configure information systems to notify users, upon each successful logon, of the date and time of their last logon	Foundational	9.4.2	SECURE LOG-ON PROCEDURES	AC-9	PREVIOUS LOGON (ACCESS) NOTIFICATION
JNCSF-447	Provide rationale for why certain user actions on information systems do not require user identification or authentication	Foundational			AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
JNCSF-448	Ensure everyone in the organization assesses the appropriate protection level of information by analyzing confidentiality, integrity, and availability	Foundational	8.2.1	CLASSIFICATION OF INFORMATION		
JNCSF-449	Develop and implement procedures to handle assets consistent with their classification	Foundational	8.2.3	HANDLING OF ASSETS		
JNCSF-450	Establish policies on the use of privately owned equipment for teleworking activities	Foundational	6.2.2	TELEWORKING		
JNCSF-451	Provide additional training for personnel using mobile devices	Foundational			AC-19	ACCESS CONTROL FOR MOBILE DEVICES
JNCSF-452	Establish terms and conditions with third-parties to establish how users access information from external information systems	Foundational	15.1.2	ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS	AC-20	USE OF EXTERNAL INFORMATION SYSTEMS
JNCSF-453	Establish terms and conditions with third parties to establish how information is processed, stored, or transmitted on external information systems	Foundational	15.1.2	ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS	AC-20	USE OF EXTERNAL INFORMATION SYSTEMS
JNCSF-454	Create a process that enables authorized users to determine if access rights to sensitive data assigned to sharing partners is appropriate.	Foundational			AC-21	INFORMATION SHARING
JNCSF-455	Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information	Foundational			AC-22	PUBLICLY ACCESSIBLE CONTENT
JNCSF-456	Determine and meet requirements for protection, confidentiality, and integrity of information involved in application services on public networks	Foundational	14.1.2	SECURING APPLICATION SERVICES ON PUBLIC NETWORKS		
JNCSF-457	Establish protection or insurance against liability associated with fraudulent transactions of information involved in application services on public networks	Foundational	14.1.2	SECURING APPLICATION SERVICES ON PUBLIC NETWORKS		
JNCSF-458	Establish procedures to ensure nonpublic information is not posted onto a publicly accessible information system	Foundational			AC-22	PUBLICLY ACCESSIBLE CONTENT
JNCSF-459	Provide ongoing security awareness training to employees and contractors upon hiring with continued training at regularly defined intervals	Foundational	7.2.2	INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING	AT-2	SECURITY AWARENESS TRAINING
JNCSF-460	Provide awareness training to employees affected by information system changes	Foundational			AT-2	SECURITY AWARENESS TRAINING
JNCSF-461	Provide ongoing role-based security awareness training to employees and contractors with assigned security roles and responsibilities	Foundational	7.2.2 13.2.1	INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING INFORMATION TRANSFER POLICIES AND PROCEDURES	AT-3	ROLE-BASED SECURITY TRAINING
JNCSF-462	Provide role-based awareness training to employees with assigned security roles and responsibilities that are affected by information system changes	Foundational			AT-3	ROLE-BASED SECURITY TRAINING
JNCSF-463	Update awareness training materials over time, incorporating lessons learned from security incidents	Foundational	7.2.2	INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING		
JNCSF-464	Update awareness training materials as employee and contractor roles change	Foundational	7.2.2	INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING		
JNCSF-465	Document, monitor, and retain individual information system security training activities and records	Foundational			AT-4	SECURITY TRAINING RECORDS
JNCSF-466	Configure information systems to provide audit record generation capabilities for auditable events	Foundational			AU-12	AUDIT GENERATION
JNCSF-467	Coordinate with external organizations to define acceptable procedures before sharing audit information cross-organizationally	Foundational			AU-16	CROSS-ORGANIZATIONAL AUDITING
JNCSF-468	Develop a security assessment plan that lists the security controls being assessed, and the assessment procedures and roles	Foundational			CA-2 SA-11	SECURITY ASSESSMENTS DEVELOPER SECURITY TESTING AND EVALUATION
JNCSF-469	Establish a procedure to assess the effectiveness of information system security controls' effectiveness	Foundational			CA-2 SA-11	SECURITY ASSESSMENTS DEVELOPER SECURITY TESTING AND EVALUATION
JNCSF-470	Produce security assessment reports that provide the results of the assessments to appropriate personnel	Foundational			CA-2 SA-11	SECURITY ASSESSMENTS DEVELOPER SECURITY TESTING AND EVALUATION
JNCSF-471	Review and update security planning based on findings from security controls assessments and security impact analyses	Foundational	18.2.2	COMPLIANCE WITH SECURITY POLICIES AND STANDARDS	CA-5 SA-11	PLAN OF ACTION AND MILESTONES DEVELOPER SECURITY TESTING AND EVALUATION
JNCSF-472	Record and review managers' corrective actions to increase compliance of information security requirements	Foundational	18.2.2	COMPLIANCE WITH SECURITY POLICIES AND STANDARDS		
JNCSF-473	Provide regular contingency training to users upon assuming a contingency role or after an information system change	Foundational			CP-3	CONTINGENCY TRAINING
JNCSF-474	Require users to sign a statement to keep personal and shared secret authentication information confidential	Foundational	9.2.4 9.3.1	MANAGEMENT OF SECRET AUTHENTICATION INFORMATION OF USERS USE OF SECRET AUTHENTICATION INFORMATION		
JNCSF-475	Define procedures to notify appropriate personnel of information spills using communication methods not associated with the spill	Foundational	16.1.5	RESPONSE TO INFORMATION SECURITY INCIDENTS	IR-9	INFORMATION SPILLAGE RESPONSE
JNCSF-476	Ensure compliance with all information system and network maintenance requirements imposed by insurance policies	Foundational	11.2.4	EQUIPMENT MAINTENANCE		
JNCSF-477	Physically control and securely store media within controlled areas	Foundational	8.3.1 18.1.3	MANAGEMENT OF REMOVABLE MEDIA PROTECTION OF RECORDS	MP-4	MEDIA STORAGE
JNCSF-478	Protect media until it is destroyed or sanitized using approved equipment and procedures	Foundational	8.3.1	MANAGEMENT OF REMOVABLE MEDIA	MP-4	MEDIA STORAGE
JNCSF-479	Sanitize media prior to disposal in accordance with federal and/or organizational policies	Foundational	8.3.2 11.2.7	DISPOSAL OF MEDIA SECURE DISPOSAL OR REUSE OF EQUIPMENT	MP-6	MEDIA SANITIZATION
JNCSF-480	Develop, approve, and maintain a list of individuals with authorized access to facilities	Foundational			PE-2	PHYSICAL ACCESS AUTHORIZATIONS
JNCSF-481	Issue authorization credentials for facility access	Foundational	11.1.2	PHYSICAL ENTRY CONTROLS	PE-2	PHYSICAL ACCESS AUTHORIZATIONS
JNCSF-482	Review facility access lists and remove any individuals for whom access is no longer required	Foundational	11.1.2	PHYSICAL ENTRY CONTROLS	PE-2	PHYSICAL ACCESS AUTHORIZATIONS
JNCSF-483	Enforce physical access authorizations at entry/exit points using devices and/or guards to verify individual access authorizations	Foundational	11.1.1	PHYSICAL SECURITY PERIMETER	PE-3	PHYSICAL ACCESS CONTROL
JNCSF-484	Maintain physical access audit logs for entry/exit points and frequently review as needed	Foundational	11.1.2	PHYSICAL ENTRY CONTROLS	PE-3 PE-6	PHYSICAL ACCESS CONTROL MONITORING PHYSICAL ACCESS
JNCSF-485	Provide safeguards to control access to publicly accessible areas within the facility	Foundational			PE-3	PHYSICAL ACCESS CONTROL
JNCSF-486	Provide safeguards to control access to publicly accessible areas within facilities	Foundational				
JNCSF-487	Secure and frequently change keys, combinations, and other physical access devices when needed (lost keys, terminated individuals)	Foundational			PE-3	PHYSICAL ACCESS CONTROL
JNCSF-488	Employ safeguards to control physical access to information system distribution and transmission lines	Foundational	11.2.3	CABLING SECURITY	PE-4	ACCESS CONTROL FOR TRANSMISSION MEDIUM
JNCSF-489	Control physical access to output devices to prevent unauthorized individuals from obtaining output	Foundational			PE-5	ACCESS CONTROL FOR OUTPUT DEVICES
JNCSF-490	Monitor physical access to the facilities to detect and respond to physical security incidents	Foundational			PE-6	MONITORING PHYSICAL ACCESS
JNCSF-491	Escort visitors and monitor activity by maintaining and frequently reviewing visitor access records to facilities	Foundational	11.1.2	PHYSICAL ENTRY CONTROLS	PE-8 PE-3	VISITOR ACCESS RECORDS PHYSICAL ACCESS CONTROL
JNCSF-492	Protect power equipment and power cabling for information systems from damage and destruction	Foundational	11.2.3	CABLING SECURITY	PE-9	POWER EQUIPMENT AND CABLING
JNCSF-493	Provide the ability to shut off power to information systems in emergency situations	Foundational			PE-10	EMERGENCY SHUTOFF
JNCSF-494	Place emergency power shutoff devices in safe location to facilitate easy access for personnel and prevent unauthorized activation	Foundational			PE-10	EMERGENCY SHUTOFF
JNCSF-495	Provide a short-term uninterruptible power supply for use in the event of a primary power source loss	Foundational	11.2.2	SUPPORTING UTILITIES	PE-11	EMERGENCY POWER
JNCSF-496	Employ and maintain automatic emergency lighting that activates in the event of an emergency	Foundational	11.2.2	SUPPORTING UTILITIES	PE-12	EMERGENCY LIGHTING
JNCSF-497	Employ and maintain fire emergency devices supported by an independent energy source	Foundational			PE-13	FIRE PROTECTION
JNCSF-498	Maintain temperature and humidity levels in facilities at an acceptable level and frequently monitor levels	Foundational	11.2.1	EQUIPMENT SITING AND PROTECTION	PE-14	TEMPERATURE AND HUMIDITY CONTROLS
JNCSF-499	Provide master shutoff valves to protect information systems from water leak damages	Foundational			PE-15	WATER DAMAGE PROTECTION
JNCSF-500	Authorize, monitor, control, and record the entry/exit of information system components into and out of facilities	Foundational	11.1.6	DELIVERY AND LOADING AREAS	PE-16	DELIVERY AND REMOVAL
JNCSF-501	Employ defined security controls at alternate work sites	Foundational			PE-17	ALTERNATE WORK SITE
JNCSF-502	Assess the effectiveness of security controls at alternate work sites	Foundational			PE-17	ALTERNATE WORK SITE
JNCSF-503	Install, monitor, and test security alarms on all fire exits, external doors, and accessible windows	Foundational	11.1.1	PHYSICAL SECURITY PERIMETER		
JNCSF-504	Establish strict access controls for areas in facilities that house confidential information	Foundational	11.1.2	PHYSICAL ENTRY CONTROLS		
JNCSF-505	Discourage the use of unauthorized photographs or videos in secure areas	Foundational	11.1.5	WORKING IN SECURE AREAS		
JNCSF-506	Inspect delivered material before it enters facilities	Foundational	11.1.6	DELIVERY AND LOADING AREAS		

JNCSF-507	Ensure individuals understand and formally acknowledge the behavior expectations regarding information system usage	Foundational	7.2.1 7.2.2	MANAGEMENT RESPONSIBILITIES INFORMATION SECURITY AWARENESS. EDUCATION AND TRAINING	PL-4	RULES OF BEHAVIOR
JNCSF-508	Implement and utilize campaigns and booklets to raise awareness about information security in the organization	Foundational	7.2.2	INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING		
JNCSF-509	Review and update behavior rules frequently and ensure individuals understand new rules	Foundational			PL-4	RULES OF BEHAVIOR
JNCSF-510	Review and re-educate individuals on appropriate skills, qualifications, and security behavior	Foundational	7.2.1	MANAGEMENT RESPONSIBILITIES	PL-4	RULES OF BEHAVIOR
JNCSF-511	Assign a risk designation to all organizational positions, and frequently review and update the designations	Foundational			PS-2	POSITION RISK DESIGNATION
JNCSF-512	Establish a process to screen all individuals filling organizational positions	Foundational	7.1.1	SCREENING	PS-2	POSITION RISK DESIGNATION
JNCSF-513	Screen individuals prior to authorizing access to the information system	Foundational	7.1.1 14.2.6	SCREENING SECURE DEVELOPMENT ENVIRONMENT	PS-3 SA-21	PERSONNEL SCREENING DEVELOPER SCREENING
JNCSF-514	Rescreen individuals after certain organization-defined conditions are met	Foundational			PS-3	PERSONNEL SCREENING
JNCSF-515	Revoke all authenticators and security-related information system-related property upon termination of employment	Foundational	8.1.4 13.2.4	RETURN OF ASSETS CONFIDENTIALITY OR NONDISCLOSURE AGREEMENTS	PS-4	PERSONNEL TERMINATION
JNCSF-516	Conduct exit interviews to discuss necessary information security topics with individuals upon termination of employment	Foundational			PS-4	PERSONNEL TERMINATION
JNCSF-517	Retain access to organizational information and information systems controlled by terminated individuals	Foundational	13.2.4	CONFIDENTIALITY OR NONDISCLOSURE AGREEMENTS	PS-4	PERSONNEL TERMINATION
JNCSF-518	Specify ownership of information. trade secrets. and intellectual property in non-disclosure agreements	Foundational	13.2.4	CONFIDENTIALITY OR NONDISCLOSURE AGREEMENTS		
JNCSF-519	Specify actions to be taken in case of a breach of non-disclosure agreements	Foundational	13.2.4	CONFIDENTIALITY OR NONDISCLOSURE AGREEMENTS		
JNCSF-520	Specify permitted use of confidential information and rights of signatories to use information in non-disclosure agreements	Foundational	13.2.4	CONFIDENTIALITY OR NONDISCLOSURE AGREEMENTS		
JNCSF-521	Review and modify access authorizations to information systems/facilities upon transferal of individuals within the organization	Foundational	7.3.1	TERMINATION OR CHANGE OF EMPLOYMENT RESPONSIBILITIES		
JNCSF-522	Identify and communicate to individuals being terminated or transferred within the organization any changes in access authorizations to information systems and/or facilities	Foundational	7.3.1	TERMINATION OR CHANGE OF EMPLOYMENT RESPONSIBILITIES		
JNCSF-523	Initiate any necessary transfer actions upon transferal of individuals (e.g., returning and issuing new ID cards, changing authorizations)	Foundational			PS-5	PERSONNEL TRANSFER
JNCSF-524	Develop and document user access agreements for information systems	Foundational	13.2.4 7.1.2	CONFIDENTIALITY OR NONDISCLOSURE AGREEMENTS TERMS AND CONDITIONS OF EMPLOYMENT	PS-6	ACCESS AGREEMENTS
JNCSF-525	Establish and document third-party personnel security requirements including security roles and responsibilities	Foundational			PS-7	THIRD-PARTY PERSONNEL SECURITY
JNCSF-526	Require third-party providers to comply with personnel security requirements	Foundational	8.1.3 15.1.2	ACCEPTABLE USE OF ASSETS ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS	PS-7	THIRD-PARTY PERSONNEL SECURITY
JNCSF-527	Require third-party providers to notify the organization of third-party personnel transfers with information system privileges/credentials	Foundational			PS-7	THIRD-PARTY PERSONNEL SECURITY
JNCSF-528	Employ a sanctions process when individuals do not comply with information security policies	Foundational	7.2.3	DISCIPLINARY PROCESS	PS-8	PERSONNEL SANCTIONS
JNCSF-529	Notify appropriate personnel of any employee sanctions processes taking place and the reason for the sanction	Foundational			PS-8	PERSONNEL SANCTIONS
JNCSF-530	Conduct background checks of prospective employees requiring character references and verification of professional and academic qualifications	Foundational	7.1.1	SCREENING		
JNCSF-531	Conduct background checks of prospective employees requiring identity verification and review of criminal records	Foundational	7.1.1	SCREENING		
JNCSF-532	Ensure access agreements state the employee's legal responsibilities and rights	Foundational	7.1.2	TERMS AND CONDITIONS OF EMPLOYMENT		
JNCSF-533	Ensure access agreements state acceptable use of information and organizational assets	Foundational	7.1.2	TERMS AND CONDITIONS OF EMPLOYMENT	PS-6	ACCESS AGREEMENTS
JNCSF-534	Ensure access agreements state acceptable use of third-party information	Foundational	7.1.2	TERMS AND CONDITIONS OF EMPLOYMENT		
JNCSF-535	Ensure access agreements state consequences for disregarding the organization's security requirements	Foundational	7.1.2	TERMS AND CONDITIONS OF EMPLOYMENT		
JNCSF-536	Categorize information and information systems in accordance to applicable laws and policies to describe adverse impacts of information being compromised	Foundational			RA-2	SECURITY CATEGORIZATION
JNCSF-537	Document and explain in security plans how security categorizations of information and information systems reflect any adverse impacts of compromised information	Foundational			RA-2	SECURITY CATEGORIZATION
JNCSF-538	Conduct assessments of risk on all projects, including the likelihood or harm from unauthorized access, use, modification or destruction of information systems and the information they store	Foundational	6.1.5	INFORMATION SECURITY IN PROJECT MANAGEMENT	RA-3	RISK ASSESSMENT
JNCSF-539	Document risk assessment results and disseminate results to appropriate personnel	Foundational			RA-3	RISK ASSESSMENT
JNCSF-540	Review risk assessment results at frequent intervals	Foundational			RA-3	RISK ASSESSMENT
JNCSF-541	Update risk assessments after significant changes to information systems occur, or other organization-defined conditions are met	Foundational			RA-3	RISK ASSESSMENT
JNCSF-542	Utilize risk assessment results to determine which security and/or physical controls should be implemented	Foundational	10.1.1 11.2.6 14.2.2 11.1.1	POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS SECURITY OF EQUIPMENT AND ASSETS OFF-PREMISES SYSTEM CHANGE CONTROL PROCEDURES PHYSICAL SECURITY PERIMETER		
JNCSF-543	Conduct risk assessments at three levels: organization, mission/business process, and information system level	Foundational			RA-3	RISK ASSESSMENT
JNCSF-544	Create acquisition contracts for information systems including security functional, strength, and assurance requirements	Foundational			SA-4	ACQUISITION PROCESS
JNCSF-545	Include security-related documentation requirements and requirements for protecting such documentation in all information system acquisition contracts	Foundational			SA-4	ACQUISITION PROCESS
JNCSF-546	Include a description of information system development environments in all information system acquisition contracts	Foundational			SA-4	ACQUISITION PROCESS
JNCSF-547	Include acceptance criteria in all information system acquisition contracts	Foundational			SA-4	ACQUISITION PROCESS
JNCSF-548	Include identified security requirements in all information system acquisition contracts	Foundational	14.1.1 15.1.1	INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS	SA-4	ACQUISITION PROCESS
JNCSF-549	Establish agreements with third parties of management responsibilities for controlling the transmission, dispatch, and receipt of business information	Foundational	13.2.2	AGREEMENTS ON INFORMATION TRANSFER		
JNCSF-550	Establish agreements with third parties of procedures to ensure traceability and non-repudiation of transferred business information	Foundational	13.2.2	AGREEMENTS ON INFORMATION TRANSFER		
JNCSF-551	Establish agreements with third parties of the minimum packing, labeling, and transmission standards for transferred business information	Foundational	13.2.2	AGREEMENTS ON INFORMATION TRANSFER		
JNCSF-552	Establish agreements with third parties of necessary protection measures for transferred business information (e.g., cryptography)	Foundational	13.2.2	AGREEMENTS ON INFORMATION TRANSFER		
JNCSF-553	Implement awareness training for personnel interacting with third-party personnel regarding appropriate behavior	Foundational	15.1.1	INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS		
JNCSF-554	Establish, document, and implement legal regulatory requirements with third parties (e.g., intellectual property rights)	Foundational	15.1.2	ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS		
JNCSF-555	Implement incident management requirements and training with third parties	Foundational	15.1.2 15.2.1	ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS MONITORING AND REVIEW OF SUPPLIER SERVICES		
JNCSF-556	Implement agreements with third parties to audit all processes and controls	Foundational	15.1.2 15.2.1	ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS MONITORING AND REVIEW OF SUPPLIER SERVICES		
JNCSF-557	Manage any changes to agreements with third-parties and re-assess any new risks as appropriate	Foundational	15.2.2	MANAGING CHANGES TO SUPPLIER SERVICES		
JNCSF-558	Manage and re-assess risks associated with any changes the organization makes to current services, systems, or policies and procedures	Foundational	15.2.2	MANAGING CHANGES TO SUPPLIER SERVICES		
JNCSF-559	Implement assurance measures to achieve satisfactory levels of trustworthiness required in information systems supporting critical business functions	Foundational			SA-13	TRUSTWORTHINESS
JNCSF-560	Require outsourced developers to remain compliant with applicable laws and control efficiency verification	Foundational	14.2.7	OUTSOURCED DEVELOPMENT		
JNCSF-561	Provide documented and approved justification for the continued use of unsupported system components	Foundational			SA-22	UNSUPPORTED SYSTEM COMPONENTS
JNCSF-562	Establish policies, controls, and restrictions associated with using communication facilities	Foundational	13.2.1	INFORMATION TRANSFER POLICIES AND PROCEDURES		
JNCSF-563	Advise personnel about the problems facsimile machines or services pose for information security	Foundational	13.2.1	INFORMATION TRANSFER POLICIES AND PROCEDURES		
JNCSF-564	Establish procedures for auditing cryptographic key management related activities	Foundational	10.1.2	KEY MANAGEMENT		
JNCSF-565	Configure information systems to implement cryptography in accordance with federal laws	Foundational	10.1.1	POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS	SC-13	CRYPTOGRAPHIC PROTECTION
JNCSF-566	Define roles and responsibilities for cryptography policy implementation and key management	Foundational	10.1.1	POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS		
JNCSF-567	Incorporate flaw remediation into the organizational configuration management process	Foundational			SI-2	FLAW REMEDIATION
JNCSF-568	Obtain legal opinion with regard to information system monitoring activities as appropriate	Foundational			SI-4	INFORMATION SYSTEM MONITORING
JNCSF-569	Provide information system monitoring information to defined personnel as needed	Foundational			SI-4	INFORMATION SYSTEM MONITORING
JNCSF-570	Establish, document, and implement rules stating acceptable use of information system information	Foundational	8.1.3	ACCEPTABLE USE OF ASSETS		
JNCSF-571	Identify and document approaches to meet all relevant legislative statutory, regulatory, and contractual requirements	Foundational	18.1.1	IDENTIFICATION OF APPLICABLE LEGISLATION AND CONTRACTUAL REQUIREMENTS	AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1 PS-1 RA-1 SA-1 SC-1 SI-1	ACCESS CONTROL POLICY AND PROCEDURES SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES CONFIGURATION MANAGEMENT POLICY AND PROCEDURES CONTINGENCY PLANNING POLICY AND PROCEDURES IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES INCIDENT RESPONSE POLICY AND PROCEDURES SYSTEM MAINTENANCE POLICY AND PROCEDURES MEDIA PROTECTION POLICY AND PROCEDURES PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES SECURITY PLANNING POLICY AND PROCEDURES PERSONNEL SECURITY POLICY AND PROCEDURES RISK ASSESSMENT POLICY AND PROCEDURES SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES
JNCSF-572	Require compliance with mandatory or discretionary methods of access by federal authorities to encrypted information	Foundational	18.1.5	REGULATION OF CRYPTOGRAPHIC CONTROLS		
JNCSF-573	Design and apply physical protection against natural disasters. malicious attacks. and accidents	Foundational	11.1.4	PROTECTING AGAINST EXTERNAL AND ENVIRONMENTAL THREATS		
JNCSF-574	Site key facilities to avoid access by the public	Foundational	11.1.3	SECURING OFFICES, ROOMS AND FACILITIES		
JNCSF-575	Ensure any directories and internal telephone books containing locations of confidential information processing facilities are not accessible to unauthorized personnel	Foundational	11.1.3	SECURING OFFICES, ROOMS AND FACILITIES		
JNCSF-576	Prevent non-privileged users from executing privileged functions and audit the execution of such functions	Foundational				