ACT CONTROL POLICY AND PROCEDURES
SECURITY ASSESSMENT AND AUTOCIDARES
SECURITY ASSESSMENT AND AUTOCIDARES
SECURITY ASSESSMENT AND AUTOCIDARES
CONTRIGUES AND AND AUTOCIDARES
CONTRIGUES AND AND AUTOCIDARES
CONTRIGUES AND AND AUTOCIDARES
CONTRIGUES AND AUTOCIDARES
CONTRIGUES AND AUTOCIDARES
SECURITY ASSESSMENT AND AUTOCIDARES
SECURITY AUTOCIDARES
SECURATIVA DISCUDARES
SESTIMA AUTOCIDARES
SECURATIVA DISCUDARES
SECURATIVA DISCUDARES
SECURATIVA DISCUDARES
SESTIMA AUTOCIDARES
SECURATIVA DISCUDARES
SESTIMA AUTOCIDAR CM-1 CP-1 IA-1 IR-1 IR-1 PE-1 PE-1 PS-1 PS-1 PS-1 SI-1 SI-1 SI-1 AC-1 CM-1 CM-1 CM-1 IA-1 IR-1 IR-1 Security in Architecture and Portfolio 5.1.1 POLICIES FOR INFORMATION SECURITY 9.1.1 ACCESS CONTROL POLICY JNCSF-1 Develop and document control policies Security in Architecture and Portfolio 5.1.1 POLICIES FOR INFORMATION SECURITY JNCSF-2 Work with information owners to set appropriate control policies MA-1 MP-1 PE-1 PL-1 PS-1 RA-1 SA-1 SC-1 SI-1 INFORMATION SECURITY IN PROJECT MANAGEMENT INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION INFORMATION SECURITY IN PROJECT MANAGEMENT INFORMATION SYSTEMS AUDIT CONTROLS nts and risks in all project management Security in Architecture and Portfolio 6.1.5 14.1.1 6.1.5 INCSE-4 Address information security in all project management Ensure management agrees with audit requirements for access to information systems and data, as appropriate Security in Architecture and Portfolio JNCSF-5 JNCSF-6 12.7.1 appropriate Acagin a senior-level executive as the authorizing official for information systems Develop and document a granular inventory of current, authorized information system components on all information excited. Benergia and concert executive and the authorized effort in domatons systems
 Benergia and concert a grandar intensity of current, authorized information systems
 Benergia and concert and grandar intensity of current, authorized information systems
 Benergia and concerts
 < SECURITY AUTHORIZATION INFORMATION SYSTEM COMPONENT INVENTORY INTELLECTUAL PROPERTY RIGHTS INVENTORY OF ASSETS INVENTORY OF ASSETS 18.1.2 8.1.1 8.1.1 JNCSF-7 CM-8 JNCSF-8 CM-8 INFORMATION SYSTEM COMPONENT INVENTORY JNCSF-9 PL-2 SYSTEM SECURITY PLAN JNCSF-10 PL-2 SYSTEM SECURITY PLAN INCSE-11 ANINTENANCE TOOLS JNCSF-12 5.1.1 POLICIES FOR INFORMATION SECURITY SYSTEM SECURITY PLAN SYSTEM SECURITY PI AN JNCSF-13 PI -2 INCSE-14 PI -8 INFORMATION SECURITY ARCHITECTURE JNCSF-15 PL-8 INFORMATION SECURITY ARCHITECTURE JNCSF-16 PL-8 INFORMATION SECURITY ARCHITECTURE JNCSF-17 PL-8 INFORMATION SECURITY ARCHITECTURE JNCSF-18 JNCSF-19 JNCSF-20 JNCSF-21 PL-9 SA-2 SA-13 CENTRAL MANAGEMENT ALLOCATION OF RESOURCES TRUSTWORTHINESS JNCSF-22 14.2.7 OUTSOURCED DEVELOPMENT SA-17 FVELOPER SECURITY ARCHITECTURE AND DESIGN DISTRIBUTED PROCESSING AND STORAGE FAIL-SAFE PROCEDURES JNCSF-23 JNCSF-24 SC-36 SI-17 JNCSF-25 18.1.4 PRIVACY AND PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION NCSF-26 Configure information systems to require re-authentication after defined circumstances (e.g., period of Inactivity) Development IA-11 RE-AUTHENTICATION SESSION LOCK Configure information systems to terminate user sessions after defined conditions or trigger events are met Configure information systems to terminate user sessions after defined conditions or triggers are met Designate individuals authorized to post information onto publicly accessible information systems Development JNCSF-27 AC-12 SESSION TERMINATION SECURE LOG-ON PROCEDURES SECURING APPLICATION SERVICES ON PUBLIC NETWORKS EVENT LOGGING INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS SYSTEM CHANGE CONTROL, RPOCEDURES INFORMATION SYSTEMS AUDIT CONTROLS MANAGEMENT OF TECHNICAL VULKERABILITIES 9.4.2 14.1.2 12.4.1 12.5.1 14.2.2 12.7.1 12.6.1 JNCSF-28 JNCSF-29 AC-22 PUBLICLY ACCESSIBLE CONTENT INCSF-30 Configure information systems to generate audit records of all relevant information about every auditable Development event CONTENT OF AUDIT RECORDS AUDIT GENERATION CONFIGURATION CHANGE CONTROL AU-3 AU-12 CM-3 NCSF-31 Document interface characteristics, security requirements, and the nature of information for each internal connection between information systems Development
 ANCSF-31
 Connection between information systems

 ANCSF-32
 Develop, document, and maintain a baseline configuration of all information systems

 ANCSF-32
 Develop, document, and maintain a baseline configuration of all information systems
 CA-9 INTERNAL SYSTEM CONNECTIONS INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS DOCUMENTED OPERATING PROCEDURES CHANGE MANAGEMENT SYSTEM CHANGE CONTROL PROCEDURES INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS CHANGE MANAGEMENT SYSTEM CHANGE CONTROL PROCEDURES 12.5.1 12.1.1 Development CM-2 BASELINE CONFIGURATION Development 12.1.2 14.2.2 CM-3 CONFIGURATION CHANGE CONTROL JNCSF-34 Document, implement, and review configuration-controlled changes to information systems Development 12.5.1 12.1.2 14.2.2 CM-3 CONFIGURATION CHANGE CONTROL Establish document, and implement restrictive configuration settings for IT components within information systems outcome, and approve and doctations from configuration settings. Development belowing document, and implement a configuration management plan for information systems that establishes note and responselbilities. Those the configuration management establishes Development. INCSE-25 CM-6 CONFIGURATION SETTINGS CONFIGURATION SETTINGS JNCSF-36 JNCSF-37 CM-6 CM-9 CONFIGURATION MANAGEMENT PLAN SECURE DEVELOPMENT ENVIRONMENT INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS RESTRICTIONS ON SOFTWARE INSTALLATIONS INTELLECTUAL PROPERTY RIGHTS JNCSF-38 CM-9 CONFIGURATION MANAGEMENT PLAN 14.2.6 12.5.1 12.6.2 18.1.2 Development JNCSF-39 Establish and enforce policies governing the installation of software installation by users CM-11 USER-INSTALLED SOFTWARE Ensure changes to operational systems are tested in a different environment requiring different user profiles than that of operational systems a testabilish a system such a diffectiveness of the contingency plan, review the results, and initiate Review the information security continuity plan when there are any changes information systems or management. JNCSE-40 Development 12.1.4 SEPARATION OF DEVELOPMENT, TESTING AND OPERATIONAL ENVIRONMENTS INCSE-41 Development 17.1.3 VERIFY, REVIEW AND EVALUATE INFORMATION SECURITY CONTINUITY CP-4 CONTINGENCY PLAN TESTING JNCSF-42 Development 17.1.3 VERIFY, REVIEW AND EVALUATE INFORMATION SECURITY CONTINUITY VIEWF, RAVIEW AND EVALUATE INFORMATION SECURITY CONTINUITY INFORMATION BACKUP ACCESS TO NETWORKS AND NETWORK SERVICES PASSWORD MAINAGEMENT SYSTEM MAIAGEMENT OSETIA JUTHENTICATION INFORMATION OF USERS SECURE LOG ON PROCEDURES PASSWORD MAINAGEMENT SYSTEM Development Development Development Development JNCSF-43 JNCSF-44 12.3.1 9.1.2 manazement Establish a system to reaular test backuo media to ensure the interrity of the information Configure information systems to identify and authenticate devices before establishing a network DEVICE IDENTIFICATION AND AUTHENTICATION JNCSF-45 JNCSF-46 Ensure authenticators are high-quality and sufficiently secure Change default authenticators prior to information system installation AUTHENTICATOR MANAGEMENT AUTHENTICATOR MANAGEMENT 9.4.3 9.2.4 IA-5 Exure authenticators are high-quality and sufficiently server
Canage default authenticators prote to information system installation
Canage default authenticators prote to information system installation
Canage default authenticators prote to information system installation
Canage default authenticators prote to information during authentication processes
Development
Configure information systems to bakaure authentication organizational users, as aspropriate
Configure information systems to bakaure authenticate no cognizational users, as aspropriate
Ensure access to program source code in restricted an deforced with artic authentication procedures and
Development
Cat supporting utilities resultivity on sume functional to explorations
Development
Information security considerations
Development
Information
Develo 9.4.2 9.4.3 JNCSF-47 14-6 AUTHENTICATOR FEEDBACK INCSE-48 14-7 CRYPTOGRAPHIC MODULE AUTHENTICATION ITIFICATION AND AUTHENTICATION (N IA-8 ON-ORGANIZATIONAL USERS JNCSF-50 ACCESS CONTROL TO PROGRAM SOURCE CODE JNCSF-51 JNCSF-52 9.4.5 11.2.2 14.2.6 ACCESS CONTROL TO PROGRAM SOURCE CODE SUPPORTING UTILITIES SECURE DEVELOPMENT ENVIRONMENT SA-3 SYSTEM DEVELOPMENT LIFE CYCLE INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION JNCSF-54 JNCSF-55 14.1.1 14.1.1 SYSTEM DEVELOPMENT LIFE CYCLE 54-3 SYSTEM DEVELOPMENT LIFE CYCLE JNCSF-56 14.2.1 SECURE DEVELOPMENT POLICY SA-3 SYSTEM DEVELOPMENT LIFE CYCLE Development Development SECURE DEVELOPMENT POLICY SECURE DEVELOPMENT POLICY JNCSF-57 JNCSF-58 14.2.1 14.2.1 JNCSF-55 SA-5 INFORMATION SYSTEM DOCUMENTATION Uddate information system documentation after anv system chanee Development Apolv information system socurity ensineering orinciples in the development of information systems. Development Review socurity engineering procedures to ensure their effectivenes. Development 14.2.2 14.2.5 14.2.5 SYSTEM CHANGE CONTROL PROCEDURES SECURE SYSTEM ENGINEERING PRINCIPLES SECURE SYSTEM ENGINEERING PRINCIPLES JNCSF-60 JNCSF-61 JNCSF-62 54-8 SECURITY ENGINEERING PRINCIPLES DEVELOPER CONFIGURATION MANAGEMENT CONFIGURATION CHANGE CONTROL DEVELOPER CONFIGURATION MANAGEMENT SA-10 CM-3 SA-10 JNCSF-63 Require information system developers to perform configuration management during system development Development 14.2.2 SYSTEM CHANGE CONTROL PROCEDURES negarie manusch system Uerbegreis us phane to linger sond angement. Gung system Uerbegreien Bereisgereis Review and ets application control and integrity procedures after making operating platform changes Review and ensystem developer to stand en values whether newly implemented socurity controls are implemented correctly and operating a intended 14.2.2 14.2.3 14.2.8 JNCSF-64 JNCSF-65 SYSTEM CHANGE CONTROL PROCEDURES TECHNICAL REVIEW OF APPLICATIONS AFTER OPERATING PLATFORM CHANGES SA-11 DEVELOPER SECURITY TESTING AND EVALUATION JNCSF-66 SYSTEM SECURITY TESTING control are implemented correctly and operating as intended
Require independent system acceptance testing for new information systems and changes to existing ones
Development
Require sequerate authorization existem into protect confidentiality of test data
Development
Require sequerate authorization existem into costect confidentiality of test data
Development
Require sequerate authorization existem into costect confidentiality of test data
Development
Require sequerate authorization existem into costect confidentiality of test data
Development
Require sequerate authorization existem interview of the costect confidentiality of test data
Development
Perform citically analyses throughout the system development life cycle to identify critical information
Development
Development JNCSF-67 14.2.9 SYSTEM ACCEPTANCE TESTING JNCSF-68 JNCSF-69 JNCSF-70 PROTECTION OF TEST DATA PROTECTION OF TEST DATA PROTECTION OF TEST DATA 14.3.1 14.3.1 14.3.1 JNCSF-71 SA-14 CRITICALITY ANALYSIS Require use of a development process that identifies and documents tools used in the development process Development JNCSF-72 SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS Require use of a development process that identifies and documents tools used in the development process. Below to the development process that identifies and documents and ensures the integrity of charges to the development process that ensures that the process, standards, and tools staffy and the staffy JNCSF-73 14.2.2 SYSTEM CHANGE CONTROL PROCEDURES SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS JNCSF-74 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS SA-15 14.2.1 SECURE DEVELOPMENT POLICY JNCSF-75 SA-16 DEVELOPER-PROVIDED TRAINING DEVELOPER SECURITY ARCHITECTURE AND DESIGN JNCSF-76 SA-17 JNCSF-77 SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN JNCSF-78 DEVELOPER SECURITY ARCHITECTURE AND DESIGN SA-17 JNCSF-79 OUTSOURCED DEVELOPMENT Employ nutrine environment of the events of the event of the Development Development Development OUTSOURCED DEVELOPMENT SECURE DEVELOPMENT ENVIRONMENT SECURE DEVELOPMENT ENVIRONMENT JNCSF-80 JNCSF-81 JNCSF-82 14.2.7 14.2.6 14.2.6 SA-21 DEVELOPER SCREENING 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 Ensure information system components have the minimal required level of functionality and information Development JNCSF-84 Ensure memoration system Compositions user use minume and exection of the composition of SC-25 THIN NODES JNCSF-85 JNCSF-86 JNCSF-87 14.2.6 12.5.1 SECURE DEVELOPMENT ENVIRONMENT INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS FLAW REMEDIATION MALICIOUS CODE PROTECTION JNCSF-88 SI-3 MALICIOUS CODE PROTECTION INCSE-89 13.2.1 INFORMATION TRANSFER POLICIES AND PROCEDURES \$1-3 MALICIOUS CODE PROTECTION

	Configure malicious code protections to perform defined actions in response to malicious code detection	
JNCSF-90 JNCSF-91	Configure maincipus code protections to perform defined actions in response to maincipus code detection (e.g., block code, send alert to administrator) Address any faise positives during malicipus code detection and their impact on the availability of	Development Development
JNCSF-92	information systems Notify appropriate personnel of any failed security verification tests and take appropriate actions upon	Development
JNCSF-93	failure Configure information systems to validate that information output from software programs is consistent with its expected content	Development
JNCSF-94	Configure information systems to implement security safeguards to protect its memory from unauthorized code execution	Development
JNCSF-95	Define and distribute user account types for information systems and networks where applicable	Delivery
JNCSF-96	Assign access rights to all user accounts, consistent with control policies	Delivery
JNCSF-97	Assign account managers for all information system accounts	Delivery
JNCSF-98 JNCSF-99	Emolov ohvsical or looical access controls to restrict users' access rights to sensitive apolications or data Ensure all information systems manage the flow of information within and between connected systems, consistent with control policies	Delivery Delivery
JNCSF-100	Formally separate sensitive duties among multiple individuals to prevent access rights abuses or conflicts of interest	Delivery
JNCSF-101 JNCSF-102	Define information system access authorizations that enforce separation of duties for sensitive activities Manaze access rights to be consistent with the principle of least privileze	Delivery
JNCSF-103	Identify and document which user actions are permitted on information systems without user identification or authentication	Delivery
JNCSF-104	Define and allocate all information security responsibilities, stating specific assets and processes for which individuals are responsible	Delivery
JNCSF-105	Prevent unauthorized access to mobile devices by using physical protection against theft, cryptographic techniques, and secret authentication information	Delivery
JNCSF-106 JNCSF-107	Establish procedures to ensure access control decisions are applied consistently with control policies Assign different user IDs to be used only for privileged access rights, separate from regular business activities	Delivery Delivery
JNCSF-108	Allow authorized personnel to select how and which auditable events will be audited by specific components of information systems	Delivery
JNCSF-109	Ensure the authorizing official authorizes information systems for processing before commencing operations	Delivery
JNCSF-110	Establish an emergency change process to quickly implement changes to processes and information systems needed to resolve an incident	
JNCSF-111	Establish a committee to periodically coordinate and provide oversight for configuration-controlled changes	Delivery
JNCSF-112 JNCSF-113	Define, document, approve, and enforce access restrictions associated with information system changes	Delivery
JNCSF-113 JNCSF-114	Establish a rollback strategy before implementing system changes Establish a formal approval for information system changes from authorized users	Delivery
JNCSF-115 JNCSF-116	Document rules for transferring software from development to operational, and ensure they are run on different systems. Configure information systems to identify and authenticate organizational users	Delivery Delivery
JNCSF-117	Establish an information systems to identify and automiticate organizational users Establish an information system and user identifier management system to select and assign identifiers to individuals or groups	Delivery
JNCSF-118	Prevent the reuse of information system and user identifiers for a defined time period	Delivery
JNCSF-119 INCSF-120	Establish procedures to verify the identity of a user prior to providing new secret authentication information	Delivery Delivery
JNCSF-121 JNCSF-122	Provide temporary, secure, and unique authentication information upon initial user registration Establish lifetime restrictions and conditions on reusing and changing authenticators Chance authenticators for reuso or role accounts when membership channes	Delivery Delivery Delivery
JNCSF-123 JNCSF-124	Identify and authenticate information system services using approved safesuard measures Restrict use, authorization, and availability of utility programs that can override system and application	Delivery
JNCSF-125 JNCSF-126	controls Establish a process for granting and documenting maintenance personnel authorization	Delivery Delivery
JNCSF-126 JNCSF-127	Ensure non-escorted maintenance personnel have required access authorizations Designate competent and authorized personnel to supervise maintenance activities of un-authorized personnel	Delivery
JNCSF-128	Establish a media downgrading process using mechanisms commensurate with the media's level of security and access authorization	Delivery
JNCSF-129 JNCSF-130	Require authorization for media removal where necessarv Grant restricted physical access to external support service personnel only when required	Delivery Delivery
JNCSF-131 JNCSF-132	Review and update user access agreements as needed Ensure that individuals sign appropriate access agreements prior to receiving access and after access agreements have been updated	Delivery Delivery
JNCSF-133	agreements have been oppared Ensure an authorized individual reviews and approves security categorization decisions associated with information and information systems	Delivery
JNCSF-134	Establish user documentation that describes how to effectively use user-accessible security functions of information systems	Delivery
JNCSF-135 JNCSF-136	Ensure security and protection of information systems and system components throughout their delivery in the supply chain process Configure information systems to verify the correct operation of security functions (e.g., authentication)	Delivery Delivery
JNCSF-138 JNCSF-137	Establish a process to assign information ownership to appropriate individuals in a timely fashion	Delivery
JNCSF-138	Require information owners to define and review access restrictions to important information	Delivery
JNCSF-139	Establish a process to routinely review that user access rights align with control policies	Operation
JNCSF-140	Establish a process to evaluate and approve or reject access right requests consistent with control policies	Operation
JNCSF-141	Establish a process to appropriately remove or adjust access rights from users as specified in control policies	Operation
JNCSF-142	Configure information systems to limit the number of unsuccessful logon attempts within a defined time period	Operation
JNCSF-143	period Configure information systems to lock user accounts after the maximum number of permitted unsuccessful logon attempts is exceeded	Operation
JNCSF-144	Log unsuccessful and successful logon attempts and display this information upon a successful login Configure information systems to limit the number of concurrent user sessions for account types, as	Operation Operation
JNCSF-146	appropriate. Configure information systems to prevent further user access (e.g., a session lock) after a defined period of user inactivity	Operation
JNCSF-147	user inactivity Provide the ability to tag information based on sensitivity. Ensure information is appropriately tagged and that tags remain associated with information at rest and in	Operation Operation
JNCSF-148	transit Establish capabilities to ensure information is appropriately tagged and that tags remain associated with	Operation
JNCSF-150 JNCSF-151	information at rest and in transit Define the range of appropriate information tags for each information system Establish clear procedures, suidelines, and requirements for all allowed types of remote user access	Operation Operation
JNCSF-152 JNCSF-153	establish clear proceedures, guidelines, and requirements for all allowed types or remote user access Maintain appropriate contacts with professional specially in the event of a security incident Maintain appropriate contacts with professional special interest groups	Operation Operation
JNCSF-154	Address communication security requirements for teleworking activities and provide suitable communication equipment	Operation
JNCSF-155 JNCSF-156	Ensure teleworking sites are secure, both physically and from unauthorized access Establish requirements and restrictions on the configuration of wireless network services and the use of	Operation Operation
JNCSF-157	home networks Establish policies on the use of malware protection for teleworking equipment Configure information systems to require appropriate authorization procedures before allowing remote	Operation
JNCSF-158 JNCSF-159	user access Establish usage restrictions (by establishing authentication or encryption protocols),	Operation Operation
JNCSF-160	configuration/connection requirements. and implementation guidance for wireless access Configure wireless networks to require appropriate authorization procedures before allowing wireless access	
JNCSF-161	Ensure users can only access networks and network services they are authorized to use	Operation
JNCSF-162	Establish usage restrictions, configuration/connection requirements, and implementation guidance for organization-controlled mobile devices	Operation
JNCSF-163 JNCSF-164	Configure information systems to require authorization procedures before connecting mobile devices Take appropriate verification and protection measures to protect payment methods on public networks	Operation Operation
JNCSF-165	from fraud Employ data-mining prevention and detection techniques to prevent unapproved data mining activity. Configure information systems to implement tamperproof reference monitors for access control policies	Operation
JNCSF-166 JNCSF-167	that are small enough to be analyzed and tested Ensure information systems are capable of logging events deemed auditable	Operation Operation
JNCSF-168 JNCSF-169 INCSF-170	Coordinate with other organizational functions to guide the selection of auditable events Configure event logs to record alarms raised by the access control system	Operation Operation Operation
JNCSF-171	Establish and maintain audit record storage requirements Conflueure information systems to alert appropriate personnel after an audit-processing failure Configure information systems to take specified actions after an audit processing failure (e.g., shut down	Operation
JNCSF-172 JNCSF-173	information system, stop generating audit records, etc.) Establish cadence to review information system audit records and report any unusual activity to appropriate	Operation Operation
JNCSF-174	personnel Log all system administrator and system operator activities and protect these logs	Operation
JNCSF-175	Configure information systems to provide on-demand audit reviews and after-the-fact security incident investigations Configure information systems to ensure the generation of audit reports and reductions do not alter any	Operation
JNCSF-176 JNCSF-177	compare information systems to ensure the generation of adult reports and reductions do not aren any orizinal log data Configure information systems to use internal system clocks to record time stamps for all audit records	Operation Operation
JNCSF-178	Configure information systems to protect against individuals falsely denying having performed auditable events	Operation
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 Monitor open source information sources for evidence of unauthorized disclosure of organizational	Operation
JNCSF-180 JNCSF-181	information Configure information systems to provide the capability for authorized users to select a user session to	Operation Operation
JNCSF-182	record or view Provide a backup audit capability in case of a failure in the primary audit capability	Operation
JNCSF-183	Document and implement approaches to establish a single reference time across all information systems and synchronize internal clocks Ensurer audit requirements and activities on operational systems are carefully planned and defined to	Operation
JNCSF-184 JNCSF-185	Ensure audit requirements and activities on operational systems are carefully planned and defined to minimize disruptions to organizational processes Control the scope of technical audit tests, and limit them to read-only access to software and data	Operation Operation
JNCSF-186	Develop and document a plan to remediate weaknesses or vulnerabilities discovered during security controls assessments	Operation
JNCSF-187	Conduct periodic independent reviews of the organization's approach to managing and implementation of information security Ensure managers review that information security requirements defined in policies are met in their area of	Operation
JNCSF-188 JNCSF-189	Ensure managers review that information security requirements defined in policies are met in their area of responsibility Establish cadence to review and update the security authorization of information systems	Operation Operation
JNCSF-190	Implement a continuous monitoring program with security control assessments, security status monitoring, analysis of information, and established response actions	Operation
JNCSF-191 JNCSF-192	Conduct frequent penetration testing on information systems and system components Ensure all penetration tests are conducted by trained specialists under supervision and are conducted in a user what minimized inclusions interaction advector provided and and according to the second statement of	Operation Operation
JNCSF-193	way that minimizes unintended, adverse impacts on the organization Ensure all internal connections of information system components to information systems are appropriately authorized	

		SI-3	MALICIOUS CODE PROTECTION
		SI-3	MALICIOUS CODE PROTECTION
		SI-6	SECURITY FUNCTION VERIFICATION
		SI-15 SI-16	INFORMATION OUTPUT FILTERING
		31-10	MEMORY PROTECTION
9.2.2 9.2.3 9.2.1	USER ACCESS PROVISIONING MANAGEMENT OF PRIVILEGED ACCESS RIGHTS USER REGISTRATION AND DE-REGISTRATION	PR	ACCESS CONTROL
9.1.2	ACCESS TO NETWORKS AND NETWORK SERVICES USER ACCESS PROVISIONING	AC-2	ACCOUNT MANAGEMENT
9.2.3	MANAGEMENT OF PRIVILEGED ACCESS RIGHTS	AC-2	ACCOUNT MANAGEMENT
9.4.1	INFORMATION ACCESS RESTRICTION	AC-4	INFORMATION FLOW ENFORCEMENT
6.1.2	SEGREGATION OF DUTIES	AC-5	SEPARATION OF DUTIES
9.4.4	USE OF PRIVILEGED UTILITY PROGRAMS	AC-5	SEPARATION OF DUTIES
9.4.4	MANAGEMENT OF PRIVILEGED ACCESS RIGHTS	AC-6	LEAST PRIVILEGE
6.1.1		AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
6.2.1	INFORMATION SECURITY ROLES AND RESPONSIBILITIES	AC-19	ACCESS CONTROL FOR MOBILE DEVICES
0.2.2	MOBILE DEVICE POLICY	AC-24	ACCESS CONTROL POR MOBILE DEVICES
9.2.3	MANAGEMENT OF PRIVILEGED ACCESS RIGHTS		
		AU-12	AUDIT GENERATION
12.1.2	CHANGE MANAGEMENT	CA-6	SECURITY AUTHORIZATION
12.1.2	CHANGE MANAGEMENT	CM-3	CONFIGURATION CHANGE CONTROL
12.5.1	INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS	CM-5	
14.2.6 14.2.2 12.5.1	SECURE DEVELOPMENT ENVIRONMENT SYSTEM CHANGE CONTROL PROCEDURES INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS	CM-5	ACCESS RESTRICTIONS FOR CHANGE
12.1.2 14.2.2	CHANGE MANAGEMENT SYSTEM CHANGE CONTROL PROCEDURES	CM-3	CONFIGURATION CHANGE CONTROL
12.1.4	SEPARATION OF DEVELOPMENT, TESTING AND OPERATIONAL ENVIRONMENTS		
9.4.1	INFORMATION ACCESS RESTRICTION	IA-2 IA-4	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) IDENTIFIER MANAGEMENT
9.4.3	PASSWORD MANAGEMENT SYSTEM USER REGISTRATION AND DE-REGISTRATION	IA-4	IDENTIFIER MANAGEMENT
9.2.1 9.2.4	USER REGISTRATION AND DE-REGISTRATION MANAGEMENT OF SECRET AUTHENTICATION INFORMATION OF USERS	IA-5	AUTHENTICATOR MANAGEMENT
9.2.4 9.4.3	MANAGEMENT OF SECRET AUTHENTICATION INFORMATION OF USERS PASSWORD MANAGEMENT SYSTEM	IA-5 IA-5	AUTHENTICATOR MANAGEMENT AUTHENTICATOR MANAGEMENT
9.2.6	REMOVAL OR ADJUSTMENT OF ACCESS RIGHTS	IA-5 IA-9	AUTHENTICATOR MANAGEMENT SERVICE IDENTIFICATION AND AUTHENTICATION
9.4.4	USE OF PRIVILEGED UTILITY PROGRAMS		
11.2.4	EQUIPMENT MAINTENANCE	MA-5 MA-5	MAINTENANCE PERSONNEL MAINTENANCE PERSONNEL
		MA-5	MAINTENANCE PERSONNEL
8.3.1	MANAGEMENT OF REMOVABLE MEDIA	MP-8	MEDIA DOWNGRADING
11.1.2 13.2.4	PHYSICAL ENTRY CONTROLS CONFIDENTIALITY OR NONDISCLOSURE AGREEMENTS	PS-6	ACCESS AGREEMENTS
7.1.2	TERMS AND CONDITIONS OF EMPLOYMENT	PS-6	ACCESS AGREEMENTS
		RA-2	SECURITY CATEGORIZATION
		SA-5	INFORMATION SYSTEM DOCUMENTATION
15.1.3	INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAIN	SA-12 SI-6	SUPPLY CHAIN PROTECTION SECURITY FUNCTION VERIFICATION
8.1.2 8.1.2	OWNERSHIP OF ASSETS OWNERSHIP OF ASSETS		
8.1.2	OWNERSHIP OF ASSETS		
9.2.5 9.2.2 9.2.3	REVIEW OF USER ACCESS RIGHTS USER ACCESS PROVISIONING MANAGEMIENT OF PRIVILEGED ACCESS RIGHTS	AC-2	ACCOUNT MANAGEMENT
9.2.3 9.2.2 9.2.3	MARAGEMENT OF PRIVILEGED ACCESS RIGHTS USER ACCESS PROVISIONING MARAGEMENT OF PRIVILEGED ACCESS RIGHTS	AC-2	ACCOUNT MANAGEMENT
9.2.6	REMOVAL OR ADJUSTICENT OF ACCESS RIGHTS USER ACCESS PROVISIONING	AC-2 PS-4	ACCOUNT MANAGEMENT PERSONNEL TERMINATION
9.2.5	REVIEW OF USER ACCESS RIGHTS	PS-5 AC-7	PERSONNEL TRANSFER UNSUCCESSFUL LOGON ATTEMPTS
			UNSUCCESSFUL LOGON ATTEMPTS
9.4.2	SECURE LOG-ON PROCEDURES	AC-7	CONCURRENT SESSION CONTROL
		AC-10	SESSION LOCK
8.2.1	CLASSIFICATION OF INFORMATION	AC-11	
		AC-16	SECURITY ATTRIBUTES
8.2.2	LABELLING OF INFORMATION	AC-16	
8.2.1 6.2.2 6.1.3	CLASSIFICATION OF INFORMATION TELEWORKING CONTACT WITH AUTHORITIES	AC-16 AC-17	SECURITY ATTRIBUTES REMOTE ACCESS
6.1.4	CONTACT WITH AD HOATIES CONTACT WITH SPECIAL INTEREST GROUPS TELEWORKING		
6.2.2	TELEWORKING		
6.2.2 13.1.1	TELEWORKING NETWORK CONTROLS		
6.2.2	TELEWORKING	AC-17	REMOTE ACCESS
		AC-18	REMOTE ACCESS WIRELESS ACCESS
9.1.2 13.1.1	ACCESS TO NETWORKS AND NETWORK SERVICES NETWORK CONTROLS	AC-18	WIRELESS ACCESS
9.1.2 13.1.1	ACCESS TO NETWORKS AND NETWORK SERVICES NETWORK CONTROLS		
6.2.1	MOBILE DEVICE POLICY	AC-19	ACCESS CONTROL FOR MOBILE DEVICES
6.2.1 14.1.2	MOBILE DEVICE POLICY SECURING APPLICATION SERVICES ON PUBLIC NETWORKS	AC-19	ACCESS CONTROL FOR MOBILE DEVICES
		AC-23 AC-25	DATA MINING PROTECTION REFERENCE MONITOR
		AU-2	AUDIT EVENTS
12.4.1	EVENT LOGGING	AU-2	AUDIT EVENTS
12.4.2	PROTECTION OF LOG INFORMATION	AU-4 AU-5	AUDIT STORAGE CAPACITY RESPONSE TO AUDIT PROCESSING FAILURES
12.4.1	EVENT LOGGING	AU-5 AU-6	RESPONSE TO AUDIT PROCESSING FAILURES AUDIT REVIEW, ANALYSIS, AND REPORTING
12.4.1	ADMINISTRATOR AND OPERATOR LOGS ADMINISTRATOR AND OPERATOR LOGS	CM-3	CONFIGURATION CHANGE CONTROL
		AU-7	AUDIT REDUCTION AND REPORT GENERATION
		AU-7	AUDIT REDUCTION AND REPORT GENERATION
12.4.4 14.1.1	CLOCK SYNCHRONISATION INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION	AU-8 AU-10	TIME STAMPS NON-REPUDIATION
18.1.3	PROTECTION OF RECORDS	AU-11	AUDIT RECORD RETENTION
		AU-13	MONITORING FOR INFORMATION DISCLOSURE
		AU-14	SESSION AUDIT
12.4.4	CLOCK SYNCHRONISATION	AU-15 AU-8	ALTERNATE AUDIT CAPABILITY
12.4.4	CLOCK SYNCHRONISATION	AU-8	THE STANTS
12.7.1	INFORMATION SYSTEMS AUDIT CONTROLS		
CA-5 SA-11 18.2.1	PLAN OF ACTION AND MILESTONES DEVELOPER SECURITY TESTING AND EVALUATION		
18.2.1	INDEPENDENT REVIEW OF INFORMATION SECURITY		
	COMPLIANCE WITH SECURITY POLICIES AND STANDARDS	CA-6	SECURITY AUTHORIZATION
18.2.3	TECHNICAL COMPLIANCE DD CT	CA-7 CA-8	CONTINUOUS MONITORING
18.2.3 18.2.3	TECHNICAL COMPLIANCE REVIEW TECHNICAL COMPLIANCE REVIEW	LA-8	PENETRATION TESTING
		CA-9	INTERNAL SYSTEM CONNECTIONS

JNCSF-194	Conduct security impact analyses of changes to information systems prior to implementing changes	Operation
JNCSF-195	Monitor and control changes to the configuration settings in accordance with organization policies	Operation
JNCSF-196 JNCSF-197	Prohibit functions, ports, protocols, and/or services on information systems as appropriate Track software usage to ensure compliance with contract agreements and copyright laws	Operation Operation
JNCSF-198 JNCSF-199	Document the use of peer-to-peer file sharing technology to ensure there is no unauthorized use of copyrighted work	Operation Operation
JNCSF-200	Monitor software installation ooliv: comoliance at frequent intervals Archive old versions of software, with all required information, procedures and configuration details Monitor the use of resources to make projections of future capacity requirements to ensure efficiency of	Operation
JNCSF-201	system performance Develop a contingency plan for all information systems that provides recovery objectives, restoration	Operation Operation
JNCSF-202	priorities, and metrics Determine if information security continuity is captured in the business continuity or disaster recovery	Operation
JNCSF-204	management process Determine requirements for the continuity of information security management during a crisis and imolement such management	Operation
JNCSF-205 JNCSF-206	Develop a contingency plan that addresses contingency roles and responsibilities Develop a contingency plan that addresses full information system restoration without compromising	Operation Operation
JNCSF-200	original security safeguards Ensure that third-parties are aware of business continuity procedures and are able to implement such	Operation
JNCSF-208	procedures if needed Develop incident response and contingency security plans and/or documented processes that meet mission, size. structure, and functions requirements of organization	Operation
JNCSF-209	Size, structure, and initiations requirements of organization Ensure security plans for maintaining information system security are reviewed frequently and are approved by appropriate personnel	Operation
JNCSF-210	Ensure incident response and contingency security plans and/or documented processes are reviewed frequently and are approved by appropriate personnel	Operation
JNCSF-211	Distribute copies of security plans for maintaining information system security to identified key personnel Distribute copies of incident response and contineency security plans and documented processes to	Operation
JNCSF-212 JNCSF-213	identified key personnel	Operation Operation
JNCSF-213	Coordinate contingency planning activities with incident handling activities Ensure contingency planning and incident response procedures are updated to address gaps as they are	Operation
JNCSF-215	discovered Communicate changes in security plans for maintaining information system security to appropriate personnel	Operation
JNCSF-216	Protect security plans for maintaining information system security from unauthorized disclosure and modification	Operation
JNCSF-217	Protect incident response and contingency security plans and documented processes from unauthorized disclosure and modification	Operation
JNCSF-218	Establish an alternate storage site with agreements to permit the storage and retrieval of system backup information	Operation
JNCSF-219	Ensure that the information security safeguards are equivalent at both primary and alternate storage sites	Operation
JNCSF-220 JNCSF-221	Establish alternate processing sites with agreements permitting the transfer and resumption of operations Ensure that the necessary equipment and support is available for transfer/resumption at alternate	Operation Operation
JNCSF-222	processing sites Ensure that the information security safeguards are equivalent at the primary and alternate processing sites	Operation
JNCSF-223	Establish alternate telecommunications services that permits the resumption of operations Establish alternate telecommunications services that permits the resumption of critical operations during	Operation Operation
JNCSF-224 JNCSF-225	disruptions Conduct frequent backups of user- and system-level information in all information systems	Operation Operation
JNCSF-226 JNCSF-227	Conduct frequent backups of information system documentation including security-related documentation	Operation
JNCSF-227 JNCSF-228 JNCSF-229	Protect confidentiality. interrity. and availability of backup information at storase locations Protect backup information by means of encryotion in situations where confidentiality is important Establish capabilities to recover and reconstitute information systems to a known state after a disruption,	Operation Operation Operation
JNCSF-229 JNCSF-230	compromise, or failure Configure information systems to be able to employ alternative communications protocols to maintain	Operation Operation
JNCSF-231	continuity of operations during disruptions Configure information systems to enter a safe mode of operation under organization-defined conditions,	Operation
JNCSF-232	such as during an incident Identify technical vulnerabilities and their associated risks using information resources and develop appropriate actions to be taken	Operation
JNCSF-233	Align technical vulnerability management with incident management activities to communicate data on vulnerabilities	Operation
JNCSF-234 JNCSF-235	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 Operation
JNCSF-235 JNCSF-236	Disable information system and user identifiers after a defined period of activity or as needed Require users to change their passwords at their first log-on	Operation
JNCSF-237 JNCSF-238	Require individuals to use safeguards to protect authenticators from unauthorized use Advise users to avoid keeping a record of secret authentication unless it can be stored in a secure and	Operation Operation
JNCSF-239	approved manner Advise users to change secret authentication information after any indication of its possible compromise	Operation
JNCSF-240	Require electronic signatures for electronic messaging and/or application service transactions to ensure authenticity of users and to protect information transfers	Operation
JNCSF-241 JNCSF-242	Require users to obtain approval prior to using external public messaging services such as instant messaging Require stronger levels of authentication controlling access from publicly accessible networks to electronic	Operation Operation
JNCSF-243	messaeline services Store application service transaction details outside of any publicly accessible environment (e.g., on a	Operation
JNCSF-244	storage platform on the organizational intranet) Ensure that all information and screet authentication involved with application service transactions remain confidential and protected	Operation
JNCSF-245	Require additional authentication information to access information systems under conditions deemed high- risk	Operation
JNCSF-246 JNCSF-247	Ensure users only have access to networks and network services they are authorized to use Maintain a record of access rights granted to users to access information systems and services	Operation Operation
JNCSF-246 JNCSF-247 JNCSF-248 JNCSF-249	Ensure users only have access to networks and network services they are authorized to use Maintain a record of access rights granted to users to access information systems and services Seareaste utility orientamis from applications software on all information systems where applicable Provide frequent incident response training to users you assuming an Riole or after a system change, as	Operation
JNCSF-247 JNCSF-248 JNCSF-249 JNCSF-250	Enum uses only have access to retenois and network survices they are authorized to use Maintain a record or access injets parated to even to access information systems and services Serverate utility corrams from autications software on all information systems where auticable howing frequent informative requests training to users upon axuming an Information Information that and document results of frequent incident response testing to determine incident response effectiveness	Operation Operation Operation Operation
JNCSF-247 JNCSF-248 JNCSF-249	Enum uses only have access to retensists and network survices they are authorised to use Maintain a record or access injets pareted to even to access information systems and services Severate utility aroraman from addications software and all information systems where auxiliable Provide frequent tracings and training to users your assuming an Irol or or after a system change, as approximate Conduct and document results of frequent incident response testing to determine incident response Conduct and document results of frequent incident response testing to determine incident response Conduct and document results of frequent incident response testing to determine incident response testing are apprecisioned and access testing to determine incident response testing are apprecisioned and access the submit of the submit and the submit and the submit and the submit and apprecisioned access the submit and the submit and the submit and the submit and the submit and the submit access the submit and the submit and the submit and testing are apprecisioned and the submit and the submit and the submit and the submit and testing and the submit and testing and the submit and testing and the submit and testing apprecision and testing and the submit and testing and the submit and the submit and testing and testing and testing and testing and testing and the submit and testing and testing and testing and testing and testing and testing and the submit and testing and testing and testing and testing and testing and	Operation Operation Operation
JNCSF-247 JNCSF-248 JNCSF-249 JNCSF-250 JNCSF-251	Ensure uses only have access to retenoisk and network services they are authorised to use Maintain a record of access injets parent do use sito to access information systems and services Serverate utility and access in the parent do use and a information systems where assolicable Provide frequent informative reponse training to users upon assuming as it for lor after a system charge, as appropriate Conduct and document results of frequent incident response testing to determine incident response affectiveness Conduct and document results of frequent incident response testing to determine its effectiveness implement an incident handling capability for security incidents including preparation, detection and applications and accessing accessing accessing and accessing accesing accessing accessing accessing accessing accessing acc	Operation Operation Operation Operation Operation
INCSF-247 INCSF-248 INCSF-249 INCSF-250 INCSF-251 INCSF-252 INCSF-253 INCSF-253	Enum uses only have access to retensivis and network survices they are authorised to use Maintain a need of access injets praced to access information systems and services Serverate utility orarrams from accilications software and all information systems where anoilcable Provide frequent inclusion testings on the survices of the survices of the survices and the survices and access of the survices of the Conduct and document results of frequent incident response testing to determine incident response disclusiversas Conduct and document results of frequent incident response testing to determine in effectiveness implement an indiversa indiversa and recovery implement incident results of incidence response testing to determine incident analysis, conduct and proceeding on the scalable, controlled recovery, and necessary communication testibility provides and the scalable recovery and the scalable and the survices of the scalable and the scalable testing of information scalable needs	Operation Operation Operation Operation Operation Operation Operation
INCSF-247 INCSF-248 INCSF-249 INCSF-250 INCSF-251 INCSF-252 INCSF-253	Enum uses only have access to retensist and network survices they are authorised to use Maintain a record of access injets pareted to sure to access information systems and services Serverate utility aroramas from acciliations software and a information systems where acciliable Provide frequent transfer response training to users yours assuming an Irole or after a system share. As a approximate Conduct and adcoument results of frequent incident response testing to determine incident response Conduct and adcoument results of frequent incident response testing to determine incident response Dendemark and adcoument results of frequent incident response testing to determine incident response analysis, constainment, endication, and recovery. Implement an incident response procedures for escalation, controlled recovery, and necessary communication Establish reporting proceedures for incident response table tables, and detailed reporting of information security events: Usable incident response opabilities based on results from incident handling activities.	Operation Operation Operation Operation Operation Operation Operation
INCSF-247 INCSF-248 INCSF-249 INCSF-250 INCSF-251 INCSF-252 INCSF-253 INCSF-254 INCSF-255	Ensure uses only have access to retensivis and network survices they are authorised to use Maintain a need of access injets pracet to access information systems and services Severate utility arcramam from adications software and al Information systems where auxiliable Provide frequent traches for tension to users your assuming a life or artist a system change, a approximation Conduct and adocument results of frequent incident response testing to determine incident response complement an incident traduition of preservity incidents incident groups and adocument analysis, containment, endication, and recovery implement an incident results of frequent incident response testing to determine incident response analysis, containment, endication, and recovery implement incident regionse procedures for accelation, controlled recovery, and encessary communication Eaclabilish sporting procedures for incident or response that ensure accuratis, immediate, and detailed resporting of information security incidents: Track and document information system varieties incident response oppositions based on results from incident handling activities Track and document information systems variety incidents:	Operation Operation Operation Operation Operation Operation Operation Operation
INCSF-247 INCSF-248 INCSF-249 INCSF-250 INCSF-251 INCSF-252 INCSF-253 INCSF-254 INCSF-256 INCSF-257 INCSF-258	Enum uses only have access to retensivis and network survices they ar authorised to use Maintain are ord of access injets praced to access information systems and services Serverate utility orarisms from accilications software and all information systems where anoilable Provide frequent includent response training to all information systems where accellable access and access the system of the system of the system of the system of the system access and access the system of the system of the system of the system of the system access and access the system of the system of the system of the system of the system analysis, containment, results of frequent incident response testing to determine incident response analysis, containment, eradication, and recovery limplement incident response produced to recaults from incident handling activities Tackand document incident of incidence response that ensure accurate, immediate, and detailed topologic of the system access the system of the system of the system control of information systems security incidents the handling activities Tackand document information system security incidents the incident response capability within a specified tore provide Define procedures to report security incidents the incident response capability within a system offering response to report security incident information to estem al authorities as appropriet	Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation
NICSF-247 JNCSF-248 JNCSF-249 JNCSF-250 JNCSF-252 JNCSF-253 JNCSF-254 JNCSF-256 JNCSF-256 JNCSF-258 JNCSF-258 JNCSF-258 JNCSF-250	Exure uses only have access to retenois and network survices they are authorized to use Maintain a record or access infaits granted to use survices many stream and services Serverate a utility circumset integrates the services in the services and the services in the service of the services of the services and sourcess treams from and solutions to behave on all information networks where avoidable provincing and sourcess treams for fingueses includes treams to the services and sourcess treams of fingueses includes treams testing to determine includes treams analysis, continueme, and and finances includes treams the services determines analysis, continuemes and and financess treams that services and the services analysis, continuemes exabilities based on results from includes treaming activities and advances therein the service sponse that essense accurate, immediate, and detailed recording of information accurity nextens treads in concern termination spectrally includes to the includes treaps treage treams to respect treams that the service treams actuating activities treage treams to respect treams that the service treaps the accurate treage tream to respect treams that the service treams actuating activities treage treams to respect treams that the service treams actuating activities and the activities to the service treams actuation accurate treams and the activities to the includes treams actuation the process to regard treams the security includes to the activities as approprieta activities and the process to provide treams that securities the service treams actuated to the process to regard the security activities to the process to regard treams the tream actuation to the service treams actuated the security includes to the service treams actuated to the treams to regard treams the security includes the topone capacities and the treams to regard treams the treams actuation is actuation actuated to the treams to the topone actuated to the topone treams that the topone acounted t	Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation
NICSF-247 JNCSF-248 JNCSF-249 JNCSF-250 JNCSF-252 JNCSF-252 JNCSF-254 JNCSF-255 JNCSF-256 JNCSF-257 JNCSF-258 JNCSF-258 JNCSF-250 JNCSF-260 JNCSF-261	Enum uses only have access to retensivis and network survives they ar authorised to use Matchian a record or access inplate particle on users to access information systems and services Serverate allife variants from autications subware on all information suberns where auticable hypothesis and document requires fringeant incident reaponse testing to determine incident reaponse directiveness. Conduct and document results of frequent incident reaponse testing to determine incident reaponse directiveness. Conduct and document results of frequent incident reaponse testing to determine incident reaponse directiveness. Canduct and document results of frequent incident reaponse testing to determine incident reaponse directiveness. Canduct and document results of request incident incident reaponse directiveness. Canduct and document results of request incident incident reaponse directiveness. Canduct and document results of results on a control of encourse, and encourse results incident registring particular directiveness. Canduct and document information system security incidents in funding activities. Tacka and document information system security incidents in fundient standing activities. Canduct and the information system security incidents in brokent reaponse approximate are avoid. Define procedures to report security incident in funding test brites as parportized provide hand bling from testing in activities and any security incident in the object reaponse approximate provide the adjustry context is report security incident in the external activities as appropriate provide the incident response particular security incident in the directiveness provide the incident response part information to external activities and argumentation provide the adjustry context in a providential security incidents in the approximate of the incident response patholity.	Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation
NICSF-247 JNICSF-248 JNICSF-249 JNICSF-250 JNICSF-251 JNICSF-252 JNICSF-254 JNICSF-255 JNICSF-256 JNICSF-257 JNICSF-258 JNICSF-250 JNICSF-261 JNICSF-262	Exercise only have access to retenois and network survices they ar authorised to use Matchian a record or access injets pracetor do users to access information system and services Serverate utility corranes from auticities on survices information systems where auticitable howing free information requires the information systems where auticitable howing free information requires of frequent incident response testing to determine incident response directiveness. Conduct and document results of frequent incident response testing to determine incident response analysis, containment, erablication and recovery linghment incident proposes procedures for scatalistics, controlled recovery, and necessary communication Exability reporting proceedures for scatalistics, controlled recovery, and necessary communication Exability reporting proceedures for incident response testing to determine incident regulates testing of information scatarly events to action response procedures for incidents response testing to determine incident and analysis, containment, erablishings based on results from incident handling activities Tackand advancement users to report scatarly incident incident handling activities are provide tability for users to report scatarly incident information to extern al activities appropriate procedures to report suggested security incident information to extern al activities appropriate procedure tability or users to report testing in contained activities appropriate procedures to report scatarly incident information to externita activities appropriate procedures to report scatarly incident information to externita activities appropriate procedures to report scatarly incident information to externita incident response capabilities beeks an incident response plant, incident in the specific testing activities in the specific testing in a contained in the indicident response and incident response plant. Indide	Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation
NICSF-247 JNCSF-248 JNCSF-249 JNCSF-250 JNCSF-252 JNCSF-252 JNCSF-254 JNCSF-255 JNCSF-256 JNCSF-257 JNCSF-258 JNCSF-258 JNCSF-250 JNCSF-260 JNCSF-261	Enumeration only have access to retensivis and network survives they are authorized to use Matchian a record or access inplot spacetor have no access information system and services Serverate allife vorcement from analizations software and information systems where available howeds frequent calculated in the service system and the or after a system hange, an access of the system of the system and the system of the order of the system of the distribution of the system of the system of the system of the order of the system and access of the system of the system of the system of the order of the system of the system of the distribution of the system of th	Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation
NICSF-247 INICSF-248 INICSF-248 INICSF-250 INICSF-251 INICSF-252 INICSF-253 INICSF-255 INICSF-255 INICSF-256 INICSF-261 INICSF-262 INICSF-264 INICSF-264	Euror used with an excess to retenois and network survices they are authorized to used Matchian a record or access inplate granted to use survices matching survices and survices and survices in the authorized to use survices and the authorized to	Operation Operation
NICSF-247 NICSF-248 NICSF-250 NICSF-251 NICSF-252 NICSF-253 NICSF-254 NICSF-256 NICSF-256 NICSF-256 NICSF-259 NICSF-250 NICSF-250 NICSF-261 NICSF-262 NICSF-263 NICSF-264	Exercises only have access to retensive and network survices they are authorised to use Matchian a record or access inplate particle on users to access information systems and services Serverate all the various frequent analysis of the users to access information systems where avoidable howers for an exercise transmitter and the users your assuming and the or after a system change, an access the analysis of the system and the order response testing to determine incident response directiveness. Conduct and document results of frequent incident response testing to determine incident response directiveness. Conduct and document results of frequent incident response testing to determine incident response directiveness. Conduct and document results of frequent incident response testing to determine incident response directiveness. Conduct and document results of frequent incident response testing to determine incident response directiveness. Conduct and document results of the results incident response testing to determine incident response directiveness. Conduct and document results of the results incident response testing to determine incident response directiveness. Conduct and the response application and results from incident handing activities. Takatin document information system security incidents in the incident response application the model model information results from indications in the approximate in the incident develops in incident response path directives in terrorism and responsion for model response applications in the response incident in indication in approximate in the indication response in approximate develops in incident response path the develops in measuring the performance of incident conduction. Conduct analytics response path the develops in measuring the performance of incident response analytics. Conduct response path the develops the rescurst response and management support for management response path the develops the rescurst responses and management support proteips an incident re	Operation Operation
NICSF-247 INICSF-248 INICSF-249 INICSF-250 INICSF-251 INICSF-253 INICSF-254 INICSF-255 INICSF-256 INICSF-257 INICSF-263 INICSF-263 INICSF-263 INICSF-264 INICSF-265 INICSF-265 INICSF-268	Even uses only have access to retensive and network survices they are authorised to use Matchian a record or access injets praced to even to access information system and services Serverat author arcmans from auticutors. Software on al information system where auticubit Provide feasibility and the event is access information system where auticubit Provide feasibility and document results of frequent incident response testing to determine incident response directiveness. Conduct and document results of frequent incident response testing to determine incident response analysis. Conduct and socienter results of frequent incident response testing to determine incident response analysis. Conduct and the socient is a socient incident incident matching accession analysis. Conduct and the socient incident response testing to determine incident response analysis. Conduct and the socient incident response testing to determine incident response analysis. Conduct response portabilities for scaladion, controlled recovery, and necessary communication Exability and the socient response to the socient of the incident response capability within a specified periodic information system exactive incident. Texability access to response teaching the incident response capability active accessing of information system exactive incident. Texability active as goverpristem accessing in contrastive response teaching incident and thereits as goverpristem accessing incident response plant the describes the articutar and approximation of the incident response in addimentation system exactive incident response capability active accessing incident response plant that describes the articutar and approximation of the incident response in addimentation system exactive and management supports for accessing incident response plant that describes the rescursar and management supports for anadation incident response plant that describes the rescursar and management supports for anadation incident response plant that defense the rescursar and manageme	Operation Operation
NICSF-247 NICSF-248 NICSF-249 NICSF-250 NICSF-252 NICSF-252 NICSF-255 NICSF-256 NICSF-256 NICSF-257 NICSF-258 NICSF-261 NICSF-263 NICSF-265 NICSF-268 NICSF-268 NICSF-268 NICSF-268	Example scales only have access to retensivis and network survives they are authorised to usel Matchian a record or access inplate spacet to use sour sourcess information system and services Serverat a click or access inplate spacet to use sour sourcess information systems where available howing factor intervations of frequent incident reaponse testing to determine incident reaponse directiveness. Consider the spacet tamping to use space a subject to the space of a system spacet spacet spacet tamping the space testing to determine incident reaponse directiveness. Consider and sourcess treaking to determine treaking to determine the space space directiveness of the space space directiveness. Consider the space space directive directiveness considers is and treaking activities. Consider treaking activities and the space space directiveness and directiveness. Consider the space space directiveness directiveness the record treaking space treaking activities are activities. Consider the space space directiveness directiveness and the space space space space directiveness. Consider the space space space space directiveness the space space space space space directiveness and the space space space directiveness and the space space space directiveness and the space space space space directiveness and the space space space space directiveness and the space space directiveness and the space space space	Operation Operation
NICSF-247 INICSF-248 INICSF-249 INICSF-250 INICSF-251 INICSF-253 INICSF-254 INICSF-255 INICSF-256 INICSF-257 INICSF-263 INICSF-263 INICSF-263 INICSF-264 INICSF-265 INICSF-265 INICSF-268	Exercise only have access to retensive and network survices they are authorised to use Matchian are order document treasmost anning have not as occess information system and services Serverate allife increases training all ourse your as anning in their or after a system charge. The order treasmost anning all ourse your as anning in their or after a system charge and anning increases the order treasmost anning in the order of a system charge and anning increases the order treasmost anning in the order of a system charge and anning increases the order treasmost anning increases the order of a system charge and anning increases the order treasmost anning increases the order of a system charge and anning increases the order treasmost and the order treasmost testing to determine includent requests and advancement results of frequest includent requests testing to determine includent requests and private models and testing or anning in the order treasmost testing to determine includent requests and private includent requests and testing includents. The order treasmost and testing and the order requests and testing includents and testing activities. The order treasmost approximation system security includent talemust accurate, immediate, and testing and and anning information system security includent talemust accurate, immediates, and testing and and anning information system security includent talemust accurate interposes approximation and the advancement information system security includent talemust accurate anning and treasmost and and anning in indicate treasmost pain, including a and many terming includent requests capabilities and an includent requests pain tale privates the securation and anning meets support for anning in indicate treasmost pain that describes the securation and management support for anning in indicate treasmost pain that describes the caccurate request and management support anning in indicate treasmost capabilities. Develops an indicate treasmost pain tale defines the recetarity resultates	Operation Operation
NICSF-247 NICSF-248 NICSF-249 NICSF-250 NICSF-251 NICSF-253 NICSF-254 NICSF-256 NICSF-256 NICSF-256 NICSF-260 NICSF-261 NICSF-263 NICSF-263 NICSF-264 NICSF-264 NICSF-265 NICSF-266 NICSF-266 NICSF-269 NICSF-269 NICSF-269 NICSF-269	Euror some hy have access to networks and network sortics they are authorised to used Matchian are cored or access index marked to use so access information systems and services Searceat a clinic viaconant from autications. Subsave on all information subsems where auticable provide and document requires fringeuses includent requires testing to determine includent requires distancess access and access and the searce of the searce of the searce of the searce of the distances access and access and the searce of the searce of the searce of the searce of the distances access and includent requires of frequent includent requires testing to determine includent requires and access and includent budging papality for searcing includents includent requires and and sourcement requires of frequent includent requires testing to determine the distances and access and includent budging papality for searcing includents includent requires and analysis, continuents and for searcing includents includent requires accessible access and includent temporus generations accessible accession accessible and accument information searcing views and accession accessible accession of information accessible accession accession accession accession accession accessible accession accession accession accession accession accession accessible accession	Operation Operation
NICSF-247 NICSF-248 NICSF-249 NICSF-251 NICSF-251 NICSF-252 NICSF-255 NICSF-255 NICSF-255 NICSF-256 NICSF-267 NICSF-263 NICSF-263 NICSF-263 NICSF-263 NICSF-263 NICSF-268 NICSF-268 NICSF-268 NICSF-268 NICSF-268 NICSF-268 NICSF-268 NICSF-267 NICSF-270 NICSF-271	Even uses only have access to retensive and network survices they are authorised to use Matchian are order of access injets pracet to access information systems and services Service at ultic vorsame from auticities uses your assume and information systems where auticitable howers for even information requests of information systems index and the order of a system system and document requests of information to descers information systems where audicable howers information requests of information index information systems where audicable howers information requests of information index information systems where audicable howers information requests of information index information index information aughys, containment, erables of includion response testing to determine includent preparation, determine includion requests and recover unplement models in the audica systems in the index information index in the audicable aughys, containment, erables of includion response testing to determine includent and even aughys, containment, erables of includions response testing to determine includion and aughys includion response apostables bare of neurols from includion tanding activities and aughys, contain includion a stemity includies and aughys, contain includion and aughys and aughys and aughys and aughys, contain includion and aughys and aughys and aughys and aughys and the response plant determine includion response apability within a specified area and aughys and aughys and aughys and aughys and aughys and aughys an indicent response plant the describes the autucant and aughys and aughys and aughys and aughys and aughys and aughys and aughys and aughys and aughys an indicent response plant the describes the accessary resources and management supports for autocation consolities. Develops an indicent response plant the describes the accessary resources and management supports and autocation response plant the describes the accessary resources and management supports and automation response plant the defers what exectis	Operation Operat
NGS-247 NGS-248 NGS-248 NGS-248 NGS-252 NGS-252 NGS-252 NGS-252 NGS-252 NGS-252 NGS-252 NGS-252 NGS-252 NGS-254 NGS-254 NGS-254 NGS-264 NGS-264 <td< td=""><td>Even uses only have access to retensive and network survices they are authorised to use Matchian are cored access inplets parted to users your sourcess information systems and services Several activity corresponds to the users your sourcess information systems where auticulable provide feasibility corresponds to the users your sourcess information systems where auticulable provide feasibility of fersaert incident response testing to determine incident response directiveness. Conduct and document results of frequent incident response testing to determine incident response analysis. Conduct results of frequent incident response testing to determine incident response analysis. Conduct results of frequent incident response testing to determine incident response analysis. Conduct results of information incident handing activities Incident response proceedores for scaladion, controlled recovery, and necessary communication Exability activities to activity incident incident handing activities and activities to activity incident incident handing activities results in activity events incident response conductives for incidents the incident response capability within a specified period in distribution structive activity incidents to the incident response capability activity and activity can be alter proport galant information to atternit authorities appropriate activity can be alter proport galant target incident response capability Develope an indicent response plant the directivity incident to measuring the performance of incident activity can be alter proport plant that describes the structure and organization of the incident activity in a scient response plant that describes the structure and activity activity and activity in a scient response plant that describes the rescurser and management support for activity and activity activity activity activity resources and management support for activity and activity activity activity activity activity and activity activity activity activity activity activity activity activ</td><td>Operation Operation Operation Operation</td></td<>	Even uses only have access to retensive and network survices they are authorised to use Matchian are cored access inplets parted to users your sourcess information systems and services Several activity corresponds to the users your sourcess information systems where auticulable provide feasibility corresponds to the users your sourcess information systems where auticulable provide feasibility of fersaert incident response testing to determine incident response directiveness. Conduct and document results of frequent incident response testing to determine incident response analysis. Conduct results of frequent incident response testing to determine incident response analysis. Conduct results of frequent incident response testing to determine incident response analysis. Conduct results of information incident handing activities Incident response proceedores for scaladion, controlled recovery, and necessary communication Exability activities to activity incident incident handing activities and activities to activity incident incident handing activities results in activity events incident response conductives for incidents the incident response capability within a specified period in distribution structive activity incidents to the incident response capability activity and activity can be alter proport galant information to atternit authorities appropriate activity can be alter proport galant target incident response capability Develope an indicent response plant the directivity incident to measuring the performance of incident activity can be alter proport plant that describes the structure and organization of the incident activity in a scient response plant that describes the structure and activity activity and activity in a scient response plant that describes the rescurser and management support for activity and activity activity activity activity resources and management support for activity and activity activity activity activity activity and activity activity activity activity activity activity activity activ	Operation Operation Operation
NGS-3/21 NGS-201 NGS-202 NGS-203 NGS-204 NGS-205 NGS-204 NGS-204 <t< td=""><td>Even used on the access to retention is and network survices they are authorised to use Matchian are cored or access inforts matched or uses uses and manuality in their or after a strategy and provide frequencies treations trateging to strategy and the strategy and they are authorised to access the strategy and trade to access and matching preparation, detections and document retuits of frequent incident response testing to determine incident response and strategy and document retuits of frequent incident response testing to determine incident response and strategy and document retuits of frequent incident response testing to determine incident response and strategy and the strategy and the strategy and the strategy and the strategy and analysis. Analysis and the strategy and the strategy and the strategy and the strategy and analysis. Analysis and the strategy and the strategy and the strategy and the strategy and analysis. Analysis and the strategy and the strategy and the strategy and the strategy and analysis. Analysis and the strategy and</td><td>Operation Operation Operation Operation Operation Operation</td></t<>	Even used on the access to retention is and network survices they are authorised to use Matchian are cored or access inforts matched or uses uses and manuality in their or after a strategy and provide frequencies treations trateging to strategy and the strategy and they are authorised to access the strategy and trade to access and matching preparation, detections and document retuits of frequent incident response testing to determine incident response and strategy and document retuits of frequent incident response testing to determine incident response and strategy and document retuits of frequent incident response testing to determine incident response and strategy and the strategy and the strategy and the strategy and the strategy and analysis. Analysis and the strategy and the strategy and the strategy and the strategy and analysis. Analysis and the strategy and the strategy and the strategy and the strategy and analysis. Analysis and the strategy and the strategy and the strategy and the strategy and analysis. Analysis and the strategy and	Operation Operation Operation Operation Operation Operation
NGS-3/21 NGS-201 NGS-201 <t< td=""><td>Even consistent and exacts to retentionis and network survices they are authorised to used Matchian are cored or access inplate matchine cores to access information systems and services Area and accument requires of information to access and matchines in access and matchines and accument requires of information incident regiones testing to determine incident regiones discusses. The access and accument requires of information incident matchines and accument and accument requires of information incident regiones testing to determine incident regiones discusses. The access and accument requires of information incident regiones testing to determine incident regiones discusses. The access and accument requires of information incident regiones testing to determine incident regiones and accument requires of information incident regiones testing to determine incident regiones and accuments requires and accument regiones that many accument accument accument accument regiones particularly incident to the information testing activation accument accument accument incident regiones testing to determine incident regiones accument accument accument incident regiones capability within a access and accument accument accument incident regiones capability activation accument accument accument incident regiones acquires and accument accument accument accument incident regiones particular accument accument accument accument accument incident regiones accument accument accument accument accument accument accument incident regiones acquires and management support for accument accument accument accument incident regiones acquires and accument acc</td><td>Question Que</td></t<>	Even consistent and exacts to retentionis and network survices they are authorised to used Matchian are cored or access inplate matchine cores to access information systems and services Area and accument requires of information to access and matchines in access and matchines and accument requires of information incident regiones testing to determine incident regiones discusses. The access and accument requires of information incident matchines and accument and accument requires of information incident regiones testing to determine incident regiones discusses. The access and accument requires of information incident regiones testing to determine incident regiones discusses. The access and accument requires of information incident regiones testing to determine incident regiones and accument requires of information incident regiones testing to determine incident regiones and accuments requires and accument regiones that many accument accument accument accument regiones particularly incident to the information testing activation accument accument accument incident regiones testing to determine incident regiones accument accument accument incident regiones capability within a access and accument accument accument incident regiones capability activation accument accument accument incident regiones acquires and accument accument accument accument incident regiones particular accument accument accument accument accument incident regiones accument accument accument accument accument accument accument incident regiones acquires and management support for accument accument accument accument incident regiones acquires and accument acc	Question Que
NGS-3/21 NGS-201 NGS-201 <t< td=""><td>Even used on the access to retenois and network survices they are authorised used Matician are cored or access index materies to access information systems and services Access in a service or access in the survice to access information systems and services Access in a service response training to access in a service or access and the access access in a service response training to access in a service or access and the access in a service response training to access in a service or access access in a service response training to access in a service or access access in a service response training to access in a service or access access in a service response training to access in a service or access access in a service response training to access in a service or access access in a service response training to access in a service or access access in a service response training to access in a service or access access in a service response training to access in a service or access access in a service response training the access in a service or access access in a service response training to access in a service or access access in a service response training the access in a service response in a construction or access training to access in a service response in a construction or access training the access in training activation access an access response plan that describe the access response capability access an access response plan that describe the access response access in a service response and access access in a service response plan that describe the access response access in a service response access an access response plan that describe the access response to a service response plan that describe the access response access access access an access response plan that describe the access response to a service response access access access access an access response plan that describe service service and management support for access an access response response training access response response response response r</td><td>Question Que</td></t<>	Even used on the access to retenois and network survices they are authorised used Matician are cored or access index materies to access information systems and services Access in a service or access in the survice to access information systems and services Access in a service response training to access in a service or access and the access access in a service response training to access in a service or access and the access in a service response training to access in a service or access access in a service response training to access in a service or access access in a service response training to access in a service or access access in a service response training to access in a service or access access in a service response training to access in a service or access access in a service response training to access in a service or access access in a service response training to access in a service or access access in a service response training to access in a service or access access in a service response training the access in a service or access access in a service response training to access in a service or access access in a service response training the access in a service response in a construction or access training to access in a service response in a construction or access training the access in training activation access an access response plan that describe the access response capability access an access response plan that describe the access response access in a service response and access access in a service response plan that describe the access response access in a service response access an access response plan that describe the access response to a service response plan that describe the access response access access access an access response plan that describe the access response to a service response access access access access an access response plan that describe service service and management support for access an access response response training access response response response response r	Question Que
B(S)-247 R(S)-248 R(S)-248 R(S)-248 R(S)-252 R(S)-262 R(S)-262 <t< td=""><td>Even consistent and exacts to retention is and network survices they are subtracted to used Matchian is record or access inplate matched to use sub assessing of matched to subtract and and and and and access the sequent to their substance and information subtram where assoliable for advances the sequent tambing to use sub as assoling of the substances in the or advances and advancessing the substances and information subtram where assoliable for advances the sequent tambing to the substance and the substances and advancessing the substances and the substances and the substancessing advancessing the substancessing to the substance and the substancessing advancessing the substancessing to the substances and the substancessing advancessing the substancessing the substancessing the substancessing advancessing the substancessing the substancessing the substancessing the substances advancessing the substancessing the substance substancessing the substancessing the advancessing the substancessing the substancessing the substancessing the substancessing advancessing the substance substancessing the substances and the substancessing advancessing the substancessing the substancessing the substances and the substances advancessing the substancessing the substances and the substancessing advancessing the substancessing the substances and the substances and the advancessing the substancessing the substances and management subspanses and the substance substancessing the substances and management subspanses and the substance substancessing the substances and the substancessing the substances and the substance substances advancessing the substances and the substances and the substance substancessing the substancessing the substancessing the substances and the substancessing the substances and the substancessing the substancessing advances and the substancessing the substances and the substancessing the substancessing advancessing the substances advancessing the substancessing the substancessing the substancessing advances adva</td><td>Operation Operation Operation Operation Operation Operation Operation</td></t<>	Even consistent and exacts to retention is and network survices they are subtracted to used Matchian is record or access inplate matched to use sub assessing of matched to subtract and and and and and access the sequent to their substance and information subtram where assoliable for advances the sequent tambing to use sub as assoling of the substances in the or advances and advancessing the substances and information subtram where assoliable for advances the sequent tambing to the substance and the substances and advancessing the substances and the substances and the substancessing advancessing the substancessing to the substance and the substancessing advancessing the substancessing to the substances and the substancessing advancessing the substancessing the substancessing the substancessing advancessing the substancessing the substancessing the substancessing the substances advancessing the substancessing the substance substancessing the substancessing the advancessing the substancessing the substancessing the substancessing the substancessing advancessing the substance substancessing the substances and the substancessing advancessing the substancessing the substancessing the substances and the substances advancessing the substancessing the substances and the substancessing advancessing the substancessing the substances and the substances and the advancessing the substancessing the substances and management subspanses and the substance substancessing the substances and management subspanses and the substance substancessing the substances and the substancessing the substances and the substance substances advancessing the substances and the substances and the substance substancessing the substancessing the substancessing the substances and the substancessing the substances and the substancessing the substancessing advances and the substancessing the substances and the substancessing the substancessing advancessing the substances advancessing the substancessing the substancessing the substancessing advances adva	Operation Operation Operation Operation Operation Operation
NGS-3/21 NGS-201 NGS-201 <t< td=""><td>Even solution are access in the stand to even solutions in system and systems and services in the stand to even solutions in second and second systems in a system and second system and second systems in a system and second system and second systems in a system and second system and second systems in a system and second system and second systems and seco</td><td>Operation Operation Operation Operation Operation Operation Operation</td></t<>	Even solution are access in the stand to even solutions in system and systems and services in the stand to even solutions in second and second systems in a system and second system and second systems in a system and second system and second systems in a system and second system and second systems in a system and second system and second systems and seco	Operation Operation Operation Operation Operation Operation
B(25-32) B(25-32) <t< td=""><td>Even consist only have access to retreavis and network survices they ar authorities of used Matchian secored of access pieth garder to access to derawing markets and services General cities correlation in the cities of a services of markets and the cities of a services derivation in the cities of the cities of the cities of the services of access of the cities of the cities of the cities of the services of access of the cities of the cities of the cities of the services and access of the cities of the cities of the cities of the services of the cities of the cities of the cities of the cities of the services of the cities of the cities of the cities of</td><td>Operation Operation Operation Operation Operation Operation Operation</td></t<>	Even consist only have access to retreavis and network survices they ar authorities of used Matchian secored of access pieth garder to access to derawing markets and services General cities correlation in the cities of a services of markets and the cities of a services derivation in the cities of the cities of the cities of the services of access of the cities of the cities of the cities of the services of access of the cities of the cities of the cities of the services and access of the cities of the cities of the cities of the services of the cities of the cities of the cities of the cities of the services of the cities of the cities of the cities of	Operation Operation Operation Operation Operation Operation
B(25-32) B(25-32) <t< td=""><td>Euror only have access to retenois and network survices they ar authoritod used Matina's need of access inplate parted to use survices materials in partenets in the or after a survices General active access inplate parted to uses your assuming and the or after a survices access in the access the survices of the uses your assuming and the or after a survices developed to access the survices of the uses your assuming and the or after a survices access the access the survices of the use of the a survices access the access access the access the survices of the access the access the use of the a survices of the access the access the survices of the access the acces the access the access the access the access the access th</td><td>Operation Operation Operation Operation Operation Operation Operation</td></t<>	Euror only have access to retenois and network survices they ar authoritod used Matina's need of access inplate parted to use survices materials in partenets in the or after a survices General active access inplate parted to uses your assuming and the or after a survices access in the access the survices of the uses your assuming and the or after a survices developed to access the survices of the uses your assuming and the or after a survices access the access the survices of the use of the a survices access the access access the access the survices of the access the access the use of the a survices of the access the access the survices of the access the acces the access the access the access the access the access th	Operation Operation Operation Operation Operation Operation
B(S)-247 R(S)-248 R(S)-248 R(S)-248 R(S)-252 R(S)-252 <t< td=""><td>Euror sonity have access to retenois and network survices they ar authorited to used Matchian are cored access inplate granel to use survices methanis networks methanis and the sonitable Generate allife increment from autications subsure on an illufermation networks where auticable Generate allife increment formal solitable access to access information networks where auticable denoises and access transmission of the source to access information networks where auticable denoises and access transmission of the source to access information networks where auticable and access and access transmission of frequent incident response testing to determine incident response discusses. Calculate and access and access the response testing to determine incident response and access the median construction of response transmission of access and access and incident response proceedances for calculation, cancellation, cancellation, access and access the access and access and access and access and access and access the formation access type access the access and access and access and access the access and access and access and access and access and access and access the access and access anotation access and a</td><td>Operation Operation Operation Incention Operation Incen</td></t<>	Euror sonity have access to retenois and network survices they ar authorited to used Matchian are cored access inplate granel to use survices methanis networks methanis and the sonitable Generate allife increment from autications subsure on an illufermation networks where auticable Generate allife increment formal solitable access to access information networks where auticable denoises and access transmission of the source to access information networks where auticable denoises and access transmission of the source to access information networks where auticable and access and access transmission of frequent incident response testing to determine incident response discusses. Calculate and access and access the response testing to determine incident response and access the median construction of response transmission of access and access and incident response proceedances for calculation, cancellation, cancellation, access and access the access and access and access and access and access and access the formation access type access the access and access and access and access the access and access and access and access and access and access and access the access and access anotation access and a	Operation Operation Operation Incention Operation Incen
B(S)-247 R(S)-248 R(S)-248 R(S)-248 R(S)-252 R(S)-271 R(S)-272 R(S)-273 R(S)-274 R(S)-275 R(S)-275 R(S)-271 R(S)-271 <t< td=""><td>Even solution area of a secure shortware and network survices they are authorized used Maticals area of a secure shortware and a largeritation surviews may services Secure and a sources response training to serve spon sources in the or a set a sources of a secure shortware the source shortware and a largeritation surviews may services and a document results of finguent incident regionse testing to determine incident regionse discurses. The source shortware shortware shortware and a largeritation surviews may shortware and sources the source spon testing to determine incident regionse discurses. The source shortware shortware shortware shortware shortware shortware and sources the source spon testing to determine incident regionse discurses. The source shortware shortware shortware shortware accurses promound shortware and sources the source spon testing to determine incident regions and sources the source spon testing to determine incident regions and sources the source spon testing to determine incident regions and sources the source spon testing to determine incident regions and sources the source spon testing to determine incident regions and sources the source spon testing the sources the sources and analysis and sources and sources the source spon testing the sources the sources and sources and sources and sources the source spon testing the sources the sources and management support for analysis the sources the sources the sources and management support and sources the sources the sources and sources and sources and sources and sources and the sources the sources and sources and sources and sources and sources and sources the sources and sources and sources and sources and sources and the sources the sources and sources an</td><td>Operation Operation Operation Incention Operation Incen</td></t<>	Even solution area of a secure shortware and network survices they are authorized used Maticals area of a secure shortware and a largeritation surviews may services Secure and a sources response training to serve spon sources in the or a set a sources of a secure shortware the source shortware and a largeritation surviews may services and a document results of finguent incident regionse testing to determine incident regionse discurses. The source shortware shortware shortware and a largeritation surviews may shortware and sources the source spon testing to determine incident regionse discurses. The source shortware shortware shortware shortware shortware shortware and sources the source spon testing to determine incident regionse discurses. The source shortware shortware shortware shortware accurses promound shortware and sources the source spon testing to determine incident regions and sources the source spon testing to determine incident regions and sources the source spon testing to determine incident regions and sources the source spon testing to determine incident regions and sources the source spon testing to determine incident regions and sources the source spon testing the sources the sources and analysis and sources and sources the source spon testing the sources the sources and sources and sources and sources the source spon testing the sources the sources and management support for analysis the sources the sources the sources and management support and sources the sources the sources and sources and sources and sources and sources and the sources the sources and sources and sources and sources and sources and sources the sources and sources and sources and sources and sources and the sources the sources and sources an	Operation Operation Operation Incention Operation Incen
B(25-24) B(25-24) B(25-24) B(25-24) B(25-24) B(25-24) B(25-24) B(25-25) B(25-25) B(25-25) B(25-25) B(25-25) B(25-25) B(25-25) B(25-25) B(25-26) B(25-26) B(25-26) B(25-26) B(25-26) B(25-26) B(25-26) B(25-27) B(25-27) <t< td=""><td>Euror soft has accos for streams in an advance stream system and system advances advances advances and system advances a</td><td>Operation Operation Operation Operation Operation Operation Operation</td></t<>	Euror soft has accos for streams in an advance stream system and system advances advances advances and system advances a	Operation Operation Operation Operation Operation Operation
B(S)-247 R(S)-248 R(S)-248 R(S)-248 R(S)-252 R(S)-252 R(S)-252 R(S)-252 R(S)-253 R(S)-254 R(S)-252 R(S)-252 R(S)-253 R(S)-254 R(S)-274 R(S)-274 <t< td=""><td>Euror only have access to retreak and network survices they ar each other works Server and access participation of our sour sour sourcess information systems and servers Server and access retreak and the our sour sour sourcess information systems and servers Server and access retreak and the our sour sour sourcess information systems and servers Server and access retreak and the out sour sour sourcess information systems and servers Server and access retreak and the server sour sourcess information systems and servers Server and access retreak and frequent incident response testing to determine incident response discusses. The advances treak and sources treak and server and the server access retreak and access server and access retreak and sources treak and access retreak and acces retreak and access ret</td><td>Operation Operation Operation Internet Operation Operation Operation Operation</td></t<>	Euror only have access to retreak and network survices they ar each other works Server and access participation of our sour sour sourcess information systems and servers Server and access retreak and the our sour sour sourcess information systems and servers Server and access retreak and the our sour sour sourcess information systems and servers Server and access retreak and the out sour sour sourcess information systems and servers Server and access retreak and the server sour sourcess information systems and servers Server and access retreak and frequent incident response testing to determine incident response discusses. The advances treak and sources treak and server and the server access retreak and access server and access retreak and sources treak and access retreak and acces retreak and access ret	Operation Operation Operation Internet Operation Operation Operation Operation
B(25-32) B(25-32) <t< td=""><td>Even solution are accord or extensions and network sortices they are subtoaled to used Matina is accord or extension to accord information systems and services Service at all or extensions from analizations sobrawer and information subtems where assoluted information information treatmost from the sources to accord information systems where assoluted information information treatmost from the sources to accord information solutions where assoluted information information treatmost from the sources to accord information solutions where assoluted information information information information testing to determine incident reapons discusses and accounter treatmost from frequent incident reapons testing to determine incident reapons discusses and accounter treatmost frequent incident reapons testing to determine incident reapons discusses and accounter treatmost frequent incident reapons testing to determine incident reapons discusses and accounter treatmost frequent incident treapons testing to determine incident reapons discusses and the source capabilities band in treatmost accounte, inmation accounte, inmation accounte, inmation discusses to resport source the account incident treapons capabilities band are accounted in the source to accounter indication treapons capabilities band discusses to resport source the accounter indication discusses and treapons discusses and accounter indication termination indication reapons discusses and accounter indication termination indication reapons discusses and accounter indication indication rea</td><td></td></t<>	Even solution are accord or extensions and network sortices they are subtoaled to used Matina is accord or extension to accord information systems and services Service at all or extensions from analizations sobrawer and information subtems where assoluted information information treatmost from the sources to accord information systems where assoluted information information treatmost from the sources to accord information solutions where assoluted information information treatmost from the sources to accord information solutions where assoluted information information information information testing to determine incident reapons discusses and accounter treatmost from frequent incident reapons testing to determine incident reapons discusses and accounter treatmost frequent incident reapons testing to determine incident reapons discusses and accounter treatmost frequent incident reapons testing to determine incident reapons discusses and accounter treatmost frequent incident treapons testing to determine incident reapons discusses and the source capabilities band in treatmost accounte, inmation accounte, inmation accounte, inmation discusses to resport source the account incident treapons capabilities band are accounted in the source to accounter indication treapons capabilities band discusses to resport source the accounter indication discusses and treapons discusses and accounter indication termination indication reapons discusses and accounter indication termination indication reapons discusses and accounter indication indication rea	
B(25-24) R(25-24) R(25-24) R(25-24) R(25-24) R(25-24) R(25-24) R(25-25) R(25-25) R(25-25) R(25-25) R(25-25) R(25-25) R(25-25) R(25-26) R(25-26) R(25-26) R(25-26) R(25-26) R(25-26) R(25-26) R(25-27) R(25-27) <t< td=""><td> Even solve have access to retreavis and network sorvess they are authorited used Matina's need of access pieths granted to use sour sourcess information systems and servess Serveral active access pieths granted to use sour sourcess information systems and servess Serveral active access pieths granted to use sour sourcess information systems and servess access and access the serveral to use sour sourcess information systems and servers access the access access pieth granted to use sour sourcess information systems and servers access access acces access access access access access access access access acces</td><td>Operations Operations Operations Operations Operations Operations <tdoperations< td=""> Operations</tdoperations<></td></t<>	 Even solve have access to retreavis and network sorvess they are authorited used Matina's need of access pieths granted to use sour sourcess information systems and servess Serveral active access pieths granted to use sour sourcess information systems and servess Serveral active access pieths granted to use sour sourcess information systems and servess access and access the serveral to use sour sourcess information systems and servers access the access access pieth granted to use sour sourcess information systems and servers access access acces access access access access access access access access acces	Operations Operations Operations Operations Operations Operations Operations <tdoperations< td=""> Operations</tdoperations<>
B(S)-247 R(S)-248 R(S)-248 R(S)-248 R(S)-252 R(S)-252 <t< td=""><td>Even solury have access to retenois and network sorties they ar subtooled to used Matchian secored or tensorts failed beaution subtoom system and services Service and accument requires of finguent incident regions testing to determine incident regions determine incident regions failed beautions testing to determine incident regions determine incident regions failed beautions testing to determine incident regions determine incident regions failed beautions testing to determine incident regions determine incident regions failed beautions testing to determine incident regions determine incident regions are not exceeding control of the context set of the determine incident regions are not exceeding control of the context set of the determine incident regions are not exceeding control of the context set of the determine incident regions are not exceeding control of the context set of the determine incident regions are not exceeding incident the area exceeding incident determine incident regions are not exceeding incident the area exceeding incident area exceeding and area exceeding incident the area exceeding incident regions area incident regions pain that detric the structure and arguments area for incident regions are incident regions pain that detric the structure and arguments in part of area incident regions pain that detric the structure and argument sequent for area incident regions pain that detric the structure and argument in argument area in incident regions pain that detric the structure and argument in argument area in incident regions pain that detric the structure and argument is argument area in incident regions pain that detric the structure and argument is argument area in incident regions pain that detric the structure and argument is argument area in incident regions</td><td>Operation Operation Operation Internet Operation Operation Operation Operation</td></t<>	Even solury have access to retenois and network sorties they ar subtooled to used Matchian secored or tensorts failed beaution subtoom system and services Service and accument requires of finguent incident regions testing to determine incident regions determine incident regions failed beautions testing to determine incident regions determine incident regions failed beautions testing to determine incident regions determine incident regions failed beautions testing to determine incident regions determine incident regions failed beautions testing to determine incident regions determine incident regions are not exceeding control of the context set of the determine incident regions are not exceeding control of the context set of the determine incident regions are not exceeding control of the context set of the determine incident regions are not exceeding control of the context set of the determine incident regions are not exceeding incident the area exceeding incident determine incident regions are not exceeding incident the area exceeding incident area exceeding and area exceeding incident the area exceeding incident regions area incident regions pain that detric the structure and arguments area for incident regions are incident regions pain that detric the structure and arguments in part of area incident regions pain that detric the structure and argument sequent for area incident regions pain that detric the structure and argument in argument area in incident regions pain that detric the structure and argument in argument area in incident regions pain that detric the structure and argument is argument area in incident regions pain that detric the structure and argument is argument area in incident regions pain that detric the structure and argument is argument area in incident regions	Operation Operation Operation Internet Operation Operation Operation Operation
BCS-3/21 BCS-3/21 BCS-3/22 BCS-3/22 BCS-3/22 BCS-3/22 BCS-3/22 BCS-3/22 BCS-3/23 BCS-3/22 BCS-3/24 BCS-3/22 BCS-3/24 BCS-3/22 BCS-3/24 BCS-3/24 BCS-3/24 BCS-3/24<	Even solution are acids access in the same of a weak sources information system and services in the same of a weak sources in	Operation Operation Operation Operation Operation Operation Operation Opera
B(S)-247 R(S)-248 R(S)-248 R(S)-248 R(S)-252 R(S)-252 <t< td=""><td> Even solution are access in petraperies or use sous solutions investion and services in the solution is access in a structure of meta-solutions investion and services in a structure of meta-solution is access in a structure of meta-solution is access in a structure of meta-solution is access in a structure of meta-solution is a structu</td><td>Operation Operation Operation Internet Operation Operation Operation Operation</td></t<>	 Even solution are access in petraperies or use sous solutions investion and services in the solution is access in a structure of meta-solutions investion and services in a structure of meta-solution is access in a structure of meta-solution is access in a structure of meta-solution is access in a structure of meta-solution is a structu	Operation Operation Operation Internet Operation Operation Operation Operation
B(25-3/2) B(25-3/2) <td< td=""><td>Even solution area of a security index to a security index in a security index i</td><td>Operation Operation Operation Operation Operation Operation Operation</td></td<>	Even solution area of a security index to a security index in a security index i	Operation Operation Operation Operation Operation Operation
BCS-3/21 BCS-3/21 BCS-3/20 BCS-3/20 BCS-3/21 BCS-3/21 BCS-3/21 BCS-3/22 BCS-3/21 BCS-3/21 <t< td=""><td>Even solution services for exact parts and returns investions system and systems Second solution second solutions systems and systems and systems Second solutions invested and systems and systems and systems and systems Conductions invested solutions systems and systems and systems and systems and systems Conductions invested solutions systems and systems and systems and systems Conductions invested solutions invested solutions systems and systems Conductions invested solutions invested solutions prevales/s, ordications Conductions invested solutions invested solutions invested solutions Conductions invested solutions invested solutions invested solutions Conductions Conductions</td><td>Operations Operations Operations Operations Operations Operations Operations</td></t<>	Even solution services for exact parts and returns investions system and systems Second solution second solutions systems and systems and systems Second solutions invested and systems and systems and systems and systems Conductions invested solutions systems and systems and systems and systems and systems Conductions invested solutions systems and systems and systems and systems Conductions invested solutions invested solutions systems and systems Conductions invested solutions invested solutions prevales/s, ordications Conductions invested solutions invested solutions invested solutions Conductions invested solutions invested solutions invested solutions Conductions	Operations Operations Operations Operations Operations Operations

12.5.1 12.1.2 12.6.1	INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS CHANGE MANAGEMENT MANAGEMENT OF TECHNICAL VULNERABILITIES	CM-4	SECURITY IMPACT ANALYSIS
14.2.2	SYSTEM CHANGE CONTROL PROCEDURES	CM-6	CONFIGURATION SETTINGS
12.5.1 18.1.2	INTELLECTUAL PROPERTY RIGHTS	CM-7 CM-10	LEAST FUNCTIONALITY SOFTWARE USAGE RESTRICTIONS
18.1.2	INTELLECTUAL PROPERTY RIGHTS	CM-10	SOFTWARE USAGE RESTRICTIONS
12.5.1 12.1.3	INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS CAPACITY MANAGEMENT		
17.1.2	CAPACITY MANAGEMENT	CP-2	CONTINGENCY PLAN
17.1.1	PLANNING INFORMATION SECURITY CONTINUITY		
17.1.1	PLANNING INFORMATION SECURITY CONTINUITY		
17.1.2	IMPLEMENTING INFORMATION SECURITY CONTINUITY IMPLEMENTING INFORMATION SECURITY CONTINUITY	CP-2	CONTINGENCY PLAN
17.1.2	IMPLEMENTING INFORMATION SECURITY CONTINUITY	CP-2	CONTINGENCY PLAN
	MONITORING AND REVIEW OF SUPPLIER SERVICES IMPLEMENTING INFORMATION SECURITY CONTINUITY		CONTINGENCY PLAN
17.1.2 16.1.1	RESPONSIBILITIES AND PROCEDURES	CP-2 IR-8	CONTINGENCY PLAN INCIDENT RESPONSE PLAN
17.1.3	VERIFY, REVIEW AND EVALUATE INFORMATION SECURITY CONTINUITY	PL-2 CP-2	SYSTEM SECURITY PLAN CONTINGENCY PLAN
16.1.1	VERIET, REVIEW AND EVALUATE INFORMATION SECURITY CONTINUITY RESPONSIBILITIES AND PROCEDURES	IR-8	INCIDENT RESPONSE PLAN
		PL-2 IR-8	SYSTEM SECURITY PLAN
		CP-2 CP-2	CONTINGENCY PLAN CONTINGENCY PLAN
17.1.3	VERIFY. REVIEW AND EVALUATE INFORMATION SECURITY CONTINUITY	IR-4 (P-2	INCIDENT HANDLING CONTINGENCY PLAN
16.1.6	LEARNING FROM INFORMATION SECURITY INCIDENTS	IR-8	INCIDENT RESPONSE PLAN
		PL-2	SYSTEM SECURITY PLAN
		PL-2 CP-2	SYSTEM SECURITY PLAN CONTINGENCY PLAN
17.2.1		IR-8 CP-6	INCIDENT RESPONSE PLAN ALTERNATE STORAGE SITE
17.2.1	AVAILABILITY OF INFORMATION PROCESSING FACILITIES AVAILABILITY OF INFORMATION PROCESSING FACILITIES	CP-6	ALTERNATE STORAGE SITE
17.2.1		CP-7	ALTERNATE PROCESSING SITE
	AVAILABILITY OF INFORMATION PROCESSING FACILITIES		
17.2.1		CP-7 CP-7	ALTERNATE PROCESSING SITE
	AVAILABILITY OF INFORMATION PROCESSING FACILITIES	CP-8	TELECOMMUNICATIONS SERVICES
17.2.1	AVAILABILITY OF INFORMATION PROCESSING FACILITIES		
12.3.1	INFORMATION BACKUP	CP-9	INFORMATION SYSTEM BACKUP
12.3.1 12.3.1	INFORMATION BACKUP	CP-9 CP-9	INFORMATION SYSTEM BACKUP
12.3.1	INFORMATION BACKUP		
		CP-10	INFORMATION SYSTEM RECOVERY AI
12.6.1		CP-11 CP-12	ALTERNATE COMMUNICATIONS PRO SAFE MODE
	MANAGEMENT OF TECHNICAL VULNERABILITIES	SC-38	OPERATIONS SECURITY
12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES	50-50	or clothold second t
12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES		
17.1.2 9.4.3	IMPLEMENTING INFORMATION SECURITY CONTINUITY PASSWORD MANAGEMENT SYSTEM	CP-13 IA-4	ALTERNATIVE SECURITY MECHANISN IDENTIFIER MANAGEMENT
9.2.4 9.4.3	MANAGEMENT OF SECRET AUTHENTICATION INFORMATION OF USERS PASSWORD MANAGEMENT SYSTEM		
9.3.1 9.3.1	USE OF SECRET AUTHENTICATION INFORMATION USE OF SECRET AUTHENTICATION INFORMATION	IA-5	AUTHENTICATOR MANAGEMENT
9.4.3 9.3.1	PASSWORD MANAGEMENT SYSTEM USE OF SECRET AUTHENTICATION INFORMATION		
14.1.3 13.2.3	PROTECTING APPLICATION SERVICES TRANSACTIONS ELECTRONIC MESSAGING		
13.2.3	ELECTRONIC MESSAGING		
13.2.3	ELECTRONIC MESSAGING		
14.1.3	PROTECTING APPLICATION SERVICES TRANSACTIONS		
14.1.3	PROTECTING APPLICATION SERVICES TRANSACTIONS		
		IA-10	ADAPTIVE IDENTIFICATION AND AUT
9.1.2 9.2.2	ACCESS TO NETWORKS AND NETWORK SERVICES USER ACCESS PROVISIONING		
9.4.4	USE OF PRIVILEGED UTILITY PROGRAMS	IR-2	INCIDENT RESPONSE TRAINING
		IR-3	INCIDENT RESPONSE TESTING
			incident nearonal rearing
16.1.1	RESPONSIBILITIES AND PROCEDURES	IR-4	INCIDENT HANDLING
16.1.1 16.1.1	RESPONSIBILITIES AND PROCEDURES RESPONSIBILITIES AND PROCEDURES		
16.1.1	RESPONSIBILITIES AND PROCEDURES LEARNING FROM INFORMATION SECURITY INCIDENTS	IR-4	
16.1.6	LEARNING FROM INFORMATION SECURITY INCIDENTS LEARNING FROM INFORMATION SECURITY INCIDENTS RESPONSE TO INFORMATION SECURITY INCIDENTS	IR-4	INCIDENT HANDLING
16.1.2	RESPONSE TO INFORMATION SECURITY EVENTS REPORTING INFORMATION SECURITY EVENTS RESPONSIBILITIES AND PROCEDURES	IR-6	INCIDENT REPORTING
16.1.1 16.1.2	REPORTING INFORMATION SECURITY EVENTS	IR-6	INCIDENT REPORTING
16.1.1 16.1.2	RESPONSIBILITIES AND PROCEDURES REPORTING INFORMATION SECURITY EVENTS	IR-7 IR-8	INCIDENT RESPONSE ASSISTANCE
		IR-8	INCIDENT RESPONSE PLAN
		IR-8	INCIDENT RESPONSE PLAN
		IR-8	INCIDENT RESPONSE PLAN
16.1.1	RESPONSIBILITIES AND PROCEDURES		
16.1.4 16.1.5	ASSESSMENT OF AND DECISION ON INFORMATION SECURITY EVENTS RESPONSE TO INFORMATION SECURITY INCIDENTS	IR-8 IR-9	INCIDENT RESPONSE PLAN INFORMATION SPILLAGE RESPONSE
-0.4.3	COLORIDA IN CONSISTENT SECONT INCLUENTS	IR-9	INFORMATION SPILLAGE RESPONSE INFORMATION SPILLAGE RESPONSE
		IR-9	INFORMATION SPILLAGE RESPONSE
16.1.7 16.1.5	COLLECTION OF EVIDENCE RESPONSE TO INFORMATION SECURITY INCIDENTS		
16.1.3	REPORTING INFORMATION SECURITY WEAKNESSES		
		IR-10	INTEGRATED INFORMATION SECURIT
11.2.4	EQUIPMENT MAINTENANCE	MA-2	CONTROLLED MAINTENANCE
11.2.4	EQUIPMENT MAINTENANCE	MA-2	CONTROLLED MAINTENANCE
11.2.5	REMOVAL OF ASSETS	MA-2	CONTROLLED MAINTENANCE
11.2.4	EQUIPMENT MAINTENANCE	MA-2	CONTROLLED MAINTENANCE
11.2.4	EQUIPMENT MAINTENANCE	MA-2	CONTROLLED MAINTENANCE
11.2.4	EQUIPMENT MAINTENANCE	MA-2 MA-4	CONTROLLED MAINTENANCE NONLOCAL MAINTENANCE
		MA-4	NONLOCAL MAINTENANCE
		MA-4	NONLOCAL MAINTENANCE
11.2.5	REMOVAL OF ASSETS	MA-4	
		MA-6	NONLOCAL MAINTENANCE TIMELY MAINTENANCE
	MANAGEMENT OF REMOVABLE MEDIA	MP-2	MEDIA ACCESS
8.3.1		MP-3	MEDIA MARKING
8.3.1		MP-3	MEDIA MARKING
8.3.3	PHYSICAL MEDIA TRANSFER PHYSICAL MEDIA TRANSFER	MP-5	MEDIA MARKING MEDIA TRANSPORT MEDIA TRANSPORT
	PHYSICAL MEDIA TRANSFER PHYSICAL MEDIA TRANSFER		MEDIA TRANSPORT MEDIA TRANSPORT MEDIA TRANSPORT
8.3.3 8.3.3 8.3.3	PHYSICAL MEDIA TRANSFER	MP-5 MP-5 MP-5 MP-5 MP-6	MEDIA TRANSPORT MEDIA TRANSPORT MEDIA TRANSPORT MEDIA TRANSPORT MEDIA SANITIZATION
8.3.3 8.3.3 8.3.3 8.3.3	PHYSICAL MEDIA TRANSFER PHYSICAL MEDIA TRANSFER PHYSICAL MEDIA TRANSFER	MP-5 MP-5 MP-5 MP-5	MEDIA TRANSPORT MEDIA TRANSPORT MEDIA TRANSPORT MEDIA TRANSPORT
8.3.3 8.3.3 8.3.3 8.3.3 8.3.3 8.3.2	PHYSICAL MEDIA TRANSFER PHYSICAL MEDIA TRANSFER PHYSICAL MEDIA TRANSFER DISPOSAL OF MEDIA	MP-S MP-S MP-S MP-6 MP-7 MP-8	MEDIA TRANSPORT MEDIA TRANSPORT MEDIA TRANSPORT MEDIA TRANSPORT MEDIA SANITIZATION MEDIA USE MEDIA DOWNGRADING
8.3.3 8.3.3 8.3.3 8.3.3 8.3.3 8.3.2 8.3.1	PHYSICLA MEDIA TRANSFER PHYSICLA MEDIA TRANSFER PHYSICLA MEDIA TRANSFER DIGROSAL OF MEDIA MANAGEMENT OF REMOVABLE MEDIA	MP-5 MP-5 MP-5 MP-5 MP-6 MP-7 MP-8	MEDIA TRANSPORT MEDIA TRANSPORT MEDIA TRANSPORT MEDIA TRANSPORT MEDIA SANITIZATION MEDIA JOWINGRADING MEDIA DOWINGRADING MONITORING PHYSICAL ACCESS
8.3.3 8.3.3 8.3.3 8.3.2 8.3.1 8.3.1	PRISCIAL MEDIA TRANSFER PRISCIAL MEDIA TRANSFER DISPOSI OL MEDIA REDIA MEDIA MANAGEMENT OF REMOVABLE MEDIA MANAGEMENT OF REMOVABLE MEDIA	MP-5 MP-5 MP-5 MP-5 MP-6 MP-7 MP-8 PE-6 PE-17	MEDIA TRANSPORT MEDIA TRANSPORT MEDIA TRANSPORT MEDIA TRANSPORT MEDIA SANITIZATION MEDIA LOUWINGRADING MONITORING PHYSICAL ACCESS ALTERNATE WORK SITE
8.3.3 8.3.3 8.3.3 8.3.3 8.3.3 8.3.2 8.3.1	PHYSICLA MEDIA TRANSFER PHYSICLA MEDIA TRANSFER PHYSICLA MEDIA TRANSFER DIGROSAL OF MEDIA MANAGEMENT OF REMOVABLE MEDIA	MP-5 MP-5 MP-5 MP-5 MP-6 MP-7 MP-8 PE-6 PE-17 PE-18	MEDIA TRANSPORT MEDIA TRANSPORT MEDIA TRANSPORT MEDIA TRANSPORT MEDIA SANITIZATION MEDIA JOWNGRADING MONTORING PHYSICAL ACCESS ALTERNATE WORK SITE LOCATION OF INFORMATION SYSTEM
8.3.3 8.3.3 8.3.3 8.3.2 8.3.1 8.3.1	PRISCIAL MEDIA TRANSFER PRISCIAL MEDIA TRANSFER DISPOSI OL MEDIA REDIA MEDIA MANAGEMENT OF REMOVABLE MEDIA MANAGEMENT OF REMOVABLE MEDIA	MP-5 MP-5 MP-5 MP-5 MP-6 MP-7 MP-8 PE-6 PE-17	MEDIA TRANSPORT MEDIA TRANSPORT MEDIA TRANSPORT MEDIA TRANSPORT MEDIA SANITIZATION MEDIA LOUWINGRADING MONITORING PHYSICAL ACCESS ALTERNATE WORK SITE

PLAN AN AN PLAN SITE SITE ING SITE ING SITE ING SITE M BACKUP M BACKUP M BACKUP RECOVERY AND RECONSTITUTION ICATIONS PROTOCOLS Y MECHANISMS IENT AGEMENT TION AND AUTHENTICATION TRAINING TESTING NG ASSISTANCE PLAN PLAN LAN LAN PLAN AGE RESPONSE AGE RESPONSE AGE RESPONSE

MATION SECURITY ANALYSIS TEAM TENANCE TENANCE TENANCE TENANCE TENANCE NANCE NANCE KE L ACCESS ATION SYSTEM COMPONENTS ND TRACKING

JNCSF-302 JNCSF-303	Advise users to terminate or lock information system settings when systems are unattended Establish a clear desk and clear screen policy to protect any sensitive information	Operation Operation
JNCSF-304	Ensure media and equipment taken off-site has appropriate protections commiserate with sensitivity levels	Operation
JNCSF-305	Maintain a log of all media and equipment taken off-site, including responsible parties for its care and protection	Operation
JNCSF-306	Develop, review, and update a security Concept of Operations (CONOPS) for information systems, as appropriate	Operation
JNCSF-307 JNCSF-308	Scan for vulnerabilities in information systems and hosted applications Automate the vulnerability management process by using vulnerability scanning tools that have standards	Operation Operation
JNCSF-309	for enumerating platforms, formatting checklists, and measuring vulnerability impact Analyze vulnerability scan reports and results from security control assessments	Operation
JNCSF-310 JNCSF-311	Remediate vulnerabilities in accordance with a risk assessment Share information from vulnerability scanning processes with appropriate personnel to prevent future	Operation Operation
JNCSF-312	similar vulnerabilities Create a timeline for remediating vulnerabilities after receiving notice of such vulnerabilities	Operation
JNCSF-313 JNCSF-314	Establish roles and responsibilities associated with technical vulnerability management Establish a procedure for what actions to carry out when there is no suitable countermeasure to a	Operation Operation
JNCSF-315	vulnerabilitv Employ technical surveillance countermeasures to detect the presence of malicious or unintended	Operation
INCSE-316	surveillance activity Determine information security requirements for information systems as part of business process planning	Operation
JNCSF-317	Determine, document and allocate necessary resources to protect information services	Operation
JNCSF-318 JNCSF-319	Establish and utilize secure repositories for storing development code Establish administrator documentation that describes effective use and maintenance of security functions	Operation Operation
JNCSF-320	and mechanisms Establish administrator documentation that describes known information system vulnerabilities	Operation
JNCSF-321	Establish user documentation that describes user responsibilities and methods for maintaining the security of information systems	Operation
JNCSF-322	Protect and distribute administrator and user information system documentation to appropriate personnel	Operation
JNCSF-323	Monitor third-parties to ensure compliance with organizational information security requirements and controls	Operation
JNCSF-324 INCSF-325	Document, manage, and control the integrity of changes to configuration items	Operation Operation
JNCSF-326	Track security flaws and flaw resolution of information systems and report findings to appropriate personnel Change business continuity plans appropriately after making operating platform changes	Operation
JNCSF-327 JNCSF-328	Log the copying and use of operational information for testing	Operation Operation
JNCSF-328 JNCSF-329	Employ security safeguards to protect against third-party supply chain threats to information systems Ensure that third parties follow organizational security requirements throughout the supply chain if they	Operation
	involve other suppliers Monitor information system components throughout the supply chain to ensure there are no unauthorized	
JNCSF-330 JNCSF-331	or unwanted modifications Identify and document the types of third parties allowed access to the organization's information	Operation Operation
JNCSF-332	Define, monitor, and control the types of information access that third parties will be allowed	Operation
INCSE-333	Establish procedures for monitoring third parties' adherence to information security requirements and	
	Establish accuracy and completeness controls to ensure the integrity of provided information to/from third	Operation
JNCSF-334	Establish accuracy and completeness controls to ensure the integrity or provided information to/rrom third parties Establish resilience, recovery and contingency arrangements to ensure the availability of third party and	Operation
34031-333	Establish resulence, recovery and contingency arrangements to ensure the availability of third party and organizational information Require third parties to deliver periodic independent reports on controls' effectiveness and establish an	Operation
JNCSF-336 JNCSF-337	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. Review third-party audit trails of information security events, operational problems, and failures	Operation Operation
JNCSF-337 JNCSF-338 JNCSF-339	Review third-party audit traits of information security events, operational problems, and failures Require the use of development processes that explicitly address security requirements Require evidence from outsourced developers of accentable levels of privacy and security quality	Operation Operation
JNCSF-339 JNCSF-340	Require evidence from outsourced developers of acceptable levels of privacy and security quality Require evidence from outsourced developers of sufficient testing to guard against malicious content and/or vulnerabilities	Operation
JNCSF-341	and/or vulnerabilities Implement a tamper protection program for all information systems as appropriate Develop and implement anti-counterfeit procedures to prevent counterfeit components from entering	Operation
JNCSF-342	Develop and implement anti-counterfeit procedures to prevent counterfeit components from entering information systems Report counterfeit information system components to the counterfeit source and appropriate	Operation
JNCSF-343 JNCSF-344	Report counterreit information system components to the counterreit source and appropriate organizational personnel Re-implement or custom develop critical information system components that cannot be trusted	Operation Operation
JNCSF-345	Replace information system components no longer supported by developers	Operation
JNCSF-346	Configure information systems to separate user functionality from information system management functionality (e.e., usine different computers or network addresses for each functionality)	Operation
JNCSF-347	Configure information systems to isolate security functions from nonsecurity functions via partitions and domains Configure information systems to prevent unauthorized and unintended information transfer via shared	Operation
JNCSF-348 JNCSF-349	system resources	Operation Operation
JNCSF-349 JNCSF-350	Configure information systems to employ safeguards to protect against denial of service attacks Configure information systems to protect the availability of resources using quotas (e.g., priority protection)	Operation
JNCSF-351	Configure information systems to implement subnetworks for publicly accessible system components that	Operation
JNCSF-352	are separated from internal networks Ensure that individual network domains have defined boundaries with appropriate gateway communication	Operation
JNCSF-353	protection Ensure network segregation assessments are in accordance with access control policies	Operation
JNCSF-354	Configure information systems to protect the confidentiality and integrity of transmitted information	Operation
JNCSF-355	Establish procedures for protecting communicated sensitive electronic information in the form of an	Operation
JNCSF-356 JNCSF-357	attachment Establish retention and disposal guidelines for all business correspondence, including messages	Operation
JNCSF-357 JNCSF-358	Discourage users from leaving messages containing confidential information on answering machines Configure information systems to terminate network connections after a session or after a period of	Operation Operation
JNCSF-359	inactivity Configure information systems to establish trusted communication paths between users and defined	Operation
JNCSF-360	security functions, such as authentication prompts Establish a cryptographic key management policy that generates keys for cryptography within information	Operation
JNCSF-361	systems Establish a cryptographic key management policy that issues and obtains public key certificates for	Operation
JNCSF-362	cryptography Establish a cryptographic key management policy that distributes keys with instructions of how keys should	Operation
JNCSF-363	be activated Establish an approach to store cryptographic keys within information systems	Operation
JNCSF-364 JNCSF-365	Establish an approach to access cryptographic keys Establish procedures for revoking or destroying cryptographic keys when necessary (i.e., when a key is	Operation Operation
JNCSF-366	compromised Establish procedures for backing up or archiving cryptographic keys	Operation
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
JNCSF-368	Configure information systems to prohibit remote activation of collaborative computing devices unless explicitly noted otherwise	Operation
JNCSF-369	Configure information systems to associate security attributes with information contained in organizational information systems	Operation
JNCSF-370 JNCSF-371	Define acceptable and unacceptable mobile code and mobile code technologies Establish usage restrictions and imolementation guidance for mobile code and mobile code technologies	Operation Operation
JNCSF-372	Authorize. monitor. and control the use of mobile code within the information system Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP)	Operation Operation
JNCSF-374	technologies based on their potential damage to information systems if used maliciously Configure information systems to provide additional data origin authentication and integrity verification	
JNCSF-374 JNCSF-375	artifacts, as appropriate Configure information systems to be able to indicate the security status of child zones to enable verification	Operation
JNCSF-375 JNCSF-376	of a chain of trust among parent and child domains Configure information systems to request and perform data origin authentication and data integrity	Operation
JNCSF-376	verification on the resoonses the system receives from authoritative sources Ensure information systems that provide address resolution services are fault tolerant and implement	Operation
JNCSF-377 JNCSF-378	internal/external role separation Configure information systems to protect the authenticity of communication sessions	Operation Operation
JNCSF-379	Configure information systems to fail to a known state in the event of a system failure to preserve information	Operation
JNCSF-380	Include information system components to attract malicious attacks to detect, deflect, and analyze attacks (i.e., honeypots)	Operation
JNCSF-381 JNCSF-382	Configure information systems to include platform-independent applications as appropriate Configure information systems to protect the confidentiality and integrity of information at rest	Operation Operation
JNCSF-383	Employ a diverse set of information technologies for information system components to reduce the impact of technology-specific vulnerabilities	Operation
JNCSF-384	Employ concealment and misdirection techniques for information systems to confuse and mislead adversaries	Operation
JNCSF-385	Perform a covert channel analysis of information system communications to identify potential avenues for covert channels	Operation
JNCSF-386 JNCSF-387	Estimate the maximum bandwidth of potential covert channels Partition information systems into components residing in separate environments or physical domains	Operation Operation
JNCSF-388	Configure information systems into components resource in separate environments or private domains Configure information systems to load and execute the operating environment from hardware-enforced, read-only media	Operation
JNCSF-389	Configure information systems to load and execute applications from hardware-enforced, read-only media as appropriate	Operation
JNCSF-389 JNCSF-390	Configure information systems to load and execute applications from hardware-enforced, read-only media	Operation Operation
JNCSF-390 JNCSF-391	Configure information systems to load and execute applications from hardware-enforced, read-only media as appropriate Configure information systems to include components that proactively seek to identify malicious activity	
JNCSF-390 JNCSF-391 JNCSF-392	Configure information systems to load and execute applications from hardware enforced, read-only media as agroroprise configure information systems to include components that proactively seek to identify malicious activity (a, b, noner(int)) implement controls that prevent or detect the use of innovan or suspected malicious websites (e.g., backisting) implement controls that arevent or detect the use of innovantorized offware on information systems conduct regular reviews of dowlarser and also content supporting orthogo labories processes and investgate conduct regular reviews of dowlarser and also content supporting orthogo labories processes and investgate conduct regular reviews of dowlarser and the content supporting orthogo labories processes and investgate conduct regular reviews of dowlarser and the content supporting orthogo labories processes and investgate content sets and sets the content sets and processes and investgate content sets and processes and investgate content sets and content sets and processes and content sets and content	Operation Operation Operation
JNCSF-390 JNCSF-391	Configure information systems to load and execute applications from hardware enforced, read-only media as appropriate an appropriate information systems to include components that proactively seek to identify malicious activity (e.g., homeylicins) implement controls that prevent or detect the use of known or suspected malicious websites (e.g., backtisting)	Operation Operation
JNCSF-390 JNCSF-391 JNCSF-392 JNCSF-393	Configure information systems to load and execute applications from hardware enforced, read-only media appropriate appropriate information systems to include components that praactively seek to identify malicious activity (Le, honerqicular), applement controls that prevent or detect the use of incomo or suspected malicous websites (e.g., bandmark controls that prevent or detect the use of incomo or suspected malicous vebsites (e.g., control that the original that the original that the original to application systems and into activity conductingular relevants and data content supporting original business processes and investigate usaparoved or unantiformed amendments.	Operation Operation Operation Operation
JNCSF-390 JNCSF-391 JNCSF-392 JNCSF-393 JNCSF-394	Configure information systems to load and execute applications from hardware enforced, read-only media a sporopriate configure information systems to include components that practively seek to identify malicous activity (Le, heneryclett) implement controls that prevent of detect the use of incomo or suspected malicous websites (e.g., backiniting) incluences controls that correct or detect the use of incomo or suspected malicous websites (e.g., backiniting) incluences controls that correct or detect the use of incomo or suspected malicous websites (e.g., backiniting) incluences controls that correct or detect the use of incomo or suspected malicous websites (e.g., backiniting) incluences and the control of the correct or approximation scatter install and regularly update malware detection and rearis of hware to scan computers and media Scan files received over networks, detection in all downloads, and web gaes for malware implement procedures to regularly colicit templator to regularly colicit templators to received over networks updated for the source is updated for the source i	Operation Operation Operation Operation
JNCSF-390 JNCSF-391 JNCSF-392 JNCSF-393 JNCSF-394 JNCSF-395	Configure information systems to load and execute applications from hardware enforced, read-only media appropriate Configure information systems to include components that proactively see to identify anilosos activity implement controls that prevent or detect the use of honors or suggested maticisus websites (e.g., blocktima) information of systems and data content suggested and blocks and investigate reviews of systems and data content suggesting obtaic blocks processes and investigate calcular aid reading blocks and evaluations and applications to the calcular and reading blocks and evaluations and evaluations calcular and reading blocks and evaluations calcular and calcular calculations and evaluations calcular and calcular calculations and evaluations calcular and calcular calculations and evaluations calculated and reading calculated to regularized and reading and executive target details and evaluations calculated and reading calculated the and reading calculated and reagonabilities for detailing with makkers presentions and reading from makkers and the procedures and executivity in the details and the and the procedures and the respectivity for the details with analysis protections and recovering from makkers and the procedures and the respectivity for the details and the analysis of the procedures and the respectivity for the details and the analysis of the procedures and the respectivity for the details and and the procedures and the respectivity for the details and the analysis of the procedures and the second s	Operation Operation Operation Operation Operation
JNCSF-390 JNCSF-391 JNCSF-392 JNCSF-393 JNCSF-394 JNCSF-395 JNCSF-396	Configure information systems to load and execute applications from hardware enforced, read-only media appropriate configure information systems to include components that proactively seek to definity malicious schrifty (a, honorelicious), and the system of a detect the use of insum or suspected malicious websites (e.g., indications), and the approximation of the systems of the systems of the systems of the systems of the system and the content systems of the systems and intro- tagement of the systems of order were and data content systems of these on information systems and investing analysismed contents in the requiring variable and the systems of the systems of the systems of the system and the systems of the system and the systems of the systems of the system and the systems of the systems of the system and the system of the system and the system of the sys	Operation Operation Operation Operation Operation Operation
JNCSF-390 JNCSF-391 JNCSF-392 JNCSF-393 JNCSF-394 JNCSF-395 JNCSF-396 JNCSF-397 JNCSF-398 JNCSF-399	Configure information systems to lock and execute applications from hardware enforced, read-only media appropriate configure information systems to include components that practicely seek to dentify mailclose schrifty applications and the systems of include components that practicely seek to dentify mailclose schrifty applications and the systems of include components that practicely seek to dentify mailclose schrift backlinds include the system of include components and entry of the system of information systems Conduct regular reviews of schware and data content supporting ortacia basines and investigate applications and regular to determine setection and regain orthware to schematic the system information or methods, determine stretching and regain orthware to schemating the source is qualified and regularity collect information about new malware, ensuing the source is qualified and regularity collect information basin and web pages for malware details. Use technical volume/ability management to reduce winterabilities that could be exploited by malware technical volume/ability management to reduce winterabilities that could be exploited by malware project and - Basing Amathematical Amathematical and and and application and encounterability malkanes of advections and reduced by malware project and - Basing Amathematica and encounterabilities that could be exploited by malware project and - Basing Amathematical Revision of the empirical or individuals	Operation Operation Operation Operation Operation Operation Operation Operation
INCSF-390 INCSF-391 INCSF-392 INCSF-393 INCSF-395 INCSF-397 INCSF-397 INCSF-398 INCSF-399 INCSF-399	Configure information systems to load and execute applications from hardware enforced, read-only media appropriate Configure information systems to include components that prasstrively seek to defaulty malicious sativity lab. Instructional to appropriate the systems of include components that prasstrively seek to defaulty and labora structure and the systems of advance and detain to use of unachino use websites (e.g., management of unachino systems to include components that prasstrively approved or unachino structure of advance to use of unachino uses conduct regularity useds malaware detection and regain software to scan computers and media. San files received one networks, electrician and denain davances, and websites (e.g., and regularity useds malaware detections and regain software to scan computers and media. San files received one networks, electrician and denain davances, and regularity useds malaware detections about new malware, ensuring the source is qualified and regularity and regularity conclusions to regularity collect information about new malware, ensuring the source is qualified and regularity and regularity collect malaware protection and recovering from malware tasks. Use technical vulnerability management to reduce vulnerabilities that could be exploited by malware famplay out-of-aband channels for the physical or electronic transmission of information to individual. Configure information systems to protect external and informal wireless links from isgal parameter attasks.	Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation
INCSF-390 INCSF-391 INCSF-392 INCSF-393 INCSF-394 INCSF-396 INCSF-396 INCSF-397 INCSF-398 INCSF-399 INCSF-400 INCSF-401	Configure information systems to load and execute applications from hardware enforced, read-only media appropriate Configure information systems to include components that practicely seek to identify malicious sativity inglement controls that prevent or detect the use of innoun or suspected malicious websites (e.g., load) and that are enter of setter to use of innoun or suspected malicious websites (e.g., load) and that are enter of setter to use of innoun or suspected malicious websites (e.g., load). The regularity cadate malware and data content supporting ortical business processes and investigate usagemore or unaxisted anometers load and regularity cadate malware detection and reas's offware to scan computers and media. Sea files received owner entersks, electronic and denoisad, and wages for malware. Insplanted pracedices to regularity callect information about new malware, ensuring the source is qualified and regularity and regularity callect malware protection and reasi velocities and reasi velocities and regularity and regularity callect information about new malware, ensuring the source is qualified and regularity callect and regularity callect information about new malware, ensuring the source is qualified and regularity callect and interval with real data interval with real with the source is equilified and regularity callect and regularity callect information about new malware, ensuring the source is equilified and regularity callect and regularity callect and regularity callect and regularity callect and regularity to produce there and an interval with reviewed less from signal parameter rataska Physically dashe or remove connection ports or input/output devices on information systems X5 APARORANT	Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation
INCSF-390 INCSF-391 INCSF-392 INCSF-393 INCSF-395 INCSF-397 INCSF-397 INCSF-398 INCSF-399 INCSF-399	Configure information systems to load and execute applications from hardware enforced, read-only media appropriate Configure information systems to include components that practicely seek to learning applicants controls that prevent or detect the use of honor or suggested malcicus setting mellionement controls that arrevent or detect the use of honor or suggested malcicus setting to the systems of software and data content suggesting of total business processes and investigate and the systems of software and data content suggesting of total business processes and investigate and that and requirely used malware detections and reads of the systems total and requirely used that makes the section and reads of the systems and that and requirely used that markes and that content suggesting and that and requirely used malware detections and reads of the systems total and requirely used that were the section and reads of the systems and the responsibilities for dealing with malware protections and recovering from malware attack. Use tachnical used independent for the sphysical or electronic transmission of information patients attack. Configure information anytems for protect esternal and information to individual Configure information systems to protect esternal and information in first and sphysical APAVQDATL Complexes in discussions of public the resolute activation of environmental sensing capabilities attacks.	Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation
INCSF-390 INCSF-391 INCSF-392 INCSF-393 INCSF-395 INCSF-396 INCSF-396 INCSF-397 INCSF-398 INCSF-400 INCSF-401 INCSF-402	Configure information systems to lock and execute applications from hardware enforced, read-only media configure information systems to include components that practicely seek to definity mailcous schrifty configure information systems to include components that practicely seek to definity mailcous schrifty polymenia controls. Beginnens controls that arrevent or detect the use of hoxen or suspected mailcous websites (e.g., backlind) information systems to include components that are used to a subscription of tradial business processes and investigate conduct regularity data makers detection and expain framework and web pages for mailware information of england to a subscription of tradial business of the second regularity of the second scheme scheme scheme scheme scheme scheme scheme and and regularity data makers detection and versite scheme to the scheme scheme scheme information of the scheme scheme scheme scheme scheme scheme scheme and and regularity data makers extension and scheme to scheme scheme scheme and regularity data makers for devination with makers protection and recovering fram makers and and and and and scheme scheme scheme scheme scheme scheme scheme and scheme scheme scheme scheme scheme scheme scheme scheme scheme polyco and -band scheme scheme scheme scheme scheme scheme scheme polycol scheme sch	Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation
INCSF-390 INCSF-391 INCSF-392 INCSF-393 INCSF-395 INCSF-395 INCSF-397 INCSF-398 INCSF-400 INCSF-401 INCSF-403 INCSF-403 INCSF-404 INCSF-405	Configure information systems to lockal and execute applications from hardware enforced, read-only media appropriate configure information systems to include components that practicely seek to detailly mailcloss schrifty application of the systems of include components that practicely seek to detail y mailcloss schrifty backing information systems of include components that practicely seek to detail y applications and the systems of include components that and comport engular reviews of software and data content supporting ortical basines and investigate analyzers of unavailable and the systems and data content supporting ortical basines and investigate analyzers of unavailable and the systems of the system of the systems of the system comported or unavailable and the systems of the system of the system comported or unavailable and the systems of the system of the system comported or unavailable and the system of the system of the system comported or unavailable to the system of the system of the system comported or unavailable of detains with malware protection and receiving from malware complex out of share darkens for the system of exections that could be exploited by malware tracks. Use technical volume/ability management to reduce universities that could be exploited by malware complex out of share darkens for the system of exections and information to information systems to Approx/ability data malware to protect external and information to information systems Approx/ability configure information systems to protect external and neuron of environmental ensuing capabilities unless an exection in noted configure information systems to protect external and ensure to information systems to configure information systems to protect external and ensure use to information systems Approx/ability unless an exection in noted Configure information systems to protect external and ensure use to information systems to protect and ensure to information systems to protect external and ensure use information systems to prote	Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation
INCSF-391 INCSF-391 INCSF-392 INCSF-393 INCSF-395 INCSF-396 INCSF-397 INCSF-399 INCSF-400 INCSF-401 INCSF-402 INCSF-402 INCSF-403 INCSF-404 INCSF-405 INCSF-405 INCSF-406	Configure information systems to look and execute applications from hardware enforced, read-only media appropriate Configure information systems to include components that practicely seek to deterily mailcloss stativity and the information systems to include components that practicely seek to deterily mailcloss stativity application of the information systems and effect content supporting orthal business on information systems configure information amendment conduct regularity colour methods, effection and regular dothware to information systems and and regularity colour methods, effection and regular dothware to sinformation and conduct regularity colour methods, effection and regular dothware to sinformation conduct regularity colour methods, effection and regular dothware to sinformation conduct regularity colour methods, effection and regular dothware to sinformation and enterpolation contendors, effection and regular dothware to sinformation to an enterpolation conduct regularity colour methods, effection and regularity applications about new makeure, ensuing the source is qualified and regularity conduction values about to regularity collect information about new makeure, ensuing the source is qualified and regularity conduction and responsibilities for dealing with makeure protection and recovering from makeure integring cond-thand hardware by the thyricity of externation and termotic to transformation collection is systems to protect external and integring to indicate Configure information systems to protect external and enternois transming capabilities unless an excertain is noted Configure information systems to protect external and information to indicate collection and emplementation guidence for information system size collections capability distribution systems to protect external and information to indicate solutions configure information systems to protect external and information to indicate collegate information systems to protect external and enternois transming capabilities includent and ent	Operation Operation
INCSF-390 INCSF-391 INCSF-392 INCSF-393 INCSF-395 INCSF-395 INCSF-397 INCSF-398 INCSF-400 INCSF-401 INCSF-403 INCSF-403 INCSF-404 INCSF-405	Configure information systems to load and execute applications from hardware enforced, read-only media a suprovints. Configure information systems to include components that practicely seek to definitly mailclose schilty provide the systems of software and seek to a system of the system of the system configure information systems to include components that practicely seek to definite and include the system of software and definite and systems of the system of the systems controls that prevent or detect the use of human or suggested mailclose schilters conduct regular revises of software and de content systems of the systems of the content systems of software and de content systems of the system of the content system of software and de content systems of the system of the content systems of software and de content systems of the system of the content system of the system of and reas of where to a concomption and mail content systems to regularize (software in the system) of the system of the content systems of the application of software systems of the content systems to regularize (software protection and recovering from mailers attack. Configure information systems to protect estemal and indexicon of information systems (Software Configure information systems to protect estemal and indexicon of information systems (Software Configure information systems to protect estemal and indexicon of information systems (Software Configure information systems to protect estemal and indexicon of information systems (Software Configure information systems to provide an explicit indication of sensor use to defined classes) of use and applications and information systems content and indication of sensor use to defined classes of uses attaches an executive systems in topolication of information systems (Software indication of sensor use to define classes) of use attaches an executive indication of sensor use to define classes of uses attaches and executive and information systems components.	Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation Operation
INCSF-393 INCSF-393 INCSF-393 INCSF-393 INCSF-395 INCSF-395 INCSF-395 INCSF-400 INCSF-401 INCSF-403 INCSF-405 INCSF-405 INCSF-405 INCSF-405 INCSF-405 INCSF-405	Configure information systems to load and execute applications from hardware enforced, read-only media a suprovint. Configure information systems to include components that practicely seek to defind mailcose schitty programme controls that prevent or detect the use of honor or suppected malicious schitty programme controls that prevent or detect the use of honor or suppected malicious schitty programme controls that prevent or detect the use of honor or suppected malicious schitty and that and equilable and examples of the second schitter and programme controls and investigation conduct regular reviews of schitters and detections and reaction scheme. Conduct regular reviews of schitters and detections and reaction scheme. Conduct regular reviews of schitters and detections and reaction scheme. Conduct regular reviews of schitters and detections and reaction scheme. Conduct regular reviews of schitters and detections and reaction scheme. Conduct regular reviews of schitters and detections and reaction schemes. Schitters and schitters and schitters and reactions and reactions and reactions and schitters. Use technical without the regularization of schitters and reactions for maintaines. Schitters and executions for the physical or detections that could be exploited by malarer attack. Configure information systems to provide a schitters in the formed in schitters and and and and and and and and and and and	Operation Operation
INCSF-390 INCSF-391 INCSF-392 INCSF-393 INCSF-396 INCSF-396 INCSF-400 INCSF-401 INCSF-401 INCSF-402 INCSF-403 INCSF-404 INCSF-405 INCSF-406 INCSF-406 INCSF-407 INCSF-408	Configure information systems to lock and execute applications from hardware enforced, read-only media appropriate Configure information systems to include components that practicely seek to defind mailcose schedy applications controls that arrevent or detect the use of hown or suppected mailcoses websites (e.g., Backing) Information and the application of the application of the applications of the configure information systems and additional on a stage of the applications of the configure information of the application of the application of the applications of the configure information of the application of the applications of the configure information of the application of the applications of the configure information of the application of the application of the applications of the configure information of the application of the application of the application of the configure information of the application of the application of the application of the provide of band channels for the application electronic transmission of alternative to individual Configure information systems to provide a respective information systems attack. Configure information systems to provide a respective information on the application of the physical dealers of the application electronic transmission of alternative information configure information systems to provide an explicit heration of the application of the physical dealers of and controls in a physical information systems and controls attack and and application of the application of sectors of the application of the physical dealers of controls and application of the application of sectors of the application applications and applications applications applications applications applications attack and applications and applications applications applications. For formation systems to information systems components and the applications attack and applications applications applications applications. For formation applications to physications applications applications applications. F	Operation Operation
INCSF-390 INCSF-391 INCSF-392 INCSF-393 INCSF-395 INCSF-395 INCSF-397 INCSF-400 INCSF-400 INCSF-401 INCSF-405 INCSF-	Configure information systems to lock and execute applications from hardware enforced, read-only media appropriate Configure information systems to include components that practicely seek to defaulty mailclose starting La, hardreflorting La, hardreflorting Hard	Operation Operation

11.2.8 11.2.9			
	UNATTENDED USER EQUIPMENT CLEAR DESK AND CLEAR SCREEN POLICY		
11.2.6	SECURITY OF EQUIPMENT AND ASSETS OFF-PREMISES		
11.2.6	SECURITY OF EQUIPMENT AND ASSETS OFF-PREMISES		
		PL-7	SECURITY CONCEPT OF OPERATIONS
12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES	RA-5 RA-5	VULNERABILITY SCANNING VULNERABILITY SCANNING
		RA-5	VULNERABILITY SCANNING VULNERABILITY SCANNING
12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES	RA-5 RA-5	VULNERABILITY SCANNING VULNERABILITY SCANNING
12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES	RA-5 RA-5	VULNERABILITY SCANNING VULNERABILITY SCANNING
12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES	101.5	VOLNERABLETT SCANNING
12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES		
		RA-6	TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY
14.1.1	INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION	SA-2	ALLOCATION OF RESOURCES
14.1.1 14.2.1	INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION SECURE DEVELOPMENT POLICY	SA-2	ALLOCATION OF RESOURCES
		SA-5	INFORMATION SYSTEM DOCUMENTATION
		SA-5 SA-5	INFORMATION SYSTEM DOCUMENTATION
14.2.6	SECURE DEVELOPMENT ENVIRONMENT	SA-5	INFORMATION SYSTEM DOCUMENTATION
15.1.2 14.2.2	ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS SYSTEM CHANGE CONTROL PROCEDURES	SA-9 SA-10	EXTERNAL INFORMATION SYSTEM SERVICES DEVELOPER CONFIGURATION MANAGEMENT
14.2.3	TECHNICAL REVIEW OF APPLICATIONS AFTER OPERATING PLATFORM CHANGES	SA-10	DEVELOPER CONFIGURATION MANAGEMENT
14.2.3 14.3.1	TECHNICAL REVIEW OF APPLICATIONS AFTER OPERATING PLATFORM CHANGES PROTECTION OF TEST DATA		
15.1.1 15.1.3	INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAIN	SA-12	SUPPLY CHAIN PROTECTION
15.1.3	INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAIN		
15.1.3	INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAIN	SA-12	SUPPLY CHAIN PROTECTION
15.1.1	INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS		
15.1.1 13.2.2	INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS AGREEMENTS ON INFORMATION TRANSFER		
15.1.2 15.1.1	ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS	SA-4	ACQUISITION PROCESS
15.2.1 15.1.1	MONITORING AND REVIEW OF SUPPLIER SERVICES INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS		
15.1.1	INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS		
15.1.2	ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS		
15.2.1 15.2.1	MONITORING AND REVIEW OF SUPPLIER SERVICES MONITORING AND REVIEW OF SUPPLIER SERVICES		
14.1.1 14.2.7	INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION OUTSOURCED DEVELOPMENT	SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS
14.2.7	OUTSOURCED DEVELOPMENT		
		SA-18	TAMPER RESISTANCE AND DETECTION
		SA-19	COMPONENT AUTHENTICITY
		SA-19 SA-20	COMPONENT AUTHENTICITY
		SA-20 SA-22	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS UNSUPPORTED SYSTEM COMPONENTS
		SC-2	APPLICATION PARTITIONING
		SC-3	SECURITY FUNCTION ISOLATION
		SC-4	INFORMATION IN SHARED RESOURCES
13.2.3	ELECTRONIC MESSAGING	SC-5	DENIAL OF SERVICE PROTECTION
		SC-6	RESOURCE AVAILABILITY
13.1.3	SEGREGATION IN NETWORKS	SC-7 SC-7	BOUNDARY PROTECTION BOUNDARY PROTECTION
13.1.3 13.1.3	SEGREGATION IN NETWORKS SEGREGATION IN NETWORKS	SC-39 SC-39	PROCESS ISOLATION PROCESS ISOLATION
13.2.3 13.2.1	ELECTRONIC MESSAGING INFORMATION TRANSFER POLICIES AND PROCEDURES	SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY
13.2.1 14.1.3	PROTECTING APPLICATION SERVICES TRANSACTIONS	30%	TRANSMISSION CONFIDENTIALITY AND INTEGRITY
13.2.1	INFORMATION TRANSFER POLICIES AND PROCEDURES		
13.2.1 13.2.1	INFORMATION TRANSFER POLICIES AND PROCEDURES INFORMATION TRANSFER POLICIES AND PROCEDURES		
		SC-10	NETWORK DISCONNECT
		SC-11	TRUSTED PATH
10.1.2	KEY MANAGEMENT	SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
10.1.2	KEY MANAGEMENT	SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES
10.1.2	KEY MANAGEMENT	SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
10.1.2 10.1.2	KEY MANAGEMENT KEY MANAGEMENT	SC-12 SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
10.1.2	KEY MANAGEMENT	SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
10.1.2	KEY MANAGEMENT		
10.1.1	POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS		
	POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS	SC-15	COLLABORATIVE COMPUTING DEVICES
	POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS	SC-16	COLLABORATIVE COMPUTING DEVICES TRANSMISSION OF SECURITY ATTRIBUTES
	POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS	SC-16 SC-18 SC-18	
	POLICY ON THE USE OF CRIPTOGRAPHIC CONTROLS	SC-16 SC-18 SC-18 SC-18	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE MOBILE CODE
	POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS	SC-16 SC-18 SC-18 SC-18 SC-19	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE MOBILE CODE VOICE OVER INTERNET PROTOCOL
	POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS	SC-16 SC-18 SC-18 SC-18 SC-19 SC-20	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE MOBILE CODE VOICE OVER INTERNET PROTOCOL SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)
10.1.1		SC-16 SC-18 SC-18 SC-18 SC-19 SC-20 SC-20	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE MOBILE CODE VOICE OVER INTERNET PROTOCOL SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)
	POLICY ON THE USE OF CRIPTOGRAPHIC CONTROLS	SC-16 SC-18 SC-18 SC-19 SC-20 SC-20 SC-21	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE MOBILE CODE VOICE OVER INTERNET PROTOCOL SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSVE OR CACHING RESOLVER
10.1.1		SC-16 SC-18 SC-18 SC-18 SC-19 SC-20 SC-20	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE MOBILE CODE VOICE OVER INTERNET PROTOCOL SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSVE OR CACHING RESOLVER ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE
10.1.1	NETWORK CONTROLS	SC-16 SC-18 SC-18 SC-19 SC-20 SC-20 SC-20 SC-21 SC-22	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE VOICE OVER INTERNET PROTOCOL SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURING OF ACHING RESOLVER)
10.1.1	NETWORK CONTROLS	SC-16 SC-18 SC-18 SC-19 SC-20 SC-20 SC-20 SC-21 SC-22 SC-22 SC-23	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE VOICE OVER INTERNET PROTOCOL SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVEN RESOLVEN RESOLVEN SERVICE SESSION AUTHORITICTY
10.1.1	NETWORK CONTROLS	SC-16 SC-18 SC-18 SC-19 SC-20 SC-20 SC-20 SC-21 SC-22 SC-23 SC-24 SC-26 SC-27	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE MOBILE CODE VOICE OVER INTERNET PROTOCOL. SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVENT ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVENT SERVICE SESSION AUTHORITORY FALL IN KNOWN STATE HONEYOTS PLATFORM-INGERENCENT APPLICATIONS
10.1.1	NETWORK CONTROLS	SC-16 SC-18 SC-18 SC-19 SC-20 SC-20 SC-21 SC-22 SC-23 SC-24 SC-26	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE MOBILE CODE VOICE CODE SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURIVE OR CACHING RESOLVER ARGUTETCURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE SESSION AUTHENTICITY FALL IN ENVOYS STATE HOMEPPOTS
10.1.1	NETWORK CONTROLS	SC-16 SC-18 SC-18 SC-19 SC-20 SC-20 SC-21 SC-22 SC-23 SC-24 SC-26 SC-26 SC-27 SC-28	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE MOBILE CODE VOICE OVER INTERNET PROTOCOL. SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)) SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSVE OR CACHING RESOLVEN RESOLVEN SERVICE ADD REOVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE SERVICE NAME / ADDRESS RESOLUTION SERVICE HERDORING PROVISION AT REST HETEROGENEITY
10.1.1	NETWORK CONTROLS	SC-16 SC-18 SC-18 SC-19 SC-20 SC-20 SC-21 SC-22 SC-23 SC-24 SC-24 SC-26 SC-27 SC-28 SC-29	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE MOBILE CODE VICE UVER INTERNET PROTOCOL SECURI NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURI NAME / ADDRESS RESOLUTION SERVICE (ELURISY DE CACHING RESOLVERI ADDRESS RESOLUTION SERVICE (ERULSY DE CACHING RESOLVERI ADDRESS RESOLVERI ADDRESS RESOLVERI RESOLVERI ADDRESS RESOLVERI RESOLVERI RESOLVERI ADDRESS RESOLVERI RESOLVERI ADDRESS RESOLVERI R
10.1.1	NETWORK CONTROLS	50.16 50.18 50.18 50.18 50.20 50.20 50.20 50.21 50.22 50.23 50.24 50.24 50.24 50.26 50.26 50.28 50.29 50.28 50.29 50.30 50.31 50.31	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE MOBILE CODE VOICE OVER INTERNIST PROTOCOL SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVEN RESOLVEN RESOLVEN SERVICE SERVICE MORE/FOTS PULATFORM NEIDPENDENT APPLICATIONS PROTOCTION OF INFORMATION AT REST HOTER/FOTS PULATFORM NEIDPENDENT APPLICATIONS PROTOCTION OF INFORMATION AT REST HITEROGENETY CONCELLIENT AND MISDRECTION COVERT CHANNEL ANALYSIS
10.1.1	NETWORK CONTROLS	52.16 52.18 52.18 52.19 52.19 52.20 52.21 52.21 52.23 52.23 52.23 52.24 52.23 52.24 52.23 52.24 52.24 52.29 52.30 52.30 52.31	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE MOBILE CODE MOBILE CODE SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SERVICE SERVICE SERVICE SERVICE SERVICE PALIFORMINGERVICENT APPLICATIONS PROTECTION OF INFORMATION AT REST HETEROGENEITY COVERT OHANNEL ANALYSIS COVERT OHANNEL ANALYSIS INFORMATION SERVICE MARTINENDING
10.1.1	NETWORK CONTROLS	50.16 50.18 50.18 50.19 50.20 50.20 50.21 50.21 50.21 50.23 50.27 50.28 50.27 50.28 50.27 50.28 50.29 50.20 50.21 50.29 50.20 50.21 50.21 50.20 50.21 50.20 50.210	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE MOBILE CODE VICE UVER INTERNET PROTOCOL SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURITION SECURITY FAIL IN KNOWN STATU FAIL IN KNOWN STATU FAIL IN KNOWN STATU CONCERLINENT ADD MISSIONECTION COVERT COMMEL ANALYSIS INFORMATION SYSTEM PARTITIONING INFORMATION STATEM PARTICIPANING
10.1.1	NETWORK CONTROLS	52.16 52.13 52.13 52.13 52.20 52.20 52.21 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE VICE OVER INTERNET PROTOCOL SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURISVE OR CACHING RESOLVEN SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURISVE OR CACHING SERVICE SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURISVE OR CACHING SERVICE SECURE NAME / ADDRESS RESOLUTION SERVICE FAIL IN FORM STATE HETEROGENEITY CONCELLANIENT ADD MISDRETCION COVERT CHANNEL ANALYSS COVERT CHANNEL ANALYSS COVERT CHANNEL ANALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS
10.1.1 13.1.1 14.1.3	NETWORK CONTROLS PROTECTING APPLICATION SERVICES TRANSACTIONS	50.16 50.18 50.18 50.19 50.20 50.20 50.21 50.21 50.21 50.23 50.27 50.28 50.27 50.28 50.27 50.28 50.29 50.20 50.21 50.29 50.20 50.21 50.21 50.20 50.21 50.20 50.210	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE MOBILE CODE VICE UVER INTERNET PROTOCOL SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURITION SECURITY FAIL IN KNOWN STATU FAIL IN KNOWN STATU FAIL IN KNOWN STATU CONCERLINENT ADD MISSIONECTION COVERT COMMEL ANALYSIS INFORMATION SYSTEM PARTITIONING INFORMATION STATEM PARTICIPANING
10.1.1	NETWORK CONTROLS	52.16 52.13 52.13 52.13 52.20 52.20 52.21 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE VICE OVER INTERNET PROTOCOL SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURISVE OR CACHING RESOLVEN SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURISVE OR CACHING SERVICE SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURISVE OR CACHING SERVICE SECURE NAME / ADDRESS RESOLUTION SERVICE FAIL IN FORM STATE HETEROGENEITY CONCELLANIENT ADD MISDRETCION COVERT CHANNEL ANALYSS COVERT CHANNEL ANALYSS COVERT CHANNEL ANALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS
10.1.1 13.1.1 14.1.3 12.2.1 12.2.1	NETWORK CONTROLS PROTECTING APPLICATION SERVICES TRANSACTIONS	52.16 52.13 52.13 52.13 52.20 52.20 52.21 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE VICE OVER INTERNET PROTOCOL SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURISVE OR CACHING RESOLVEN SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURISVE OR CACHING SERVICE SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURISVE OR CACHING SERVICE SECURE NAME / ADDRESS RESOLUTION SERVICE FAIL IN FORM STATE HETEROGENEITY CONCELLANIENT ADD MISDRETCION COVERT CHANNEL ANALYSS COVERT CHANNEL ANALYSS COVERT CHANNEL ANALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS
10.1.1 13.1.1 14.1.3 12.2.1 12.2.1 12.2.1	NETWORK CONTROLS PROTECTING APPLICATION SERVICES TRANSACTIONS CONTROLS AGAINST MALWARE	52.16 52.13 52.13 52.13 52.20 52.20 52.21 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE VICE OVER INTERNET PROTOCOL SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURISVE OR CACHING RESOLVEN SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURISVE OR CACHING SERVICE SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURISVE OR CACHING SERVICE SECURE NAME / ADDRESS RESOLUTION SERVICE FAIL IN FORM STATE HETEROGENEITY CONCELLANIENT ADD MISDRETCION COVERT CHANNEL ANALYSS COVERT CHANNEL ANALYSS COVERT CHANNEL ANALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS
1011 1311 1413 1221 1221 1221 1221 1221 12	NETWORK CONTROLS PROTECTING APPLICATION SERVICES TRANSACTIONS CONTROLS AGAINST MALWARE CONTROLS	52.16 52.13 52.13 52.13 52.20 52.20 52.21 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE VICE OVER INTERNET PROTOCOL SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVEN SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING SERVICE SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING SERVICE SECURE NAME / ADDRESS RESOLUTION SERVICE FAIL IN FORM STATE HETEROGENEITY CONCELLANIENT ADD MISDRETCION COVERT CHANNEL ANALYSS COVERT CHANNEL ANALYSS COVERT CHANNEL ANALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS
10.1.1 13.1.1 14.1.3 14.2.3 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1	NETWORK CONTROLS PROTECTING APPLICATION SERVICES TRANSACTIONS CONTROLS AGAINST MALWARE CONTROL	52.16 52.13 52.13 52.13 52.20 52.20 52.21 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE VICE OVER INTERNET PROTOCOL SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVEN SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING SERVICE SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING SERVICE SECURE NAME / ADDRESS RESOLUTION SERVICE FAIL IN FORM STATE HETEROGENEITY CONCELLANIENT ADD MISDRETCION COVERT CHANNEL ANALYSS COVERT CHANNEL ANALYSS COVERT CHANNEL ANALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS
1011 1311 1413 1221 1221 1221 1221 1221 12	NETWORK CONTROLS PROTECTING APPLICATION SERVICES TRANSACTIONS CONTROLS AGAINST MALWARE CONTROLS	52.16 52.13 52.13 52.13 52.20 52.20 52.21 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE VICE OVER INTERNET PROTOCOL SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVEN SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING SERVICE SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING SERVICE SECURE NAME / ADDRESS RESOLUTION SERVICE FAIL IN FORM STATE HETEROGENEITY CONCELLANIENT ADD MISDRETCION COVERT CHANNEL ANALYSS COVERT CHANNEL ANALYSS COVERT CHANNEL ANALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS
1011 1011 1013 1013 1013 1013 1013 1013	NETWORE CONTROLS PROTECTING APPLICATION SERVICES TRANSACTIONS CONTROLS AGAINST MALWARE CONTROL	6-1-6 6-13 6-23	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE MOBILE CODE MOBILE CODE CONTRACTION AND ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURIE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURIE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURIE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURIES NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SOURCE NAME / REPORTSOL REPORTSOL SOURCE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE ROBES RESOLUTION SOURCE) NAME / REPORTSOL RAME / ADDRESS RESOLUTION SOURCE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE ROBES RESOLUTION SOURCE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE ROBES) ADDRESS RESOLUTION SERVICE (RECURSIVE ROBES) ADDRESS RESOLUTION SERVICE RECURSIVE ROBES NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE ROBES) ADDRESS RESOLUTION SERVICE ADDRESS NAME / ADDRESS RESOLUTION SERVICE ADDRESS RESOLUTION SERVICE ADDRESS NAME / ADDRESS RESOLUTION SERVICE ADDRESS RESOLUTION SERVICE ADDRESS NAME / ADDRESS RESOLUTION SERVI
10.1.1 10.1.1 14.1.3 14.2.3 14.2.3 12.2.1 12.2.1 12.2.1	NETWORK CONTROLS PROTECTING APPLICATION SERVICES TRANSACTIONS CONTROLS AGAINST MALWARE CONTROL	52.16 52.13 52.13 52.13 52.20 52.20 52.21 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24 52.24	TRANSMISSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE VICE OVER INTERNET PROTOCOL SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVEN SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING SERVICE SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING SERVICE SECURE NAME / ADDRESS RESOLUTION SERVICE FAIL IN FORM STATE HETEROGENEITY CONCELLANIENT ADD MISDRETCION COVERT CHANNEL ANALYSS COVERT CHANNEL ANALYSS COVERT CHANNEL ANALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS INFOMMEL NALYSS
10.1.1 33.1.1 44.3 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1	NETWORK CONTROLS PROTECTING APPLICATION SERVICES TRANSACTIONS CONTROLS AGAINST MALWARE CONTROL	92-14 92-13 92-23 92-23 92-23 92-23 92-24 92-24 92-24 92-24 92-24 92-24 92-24 92-24 92-24 92-24 92-24 92-24 92-24 92-24 92-24 92-25 92	Indefinition of Security Attributes Mailling of Mailling of Mailli
10.1.1 33.1.1 44.3 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1	NETWORK CONTROLS PROTECTING APPLICATION SERVICES TRANSACTIONS CONTROLS AGAINST MALWARE CONTROL	52-16 52-18 52-18 52-28 52-20 52-21 52-22 52-23 52-23 52-23 52-23 52-23 52-23 52-23 52-23 52-23 52-23 52-23 52-23 52-25 52-25 52-25 52-25 52-25	INNERSION OF SICURITY ATTRIBUTES MOBILI CODE MOBILI CO
10.1.1 33.1.1 44.3 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1	NETWORK CONTROLS PROTECTING APPLICATION SERVICES TRANSACTIONS CONTROLS AGAINST MALWARE CONTROL	6-14 6-13 6-14 6-14 6-14 6-20 6-20 6-20 6-20 6-20 6-21 6-24	INVERSION OF SICURITY ATTRIBUTES MOBILE 2003 MOBILE 20
10.1.1 33.1.1 44.3 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1	NETWORK CONTROLS PROTECTING APPLICATION SERVICES TRANSACTIONS CONTROLS AGAINST MALWARE CONTROL	6-1-16 6-13 6-23 6-23 6-23 6-23 6-23 6-23 6-24 6-24 6-25	INNERSION OF SICURITY ATTRIBUTES MOBILI CODE MOBILI CODE MOBILI CODE MOBILI CODE UNICI VIRI MEMINI PROTOCIO. SICURIE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SICURIE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) COLLECTION REVERSION SICURIES NOTAMALINA STATE COLLECTION REVERSION SCIENCE NOTAMALINA STATE ADDRESS RESOLUTION SERVICE NOTAMALINA STATE ADDRESS RESOLUTION SERVICE NO
10.1.1 33.1.1 44.3 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1	NETWORK CONTROLS PROTECTING APPLICATION SERVICES TRANSACTIONS CONTROLS AGAINST MALWARE CONTROL	2-1-6 2-13 2-13 2-23 2-23 2-24	INNERSION OF SECURITY ATTRIBUTES MOBILE CODE MOBILE CODE MOBILE CODE CONTRIBUTE MOBILE CODE CONTRIBUTE MOBILE CODE MOBILE CODE CONTRIBUTE SECURITY AND ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) CONTRIBUTE RESOLUTION TO ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURITY AND ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SECURITY ALL RECOMPSISION OF ADDRESS RESOLUTION SERVICE MORTORITY CONCELLATION INFORMATIVE AT REST INFORMATION SYSTEM PARTITIONING NON MOBILE ELECULTABLE PROGRAMS INFORMATION SYSTEM PARTITIONING NON MOBILE ELECULTABLE PROGRAMS INFORMATIVE SOURCES MORTORISTICE SECURITY AND ADDRESS INFORMATIVE SOURCES MORTORISTICE SECURITY ADDRESS SINCOR CAMPANELY MILESS LINE REFORTETION SINCOR CAMPANELY AND DATA SINCOR CAMPANELY AND DATA SINCOR CAMPANELY AND DATA
10.1.1 33.1.1 44.3 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1	NETWORK CONTROLS PROTECTING APPLICATION SERVICES TRANSACTIONS CONTROLS AGAINST MALWARE CONTROL	6-1-16 6-13 6-23 6-23 6-23 6-23 6-23 6-23 6-24 6-24 6-25	INNERSION OF SICURITY ATTRIBUTES MOBILI CODE MOBILI CODE MOBILI CODE MOBILI CODE UNICI VIRI MEMINI PROTOCIO. SICURIE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SICURIE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) COLECT COMMENDATION STATE SOURCE COLUMNE RAVIESS NOME ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) COVERT COMMENDE REVUENTATIVE ROBCAMAS COVERT COMMENDE SECURIESE FROGRAMAS SICURIE NAME / ADDRESS RESOLUTION SERVICE MICHAESE LINE REVOETECTION COVERT COMMENDE SECURIESE FROGRAMAS SICURIESE LINE REVOETECTION COVERT COMMENDE SECURIESE FROGRAMAS SICURIESE LINE REVOETECTION COVERT COMMENDELSENCE SISSICE COMMENDES SICURIESE LINE REVOETECTION COVERT COMMENDES SICURIESE LINE REVOETECTION SICURIESE LINE REVOETECTION COVERT COMMENDES SICURIESE LINE REVOETECTION SICURIESE LINE REVOETECTION COVERT COMMENDES SICURIESE LINE REVOETECTION SICURIESE LINE REVOETECTION
10.1.1 33.1.1 44.3 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1	NETWORK CONTROLS PROTECTING APPLICATION SERVICES TRANSACTIONS CONTROLS AGAINST MALWARE CONTROL	6-14 6-13 6-13 6-23 6-20 9-20	INNERSION OF SICURITY ATTRIBUTES MOBILI CODE MOBILI CODE MOBILI CODE MOBILI CODE MOBILI CODE MOBILICADE SICURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SICURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SICURITY ALL REMOVINITION SOURCE) MOBILITY SOURCE AND MOSIDIRECTION COMET COMMEL ANALYSIS NOM MOBILIFALE EXECUTABLE PROGRAMS NOM MOBILIFALE EXECUTABLE PROGRAMS NOM MOBILIFALE EXECUTABLE PROGRAMS MOBILIFACIONS SOURCE) SIGNOCACIMALITY AND DATA SISSICO CAMBILITY AND DATA
10.1.1 33.1.1 44.3 44.3 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1 12.2.1	NITWORK CONTROLS PROTECTING APPLICATION SERVICES TRANSACTIONS CONTROLS AGAINST MALWARE CONTROLS CONTROLS CONTROLS AGAINST MALWARE CONTROLS CONTROLS AGAINST MALWARE CONTROLS CONTROLS CONTROLS CONTROLS	2-14 2-13 2-13 2-23 2-23 2-24 2-24 2-24 2-24 2-24 2-24 2-24 2-25 2-24	INNIMISSION OF SICURITY ATTRIBUTES MOBILI CODE MOBILI CODE CONTRIBUTE CODE CONTRIBUTE CONTRIBUTES MOBILI CODE CONTRIBUTES RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SICURI NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) CONTROL NAME / ADDRESS RESOLUTION SOURCE / ADDRES
10.1.1 10.1.1 14.1.3 14.1.3 14.1.3 12.1.1 12.1.1 12.1.1 12.1.1 13.1.1	NETWORK CONTROLS PROTECTING APPLICATION SERVICES TRANSACTIONS CONTROLS AGAINST MALVARE CONTROLS	6-1-6 6-1-8 6-1-8 9-1-9 9-	INNERSION OF SICURITY ATTRIBUTES MOBILI CODE MOBILI CODE MOBILI CODE MOBILI CODE MOBILI CODE MOBILI CODE MOBILICADE SICURI NAME / ADDRESS RESOLUTION SIRVICE (AUTHORITATIVE SOURCE) SICURI NAME / ADDRESS RESOLUTION SIRVICE (RUINING OLICADINA RESOLUTION SIRVICE MATINE (REINING INDOBESS RESOLUTION RESOLUTION SINGERS RESOLUTION SIRVICE (RUINING OLICADINA RESOLUTION SIRVICE MATINE (REINING INDOBESS RESOLUTION RESOLUTION SIRVICE MATINE (REINING INDOBESS RESOLUTION RESOLUTION SIRVICE MATINE (REINING INDOBESS RESOLUTION RESOLUTION SIRVICE RESOLUTION SIRVICE (RUINING OLICADINA RESOLUTION SIRVICE RESOLUTION SIRVICE (RUINING INDOBESS RESOLUTION SIRVICE) MOBILI COMPANIES RESOLUTION SIRVICE (RUINING INDOBESS RESOLUTION SIRVICE) MOBILI COMPANIES RESOLUTION SIRVICE NON MOBILIALE DECUTABLE PROGRAMS NON MOBILIALE DECUTABLE PROGRAMS MOBILI DECUTABLE PROGRAM

JNCSF-413	Deploy monitoring devices at ad hoc locations within systems to track specific types of transactions as				SI-4	
	necessarv Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and	Operation				INFORMATION SYSTEM MONITORING
JNCSF-414	deletion Establish procedures to appropriately increase monitoring upon indication of increased risk to operations,	Operation			SI-4	INFORMATION SYSTEM MONITORING
JNCSF-415 JNCSF-416	assets, or individuals	Operation Operation	6.1.4	CONTACT WITH SPECIAL INTEREST GROUPS	SI-4 SI-5	INFORMATION SYSTEM MONITORING SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
JNCSF-417	Receive information system security alerts, advisories, and directives from external organizations Disseminate security alerts, advisories, and directives to appropriate personnel	Operation	6.1.4	CONTACT WITH SPECIAL INTEREST GROUPS	SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
JNCSF-418 JNCSF-419	Implement external security directives in a timely fashion, as defined by security policies Employ integrity verification tools to detect unauthorized changes to software, firmware, and/or information	Operation Operation	13.2.1	INFORMATION TRANSFER POLICIES AND PROCEDURES	SI-5 SI-7	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES 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 JNCSF-422	Update spam protection mechanisms when new releases are available Configure information systems to check the validity of information inputs	Operation Operation			SI-8 SI-10	SPAM PROTECTION 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 Handle and retain information and output from information systems over its full life cycle in accordance	Operation			SI-11	ERROR HANDLING
JNCSF-425	with policies Determine mean time to failure (MTTF) for information system components in specific operation	Operation			SI-12	INFORMATION HANDLING AND RETENTION
JNCSF-426	environments Create substitute information system components and a means to exchange active and standby	Operation			SI-13	PREDICTABLE FAILURE PREVENTION
JNCSF-427	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 orotected	Operation	8.1.2 14.1.1	OWNERSHIP OF ASSETS INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION		
JNCSF-430 JNCSF-431	Separate operational responsibility for networks from computer operations where appropriate Identify and include security mechanisms, service levels, and management requirements of all network	Operation Operation	13.1.1 13.1.2	NETWORK CONTROLS SECURITY OF NETWORK SERVICES		
JNCSF-432	services in network services agreements Protect all types of records from destruction, unauthorized access, and falsification	Operation	18.1.3	PROTECTION OF RECORDS	AU-9	PROTECTION OF AUDIT INFORMATION
JNCSF-433	Issue guidelines on the retention, storage, handling and disposal of records and information	Operation	12.4.2 18.1.3	PROTECTION OF LOG INFORMATION PROTECTION OF RECORDS	10.5	PROTECTION OF ADDIT INFORMATION
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				
					AC-1 AT-1	ACCESS CONTROL POLICY AND PROCEDURES SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
					AU-1 CA-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES
					CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES
					CP-1 IA-1	CONTINGENCY PLANNING POLICY AND PROCEDURES IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES
JNCSF-438	Establish cadence to review and update control policies	Foundational	5.1.2	REVIEW OF THE POLICIES FOR INFORMATION SECURITY	IR-1 MA-1	INCIDENT RESPONSE POLICY AND PROCEDURES SYSTEM MAINTENANCE POLICY AND PROCEDURES
					MP-1 PE-1	MEDIA PROTECTION POLICY AND PROCEDURES PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES
					PL-1 PS-1	SECURITY PLANNING POLICY AND PROCEDURES PERSONNEL SECURITY POLICY AND PROCEDURES
					RA-1 SA-1	RISK ASSESSMENT POLICY AND PROCEDURES SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES
					SC-1 SI-1	SYSTEM AND COMMUNICATION PROTECTION POLICY AND PROCEDURES SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES
					AC-1 AT-1	STSTEM AND INFORMATION INTEGRITP OULT AND PROCEDURES ACCESS CONTROL POLICY AND PROCEDURES SFCIIRITY AWARFNESS AND TRAINING POLICY AND PROCEDURES
					AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES
					CA-1 CM-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES CONFIGURATION MANAGEMENT POLICY AND PROCEDURES
					CP-1 IA-1	CONTINGENCY PLANNING POLICY AND PROCEDURES IDENTIFICATION AND AUTHENTICATION 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	IR-1 MA-1	INCIDENT RESPONSE POLICY AND PROCEDURES SYSTEM MAINTENANCE POLICY AND PROCEDURES
			12.1.1	DOCUMENTED OPERATING PROCEDURES	MP-1 PE-1	MEDIA PROTECTION POLICY AND PROCEDURES PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES
					PL-1 PS-1	SECURITY PLANNING POLICY AND PROCEDURES PERSONNEL SECURITY POLICY AND PROCEDURES
					RA-1 SA-1	RISK ASSESSMENT POLICY AND PROCEDURES SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES
					SC-1 SI-1	SYSTEM AND COMMUNICATION PROTECTION 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	and recorded	Foundational			AC-8	SYSTEM USE NOTIFICATION
JNCSF-444 JNCSF-445	Require users to acknowledge security notices before attempting to access information systems Configure publicly accessible information systems to display appropriate security notices before granting	Foundational			AC-8 AC-8	SYSTEM USE NOTIFICATION SYSTEM USE NOTIFICATION
	access to users Configure information systems to notify users, upon each successful logon, of the date and time of their last					
JNCSF-446	lozon		9.4.2	SECURE LOG-ON PROCEDURES	AC-9	PREVIOUS LOGON (ACCESS) NOTIFICATION
JNCSF-447	Ensure everyone in the organization assesses the appropriate protection level of information by analyzing	Foundational			AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
JNCSF-448 JNCSF-449	confidentiality, integrity, and availability Develop and implement procedures to bandle assets consistent with their classification	Foundational	8.2.1 8.2.3	CLASSIFICATION OF INFORMATION HANDLING OF ASSETS		
JNCSF-450	Establish policies on the use of privately owned equipment for teleworking activities	Foundational	6.2.2	TELEWORKING		
JNCSF-451 JNCSF-452	Provide additional training for personnel using mobile devices Establish terms and conditions with third-parties to establish how users access information from external	Foundational	15.1.2	ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS	AC-19 AC-20	ACCESS CONTROL FOR MOBILE DEVICES USE OF EXTERNAL INFORMATION SYSTEMS
JNCSF-453	information systems Establish terms and conditions with third parties to establish how information is processed, stored, or	Foundational	15.1.2	ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS	AC-20	USE OF EXTERNAL INFORMATION SYSTEMS
JNCSF-454	transmitted on external information systems Create a process that enables authorized users to determine if access rights to sensitive data assigned to	Foundational	10.11	ADDRESSING SECORITY WITHIN SUPPLIER AGREEMENTS	AC-21	
	sharing partners is appropriate. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic					INFORMATION SHARING
JNCSF-455	information Determine and meet requirements for protection, confidentiality, and integrity of information involved in	Foundational			AC-22	PUBLICLY ACCESSIBLE CONTENT
JNCSF-456	application services on public networks Establish protection or insurance against liability associated with fraudulent transactions of information	Foundational	14.1.2	SECURING APPLICATION SERVICES ON PUBLIC NETWORKS		
JNCSF-457	establish protection of insurance against maxing associated with radioteric transactions of information involved in application services on public networks Establish procedures to ensure nonpublic information is not posted onto a publicly accessible information	Foundational	14.1.2	SECURING APPLICATION SERVICES ON PUBLIC NETWORKS		
JNCSF-458	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 JNCSF-461	Provide awareness training to employees affected by information system changes Provide ongoing role-based security awareness training to employees and contractors with assigned security	Foundational	7.2.2	INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING	AT-2 AT-3	SECURITY AWARENESS TRAINING ROLE-BASED SECURITY TRAINING
JNCSF-462	roles and responsibilities Provide role-based awareness training to employees with assigned security roles and responsibilities that	Foundational	13.2.1	INFORMATION TRANSFER POLICIES AND PROCEDURES	AT-3	
JNCSF-462 JNCSF-463	are affected by information system changes Update awareness training materials over time, incorporating lessons learned from security incidents	Foundational	7.2.2	INFORMATION SECURITY AWARENESS. EDUCATION AND TRAINING	Alis	ROLE-BASED SECURITY TRAINING
JNCSF-464 JNCSF-465	Update awareness training materials as employee and contractor roles change Document, monitor, and retain individual information system security training activities and records	Foundational Foundational	7.2.2	INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING	AT-4	SECURITY TRAINING RECORDS
JNCSF-466	Document, monitor, and retain individual information system security training activities and records Configure information systems to provide audit record generation capabilities for auditable events Coordinate with external organizations to define acceptable procedures before sharing audit information	Foundational			AU-12	AUDIT GENERATION
JNCSF-467	cross-organizationally	Foundational			AU-16	CROSS-ORGANIZATIONAL AUDITING SECURITY ASSESSMENTS
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 CA-2	SECURITY ASSESSMENTS DEVELOPER SECURITY TESTING AND EVALUATION SECURITY ASSESSMENTS
JNCSF-469	Establish a procedure to assess the effectiveness of information system security controls' effectiveness	Foundational			SA-11	DEVELOPER SECURITY TESTING AND EVALUATION
JNCSF-470		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	contraental Define procedures to notify appropriate personnel of information spills using communication methods not associated with the spill	Foundational	9.3.1	RESPONSE TO INFORMATION SECURITY INCIDENTS	IR-9	INFORMATION SPILLAGE RESPONSE
JNCSF-476	Ensure compliance with all information system and network maintenance requirements imposed by	Foundational	11.2.4	EQUIPMENT MAINTENANCE		
JNCSF-477	insurance policies Physically control and securely store media within controlled areas	Foundational	8.3.1	MANAGEMENT OF REMOVABLE MEDIA	MP-4	MEDIA STORAGE
JNCSF-478	Protect media until it is destroyed or sanitized using approved equipment and procedures	Foundational	18.1.3 8.3.1	PROTECTION OF RECORDS 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
		Foundational Foundational	11.1.2	PHYSICAL ENTRY CONTROLS	PE-2 PE-2	PHYSICAL ACCESS AUTHORIZATIONS PHYSICAL ACCESS AUTHORIZATIONS
JNCSF-480 JNCSF-481	Develop, approve, and maintain a list of individuals with authorized access to facilities Issue authorization credentials for facility access	Foundational	11.1.2 11.1.1	PHYSICAL ENTRY CONTROLS	PE-2	PHYSICAL ACCESS AUTHORIZATIONS
JNCSF-481 JNCSF-482	Issue authorization credentials for facility access Review facility access lists and remove any individuals for whom access is no longer required			PHYSICAL SECURITY PERIMETER	PE-3 PE-3	PHYSICAL ACCESS CONTROL PHYSICAL ACCESS CONTROL
JNCSF-481 JNCSF-482 JNCSF-483	Issue authorization credentials for facility access Review facility access lists and remove any individuals for whom access is no longer required Enforce physical access authorizations at entry/exit points using devices and/or guards to verify individual access authorizations	Foundational				MONITORING PHYSICAL ACCESS
JNCSF-481 JNCSF-482	Issue authorization credentials for facility access Review facility access its and renove any individuals for whom access is no longer required Enforce physical access authorizations at entry/exit points using devices and/or guards to verify individual access authorizations Maintain physical access audit logs for entry/exit points and frequently review as needed		11.1.2	PHYSICAL ENTRY CONTROLS	PE-6 PE-3	
JNCSF-481 JNCSF-482 JNCSF-483 JNCSF-484 JNCSF-485 JNCSF-486	Issue autorotation credentials for faulty access Review facility access its and remova en individuals for whom access is no longer required Enforce physical access authorizations at entry/exit points using devices and/or guards to verify individual access authorizations Maintain physical access audo logs for entry/exit points and frequently review as needed Provide and required to control access to publicly accessible areas within the facility Provide and required to control access to publicly accessible areas within facilities	Foundational Foundational Foundational Foundational		PHYSICAL ENTRY CONTROLS	PE-3	PHYSICAL ACCESS CONTROL
JNCSF-481 JNCSF-482 JNCSF-483 JNCSF-484 JNCSF-485 JNCSF-486 JNCSF-487	Issue autoincation condentials of facility access Biorela facility access that and remova any individuals for whom access is no longer required Enforce physical access authorizations at entrylent points using devices and/or guards to verify individual advantain physical access audio logs for entryl-rela points and frequently verifies as needed Maintain physical access audio logic for entryl-rela points and frequently verifies as needed Pointee and frequencing access to publicly accessible areas within the facility Provide and frequencing access to publicly accessible areas within the facility Provide and frequencing access to publicly accessible areas within the facility Provide and Registering access for access to publicly accessible access dates areas within the facility Provide and Registering access for access for access to publicly accessible	Foundational Foundational Foundational Foundational	11.1.2		PE-3 PE-3	PHYSICAL ACCESS CONTROL PHYSICAL ACCESS CONTROL
JNCSF-481 JNCSF-482 JNCSF-483 JNCSF-484 JNCSF-485 JNCSF-486 JNCSF-486 JNCSF-487 JNCSF-488 JNCSF-489	Issue autorotation codentials for faulty access Issues autorotation codentials for faulty access Issues autorotations at entropicet points using devices and/or guards to verify individual Enforce physical access authorizations at entropicet points using devices and/or guards to verify individual access authorizations Individual access audo Ispans for entry/enit points and frequently review as needed Provide and guards to control access to publicy accessible areas within facilities Newlet and guards to control access to publicy accessible areas within facilities Review and interpreters Individual access access to publicity accessible areas within facilities Review and Review Individual Review and Review Individual Review In	Foundational Foundational Foundational Foundational Foundational Foundational		PHYSICAL EMTRY CONTROLS	PE-3 PE-3 PE-4 PE-5	PHYSICAL ACCESS CONTROL PHYSICAL ACCESS CONTROL ACCESS CONTROL FOR TRANSMISSION MEDIUM ACCESS CONTROL FOR OUTPUT DEVICES
JNC5F-481 JNC5F-482 JNC5F-483 JNC5F-484 JNC5F-485 JNC5F-486 JNC5F-487 JNC5F-487 JNC5F-489 JNC5F-490	Isue astrolation credentials for failiny access Reverse facility access Facility access the no longer required Factors physical access authorizations at entrylexe points using devices and/or guards to verify individual access authorizations at entrylexe points using devices and/or guards to verify individual access authorizations and the points and frequently review as needed Provide selegators to control access to publicly accessible areas within facilities Provide selegators to control access to publicly accessible areas within facilities Review and forequently theory theory theory theory theory theory accessible areas within facilities Review and requestive theory theory theory theory theory theory theory accessible areas within facilities Review and requestive theory theory theory theory theory theory theory theory theory accessible areas within facilities Review and theory	Foundational foundational foundational foundational foundational foundational foundational	11.1.2	CABUNG SECURITY	PE-3 PE-3 PE-5 PE-6 PE-8	PHYSICAL ACCESS CONTROL PHYSICAL ACCESS CONTROL ACCESS CONTROL FOR TRANSMISSION MEDIUM ACCESS CONTROL FOR OUTPUT DEVICES MONITORING PHYSICAL ACCESS VISITOR ACCESS BECORDS
JNCSF-481 JNCSF-482 JNCSF-483 JNCSF-484 JNCSF-485 JNCSF-485 JNCSF-486 JNCSF-487 JNCSF-488 JNCSF-489 JNCSF-490 JNCSF-491 JNCSF-492	Issue astrolation credentials for failiny access Reverse facility access Reverse authorizations at entrylveit points using devices and/or guards to verify individual access authorizations Reverse authorizations Reverse authorization Reverse authorization Reverse authorization Reverse R	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational	11.1.2		PE-3 PE-4 PE-5 PE-6 PE-8 PE-9	PHYSICAL ACCESS CONTROL PHYSICAL ACCESS CONTROL ACCESS CONTROL FOR TRANSMISSION MEDIUM ACCESS CONTROL FOR OUTPUT DEVICES MONTONICH PHYSICAL ACCESS VIENCIAL ACCESS CONTROL PHYSICAL ACCESS CON
JNCSF-481 JNCSF-482 JNCSF-483 JNCSF-484 JNCSF-485 JNCSF-486 JNCSF-487 JNCSF-487 JNCSF-489 JNCSF-490 JNCSF-491 JNCSF-491 JNCSF-492 JNCSF-493	Issue astronation codentials for facility access Browner State Control and Control and Control and Control Con	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational	11.1.2 11.2.3 11.1.2	CABLING SECURITY PHYSICAL ENTRY CONTROLS	PE-3 PE-4 PE-5 PE-6 PE-8 PE-9 PE-9 PE-9 PE-10	PHYSICAL ACCESS CONTROL PHYSICAL ACCESS CONTROL ACCESS CONTROL FOR TRANSMISSION MEDIUM ACCESS CONTROL FOR TRANSMISSION MONTORING PHYSICAL ACCESS VISITOR ACCESS RECORDS PHYSICAL ACCESS CONTROL POWRE (QUIPMENT AND CABLING EMERGENCY STUTOFF
INCSF-481 INCSF-482 INCSF-483 INCSF-484 INCSF-484 INCSF-486 INCSF-487 INCSF-487 INCSF-489 INCSF-491 INCSF-493 INCSF-494	Issue astronation codentials for facility access Review facility Review facilit	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational	11.1.2 11.2.3 11.1.2 11.2.3	CABLING SECURITY PHYSICAL ENTRY CONTROLS CABLING SECURITY	PE-3 PE-4 PE-5 PE-6 PE-8 PE-9 PE-9 PE-10 PE-10	PHYSICAL ACCESS CONTROL PHYSICAL ACCESS CONTROL ACCESS CONTROL FOR TRANSMISSION MEDIUM ACCESS CONTROL FOR OUTPUT DEVICES MONTONION FHYSICAL ACCESS MONTONION FHYSICAL ACCESS MONTONION FHYSICAL ACCESS MONTONIC FILL SECONDAL ACCESS CONTROL POWRE TO ACCESS TO ACCESS EMERGINCY SHUTOFF
NCSF-481 NCSF-482 NCSF-483 NCSF-484 NCSF-485 NCSF-486 NCSF-487 NCSF-487 NCSF-491 NCSF-491 NCSF-493 NCSF-494 NCSF-495 NCSF-495	Issue astronation codentials for faulty access Reverse facility access Reverse facility access tandronations at entrylveit points using devices and/or guards to verify individual Enforce physical access authorizations at entrylveit points using devices and/or guards to verify individual access authorizations Control Access authorization at entrylveit points and frequently review as needed Pointee and Regards to control access to publicy accessible areas within facilities Newlet enfoquently house lyncs, control access to publicy accessible areas within facilities Secure and frequently house lyncs, control access to publicy accessible areas within facilities Review and access access to publicity accessible areas within facilities Review and access access to access to information, and other physical access devices then needed (loss larve, terminated individual) Excort visitors and monitor activity by maintaining of frequently reviewing visitor access records to facilities Review to individual access to the facilities to detect and responsible visitors Review and monitor activity by maintaining ond frequently reviewing visitor access records to facilities Review shared access and build of power to information systems in entergency abaatoon Provide a ablent to that of paperts in blockatoots to facilities Review shared access accoss frequency and the access in entergency abaatoon Provide a ablent to abud the access access for the needed of the review of a monitor access records to facilities Review and and access ac	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational	11.1.2 11.2.3 11.1.2	CABLING SECURITY PHYSICAL ENTRY CONTROLS	PE-3 PE-4 PE-5 PE-6 PE-8 PE-3 PE-9 PE-10 PE-10 PE-11 PE-12	PHYSICAL ACCESS CONTROL ACCESS CONTROL FOR TRANSMISSION MEDIUM ACCESS CONTROL FOR TRANSMISSION MEDIUM ACCESS CONTROL FOR OUTPUT DEVICES MONTORING PHYSICAL ACCESS VIENCIAL ACCESS CONTROL POWER GUIMPRENT AND CARLING EMERGING VIENTOFF EMERGING VIENTOFF EMERGING VIENTING
NCSF-481 NCSF-482 NCSF-483 NCSF-484 NCSF-484 NCSF-485 NCSF-489 NCSF-489 NCSF-491 NCSF-491 NCSF-491 NCSF-494 NCSF-494	Issue astronation contentiation fractily access Below astronation contentiation fractily access Information access and/or access	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational	11.1.2 11.2.3 11.1.2 11.2.3	CABLING SECURITY PHYSICAL ENTRY CONTROLS CABLING SECURITY SUPPORTING UTILITIES SUPPORTING UTILITIES	PE-3 PE-4 PE-5 PE-6 PE-8 PE-3 PE-9 PE-10 PE-10 PE-10 PE-11	PHYSICAL ACCESS CONTROL PHYSICAL ACCESS CONTROL ACCESS CONTROL FOR TRANSMISSION MEDIUM ACCESS CONTROL FOR TRANSMISSION MEDIUM ACCESS CONTROL FOR TRANSMISSION MEDIUM MONTORING PHYSICAL ACCESS VISITOR ACCESS BECORES POVIET EQUIVALITY AND CALUNG BERKBIRCH SUITOFF BERKBIRCH SUITOFF BERKBIRCH SUITOFF BERKBIRCH SUITOFF
INCSF-481 INCSF-482 INCSF-483 INCSF-485 INCSF-485 INCSF-487 INCSF-489 INCSF-491 INCSF-491 INCSF-493 INCSF-494 INCSF-495 INCSF-495 INCSF-495 INCSF-495	Issue astronation contentiation fractility access Benefin facility access Benefin Bene	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational	11.1.2 11.2.3 11.1.2 11.2.3 11.2.2 11.2.2	CABLING SECURITY PHYSICAL ENTRY CONTROLS CABLING SECURITY SUPPORTING UTILITIES	PE-3 PE-4 PE-5 PE-6 PE-8 PE-10 PE-10 PE-10 PE-11 PE-11 PE-12 PE-13	PHYSICAL ACCESS CONTROL ACCESS CONTROL FOR TRANSMISSION MEDIUM ACCESS CONTROL FOR TRANSMISSION MEDIUM ACCESS CONTROL FOR OUTPUT DEVICES MONTORING PHYSICAL ACCESS VIENCIAL ACCESS CONTROL POWER GUIMPRENT AND CARLING EMERGING VIENTOFF EMERGING VIENTOFF EMERGING VIENTING
INCSF-481 INCSF-482 INCSF-483 INCSF-485 INCSF-485 INCSF-485 INCSF-489 INCSF-489 INCSF-492 INCSF-492 INCSF-493 INCSF-494 INCSF-496 INCSF-496 INCSF-499 INCSF-499 INCSF-499 INCSF-499	Issue astronation codentials for facility access Biorela facility access tank in termore any individual for whom access is no longer required Enforce physical access authorstances at entrylent points using devices and/or guards to verify individual activation authorstances and tags for entrylent points and frequently review as needed Novide and/guards to control access to publicly accessible areas within facility Provide and/guards to control access to publicly accessible areas within facility Provide and/guards to control access to publicly accessible areas within facility Provide and/guards to control access to publicly accessible areas within facility Provide and/guards to control access to publicly accessible areas within facility Entryle deparation to control access to publicly accessible areas within facility Entryle deparation to control access to publicly accessible areas within facility Entryle deparation to control access to publicly accessible areas within facility Entryle deparation to control access to publicly accessible areas within facility Entryle deparation and accessible to detects and response to physical access forces and areas mission Entryle and access to the facilities to detect and response to physical access forces are needs to facilities Protect pages and to and grower colling for information system from damage and destruction Provide the ability to and grower to information systems from damage and destruction Provide the ability for entryle most for the in the needs of a nemeroners Employ and maintain automatic accessificity maintain systems from damage and destruction Provide the ability of the entryle accessification accessification and prevent Employ and maintain automatic accessification and accessification accessification and accessive Employ and maintain automatic accessification acce	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational	11.1.2 11.2.3 11.1.2 11.2.3 11.2.2 11.2.2	CABLING SECURITY PHYSICAL ENTRY CONTROLS CABLING SECURITY SUPPORTING UTILITIES SUPPORTING UTILITIES	PE-3 PE-4 PE-5 PE-6 PE-8 PE-10 PE-10 PE-10 PE-10 PE-12 PE-14 PE-15 PE-16	PHYSICAL ACCESS CONTROL PHYSICAL ACCESS CONTROL CCCSS CONTROL FOR THANGHASSION MEDIUM ACCESS CONTROL FOR THANGHASSION MEDIUM ACCESS CONTROL FOR THANGHASSION MEDIUM MONTORING PHYSICAL ACCESS VISITOR ACCESS RECORDS PHYSICAL ACCESS CONTROL PROVER (AUGUMENT AND CABLING) BERESERVEY SUITORF BERESERVEY SUITORF BERESERVEY SUITORF BERESERVEY SUITORF TEMPERATURE AND HUMIDITY CONTROLS WATER DAMAGE PROTECTION BULKYET AND REMOVAL
NCSF-481 NCSF-482 NCSF-483 NCSF-485 NCSF-485 NCSF-485 NCSF-489 NCSF-490 NCSF-491 NCSF-492 NCSF-494 NCSF-494 NCSF-494 NCSF-495 NCSF-495	Issue astronation codentials for facility access Review Facility Rev	Foundational Foundational	11.12 11.23 11.12 11.23 11.22 11.22 11.22 11.21 11.21	CABLING SECURITY PHYSICAL ENTRY CONTROLS CABLING SECURITY SUPPORTING UTILITIES SUPPORTING UTILITIES EQUIPMENT STING AND PROTECTION DELIVERY AND LOADING AREAS	PE-3 PE-4 PE-5 PE-6 PE-6 PE-10 PE-10 PE-10 PE-11 PE-13 PE-13 PE-15	PHYSICAL ACCESS CONTROL PHYSICAL ACCESS CONTROL ACCESS CONTROL FOR TRANSMISSION MICHUM ACCESS CO
NCSF-481 NCSF-482 NCSF-483 NCSF-485 NCSF-485 NCSF-485 NCSF-489 NCSF-491 NCSF-492 NCSF-493 NCSF-493 NCSF-495 NCSF-496 NCSF-496 NCSF-496 NCSF-498 NCSF-499 NCSF-500	Issue astronation condensition for facility access Benefina Facility Benefina Facility access Benefina Facility Benefina Facility Benefina Facility Benefina Facility Benefina Benefina Facility Benef	Foundational	11.12 11.23 11.12 11.23 11.22 11.22 11.21	CABLING SECURITY PHYSICAL ENTRY CONTROLS CABLING SECURITY SUPPORTING UTILITIES SUPPORTING UTILITIES EQUIPMENT STING AND PHOTECTION	PE-3 PE-4 PE-5 PE-6 PE-6 PE-10 PE-10 PE-11 PE-12 PE-13 PE-14 PE-15 PE-16 PE-17	PHYSICAL ACCESS CONTROL PHYSICAL ACCESS CONTROL ACCESS CONTROL FOR TRANSMISSION MEDIUM ACCESS CONTROL FOR TRANSMISSION MEDIUM ACCESS CONTROL FOR TRANSMISSION MEDIUM ACCESS CONTROL FOR OUTPUT PERCESS VISITOR ACCESS BECORES VISITOR ACCESS BECORES VISITOR ACCESS BECORES VISITOR ACCESS BECORES BERGENCY TOWNE BERGENCY SUITOFF EMERGENCY TOWNE BERGENCY TOW
NCSF-481 NCSF-483 NCSF-485 NCSF-485 NCSF-486 NCSF-486 NCSF-487 NCSF-489 NCSF-490 NCSF-491 NCSF-492 NCSF-493 NCSF-494 NCSF-495 NCSF-495 NCSF-502 NCSF-503 NCSF-504 NCSF-504	Issue astronation coelestials for facility access Benefa facility access authorizations at entryleat points using devices and/or guards to verify individual activations authorizations at entryleat points using devices and/or guards to verify individual activations applysical access audits togs for entryleat points and frequently verifies an ended Novies affigurant is control access to publicly accessible areas within facility howles defigurants to control access to publicly accessible areas within facility howles defigurants to control access to publicly accessible areas within facility howles defigurants to control access to publicly accessible areas within facility through any deparation to control access to publicly accessible areas within facility accessible accessible accessible accession and access points and the application access devices and transmission less factored behavior accessible accessible accessible accessible accessible and transmission less Control abrival accessible to device and excession to phylical accessible accession access recents to facilitate Notes to phylical access to the facilitate to device and excession accession accession accession accessible and accession accessible and accession accessible and accession accession accession accessible and accession accessio	Foundational Found	11.12 11.23 11.12 11.23 11.22 11.22 11.22 11.21 11.16 11.11 11.12 11.15	CABLING SECURITY PHYSICAL ENTRY CONTROLS CABLING SECURITY SUPPORTING UTILITIES SUPPORTING UTILITIES EQUIPMENT SITING AND PROTECTION DELIVERY AND LOADING AREAS PHYSICAL SECURITY VERMETER PHYSICAL MITRY CONTROLS	PE-3 PE-4 PE-5 PE-6 PE-6 PE-10 PE-10 PE-11 PE-12 PE-13 PE-14 PE-15 PE-16 PE-17	PHYSICAL ACCESS CONTROL PHYSICAL ACCESS CONTROL ACCESS CONTROL FOR TRANSMISSION MEDIUM ACCESS CONTROL FOR TRANSMISSION MEDIUM ACCESS CONTROL FOR TRANSMISSION MEDIUM ACCESS CONTROL FOR OUTPUT PERCESS VISITOR ACCESS BECORES VISITOR ACCESS BECORES VISITOR ACCESS BECORES VISITOR ACCESS BECORES BERGENCY TOWNE BERGENCY SUITOFF EMERGENCY TOWNE BERGENCY TOW
NCSF-481 NCSF-482 NCSF-482 NCSF-485 NCSF-485 NCSF-486 NCSF-489 NCSF-489 NCSF-491 NCSF-491 NCSF-491 NCSF-493 NCSF-494 NCSF-493 NCSF-498 NCSF-498 NCSF-491 NCSF-501 NCSF-501 NCSF-503 NCSF-503	Issue astronation condensition for facility access facility access a final long access is no longer required facility access and/or paces to the formation facility access and/or paces to the formation facility access and/or paces to the facility access facility access and/or paces facility access and/or paces facility access facility access facility access facility access facility access facility fa	Foundational Found	11.12 11.23 11.12 11.23 11.22 11.22 11.21 11.16 11.11	CABLING SECURITY PHYSICAL ENTRY CONTROLS CABLING SECURITY SUPPORTING UTULITIES SUPPORTING UTULITIES EQUIPMENT STING AND PROTECTION DELIVERY AND LOADING AREAS PHYSICAL ENTRY CONTROLS	PE-3 PE-4 PE-5 PE-6 PE-6 PE-10 PE-10 PE-11 PE-12 PE-13 PE-14 PE-15 PE-16 PE-17	PHYSICAL ACCESS CONTROL PHYSICAL ACCESS CONTROL ACCESS CONTROL FOR DIARAMENSION MEDIUM ACCESS CONTROL FOR DIARAMENSION MEDIUM ACCESS CONTROL FOR DIARAMENSION MEDIUM ACCESS ACCESS BECORE WINTON ACCESS BECORE WINTON ACCESS BECORE WINTON ACCESS BECORE BENERATIVE SUITORF BENERATIVE VIEWTORF BENERATIVE VIEWTORF HER PROTECTION TEMPERATURE AND HUMODITY CONTROLS WINTE RAMAGE REDICTION DELIVERY AND EMMORIAL ALTERNATE WORK STE

JNCSF-507		
	Ensure individuals understand and formally acknowledge the behavior expectations regarding information system usage	Foundational
JNCSF-508	Implement and utilize campaigns and booklets to raise awareness about information security in the	Foundational
JNCSF-509	organization Review and update behavior rules frequently and ensure individuals understand new rules	Foundational
JNCSF-510	Review and re-educate individuals on appropriate skills, qualifications, and security behavior	Foundational
JNCSF-511	Assign a risk designation to all organizational positions, and frequently review and update the designations	Foundational
JNCSF-512	Establish a process to screen all individuals filling organizational positions	Foundational
JNCSF-513	Screen individuals prior to authorizing access to the information system	Foundational
JNCSF-514	Rescreen individuals after certain organization-defined conditions are met	Foundational
JNCSF-515	Revoke all authenticators and security-related information system-related property upon termination of employment	Foundational
JNCSF-516	Conduct exit interviews to discuss necessary information security topics with individuals upon termination	Foundational
	of employment	
JNCSF-517	Retain access to organizational information and information systems controlled by terminated individuals	Foundational
JNCSF-518 INCSE-519	Soecify ownership of information, trade secrets, and intellectual property in non-disclosure agreements Specify actions to be taken in case of a breach of non-disclosure agreements	Foundational
INCSF-520	Specify actions to be taken in case of a preach of non-disclosure agreements Specify permitted use of confidential information and rights of signatories to use information in non-	Foundational
	disclosure agreements Review and modify access authorizations to information systems/facilities upon transferal of individuals	
JNCSF-521	Review and modify access authorizations to information systems/facilities upon transferal of individuals within the organization	Foundational
JNCSF-522	Identify and communicate to individuals being terminated or transferred within the organization any	Foundational
JNCSF-523	changes in access authorizations to information systems and/or facilities Initiate any necessary transfer actions upon transferal of individuals (e.g., returning and issuing new ID	Foundational
INCSF-523	cards, changing authorizations)	Foundational
INCSF-524	Develop and document user access agreements for information systems	Foundational
INCSF-525	Establish and document third-party personnel security requirements including security roles and	Foundational
	responsibilities	
JNCSF-526	Require third-party providers to comply with personnel security requirements	Foundational
INCSF-527	Require third-party providers to notify the organization of third-party personnel transfers with information system privileges/credentials	Foundational
INCSF-528	Employ a sanctions process when individuals do not comply with information security policies	Foundational
INCSF-529	Notify appropriate personnel of any employee sanctions processes taking place and the reason for the	Foundational
INCSE-530	sanction Conduct background checks of prospective employees requiring character references and verification of	Foundational
INCSF-530	professional and academic qualifications	roundational
INCSF-531	Conduct background checks of prospective employees requiring identity verification and review of criminal records	Foundational
INCSF-532	Ensure access agreements state the employee's legal responsibilities and rights	Foundational
NCSF-533 NCSF-534	Ensure access agreements state acceptable use of information and organizational assets Ensure access agreements state acceptable use of third-party information	Foundational Foundational
NCSF-535	Ensure access agreements state consequences for disregarding the organization's security requirements	Foundational
NCSF-536	Categorize information and information systems in accordance to applicable laws and policies to describe adverse impacts of information being compromised	Foundational
NCSF-537	Document and explain in security plans how security categorizations of information and information	Foundational
	systems reflect any adverse impacts of compromised information	
INCSF-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
INCSF-539 INCSF-540	Document risk assessment results and disseminate results to appropriate personnel Review risk assessment results at frequent intervals	Foundational Foundational
INCSF-540	Review risk assessment results at requent intervals Update risk assessments after significant changes to information systems occur, or other organization-	Foundational
JNCSF-541	defined conditions are met	Foundational
	Utilize risk assessment results to determine which security and/or physical controls should be implemented	
INCSF-542		Foundational
	Conduct risk assessments at three levels: organization, mission/business process, and information system level	Foundational
INCSF-543	Conduct risk assessments at three levels: organization, mission/business process, and information system level Create acquisition contracts for information systems including security functional, strength, and assurance	
INCSF-543 INCSF-544	Conduct risk assessments at three levels: organization, mission/business process, and information system level	Foundational
INCSF-543 INCSF-544 INCSF-545	Conduct risk assessments at three levels: organization, mission/business process, and information system level Costex acquisition contracts for information systems including security functional, strength, and assurance reasonments and information system acquisition contracts.	Foundational
INCSF-543 INCSF-544 INCSF-545	Conduct risk sussements at three levels: organization, mission/business process, and information system level Create acquisitions contracts for information systems including security functional, strength, and assurance requirements. Include security-related accumentation requirements for protecting such documentation in all information system acquisitions contracts.	Foundational
NCSF-543 NCSF-544 NCSF-545 NCSF-546	Conduct risk assessments at three levels: organization, mission/business process, and information system level Costex acquisition contracts for information systems including security functional, strength, and assurance reasonments and information system acquisition contracts.	Foundational Foundational Foundational
NCSF-543 NCSF-544 NCSF-545 NCSF-546 NCSF-547	Conduct risk susessments at three levels: organization, mission/business process, and information system level Center acquisition contracts for information systems including security functional, strength, and assurance requirements louidar security-resolution requirements and requirements for protecting such documentation inducts as description of Information system development environments in al Information system acquisitions contracts	Foundational Foundational Foundational
NCSF-543 NCSF-544 NCSF-545 NCSF-546 NCSF-547 NCSF-548	Conduct risk assessments at three levels: organization, mission/business process, and information system level Cente acquisition: contracts for information systems including security functional, strength, and assumace requirements includie as each right or information organizements and requirements for protecting such documentation in all information system acquisition contracts includies a each right on information system acquisition contracts includies accurring to information system acquisition contracts includies accurring to information system acquisition contracts includies accurring to within organics of management reprosellishings for contracting the transmission, stabilish agreements with right artic of management reprosellishings for contracting the transmission,	Foundational Foundational Foundational Foundational Foundational
INCSF-543 INCSF-544 INCSF-545 INCSF-546 INCSF-547 INCSF-548 INCSF-549	Conduct risk assessments at three levels: organization, mission/business process, and information systems level Costes acquisition contracts for information systems including security functional, strength, and assurance reaurements and an information system acquisition contracts. Include a description of information system development environments in al information system acquisition contracts. Include security accurity requirements and information system acquisition contracts. Include security accurity requirements and information system acquisition contracts. Exability agreements with bird gatte of management reponsibilities for controlling the transmission, digatch, and receipt o faulons information.	Foundational Foundational Foundational Foundational Foundational Foundational
INCSF-543 INCSF-544 INCSF-545 INCSF-546 INCSF-547 INCSF-548 INCSF-549	Conduct risk susements at three levels: organization, mission/business process, and information systems level. Center acquisition contracts for information systems including security functional, strength, and assumce requirements include security-rotated accumentation requirements and requirements for protecting such documentation includes security-rotated accumentation contracts. Include security-rotated accumentation requirements and requirements in all information system acquisition contracts. Include security-rotated information systems acquisition contracts. Include security-requirements in all information system acquisition contracts. Include security-requirements in all information system acquisition contracts. Exability agreements with third parties of procedures to ensure traceability and non-regulation of transferred basiness formation.	Foundational Foundational Foundational Foundational Foundational
NCSF-543 NCSF-544 NCSF-545 NCSF-546 NCSF-547 NCSF-548 NCSF-549 NCSF-550	Conduct risk assessments at three levels: organization, mission/business process, and information systems level Contex acquisition contracts for information systems including security functional, strength, and assurance trackets accurity-related documentation requirements and requirements for protecting such documentation in all information systems acquisition contracts include accuration of information system development environments in all information system acquisations contracts include accurates contracts in all information system acquisition contracts Exability agreements with hird parties of management reponsibilities for contening the transmission, detacht, and receipt requirements in all information system acquisations contracts Exability agreements with hird parties of the minimum packing balance and management reponsibilities for contening the transmission, Exability agreements with hird parties of the minimum packing balance and the minimum darket balance and the source of the context is transmission of Exability agreements with hird parties of the minimum packing balance and the regulations transmission for the source of the context is the source of the minimum packing balance and the source to accessibility and non-regulation than the source of the source	Foundational Foundational Foundational Foundational Foundational Foundational
NCSF-543 NCSF-544 NCSF-545 NCSF-546 NCSF-547 NCSF-549 NCSF-549 NCSF-550	Conduct risk assessments at three levels: organization, mission/business process, and information systems level Contex acquisition contracts for information systems including security functional, strength, and assurance maximumos. In all information system acquisition contracts include a description of information system development environments in all information system acquisition contracts include a description of information system development environments in all information system acquisition contracts include a description of information system acquisition contracts include description of information system acquisition contracts Exability agreements with third parties of management regressibilities for controlling the traumission, dutach, and receipt requirements in all information system Exability agreements with third parties of management regressibilities and traumission and and for Exability agreements with third parties of measure systems for trauteries busines information explores thermation.	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational
NCSF-543 NCSF-544 NCSF-545 NCSF-546 NCSF-547 NCSF-548 NCSF-549 NCSF-550 NCSF-551 NCSF-551	Conduct risk assessments at three levels: organization, mission/business process, and information systems including security functional, strength, and assurance conservations contracts for information systems including security functional, strength, and assurance and assessments and the security related documentation in a similar metal organization contracts include a security on of information system development environments in all information systems adjustices contracts. There is all information system acquisition contracts. Include is derived environ requirements in all information system acquisitions contracts. Exability agreements with hird partice of management trapeopublistics for contracts. Exability agreements with hird partice of the minimum packing, labeling, and transmission, attability agreements with hird partice of the minimum packing. Useling, and transmission and/ord for transformed business information for advectory providences of the minimum packing. Useling, and transmission attabulated for transformed business information for advectory partices and the executive protection measures for transformed business information (accurate system).	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational
NCSF-543 NCSF-544 NCSF-545 NCSF-546 NCSF-547 NCSF-548 NCSF-549 NCSF-550 NCSF-551 NCSF-551	Conduct risk assessments at three levels: organization, mission/business process, and information systems level Contex acquisition contracts for information systems including security functional, strength, and assurance maximumos. In all information system acquisition contracts include a description of information system development environments in all information system acquisition contracts include a description of information system development environments in all information system acquisition contracts include a description of information system acquisition contracts include description of information system acquisition contracts Exability agreements with third parties of management regressibilities for controlling the traumission, dutach, and receipt requirements in all information system Exability agreements with third parties of management regressibilities and traumission and and for Exability agreements with third parties of measure systems for trauteries busines information explores thermation.	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational
NCSF-543 NCSF-544 NCSF-545 NCSF-546 NCSF-547 NCSF-549 NCSF-550 NCSF-551 NCSF-552 NCSF-552	Conduct risk susements at three levels: organization, mission/business process, and information systems level. Center acquitation contracts for information systems including security functional, strength, and assumce requirements. Include security-rotated accumentation requirements and requirements for protecting such documentation acquirements. Include security-rotated accumentation requirements and information system acquiration contracts. Include security-rotated accumentation requirements in all information system acquiration contracts. Include security-rotated accumentation requirements in all information system acquiration contracts. Include security-rotated resources and information system acquirations and the security requirements in all information system acquirations and the security requirements in all information system acquirations and here a discuss a information tradeoling agreements with hird parties of procedures to ensure traceability and non-requiration of tradeoling agreements with hird parties of procedures to meanse for transformation Exabiling agreements with hird parties of processary protection measures for transformed business information Exabiling agreements with hird parties of processary protection measures for transformed business information accuments and processary protection measures for transformed business information (e.g., current transformed business) and the second processary protection measures for transformed business information (e.g., current transformed business) and the second processary protection measures for transformed business information (e.g., current transformed business) and the second processary protection measures for transformed business) and transformed business and transformed business information (e.g., current business and transformed business) and transformed and transformed business and transformed and transformed and transformed and transformed and transformed and transformed and transformed and transform	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational
NCSF-543 NCSF-544 NCSF-545 NCSF-546 NCSF-547 NCSF-549 NCSF-550 NCSF-551 NCSF-551 NCSF-552 NCSF-553 NCSF-553	Conduct risk assessments at three levels: organization, mission/business process, and information systems level Contex acquisition: contracts for information systems including security functional, strength, and assurance realize accurity related documentation requirements and requirements for protecting such documentation in al information system acquisition contracts include a description of information system acquisition contracts include accurity requirements in all information system acquisitions contracts. Exability agreements with third parties of management reprosmalities for contenting the transmission, disatch, and receipt requirements in all information system acquisitions contracts. Exability agreements with third parties of the minimum packing, labeling, and transmission, disatch, and receipt with the diparties of necessary protection measures for transferred business information (i.e., contacquisition) of the ensures of transferred business information (i.e., contacquisition).	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational
NCSF-543 NCSF-544 NCSF-545 NCSF-546 NCSF-547 NCSF-548 NCSF-550 NCSF-550 NCSF-551 NCSF-552 NCSF-553 NCSF-553 NCSF-555	Conduct risk susements at three levels: organization, mission/business process, and information systems level. Center acquitation contracts for information systems including security functional, strength, and assumce requirements. Include security-rotated accumentation requirements and requirements for protecting such documentation acquirements. Include security-rotated accumentation requirements and information system acquiration contracts. Include security-rotated accumentation requirements in all information system acquiration contracts. Include security-rotated accumentation requirements in all information system acquiration contracts. Include security-rotated resources and information system acquirations and the security requirements in all information system acquirations and the security requirements in all information system acquirations and here a discuss a information tradeoling agreements with hird parties of procedures to ensure traceability and non-requiration of tradeoling agreements with hird parties of procedures to meanse for transformation Exabiling agreements with hird parties of processary protection measures for transformed business information Exabiling agreements with hird parties of processary protection measures for transformed business information accuments and processary protection measures for transformed business information (e.g., current transformed business) and the second processary protection measures for transformed business information (e.g., current transformed business) and the second processary protection measures for transformed business information (e.g., current transformed business) and the second processary protection measures for transformed business) and transformed business and transformed business information (e.g., current business and transformed business) and transformed and transformed business and transformed and transformed and transformed and transformed and transformed and transformed and transformed and transform	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational
NCSF-543 NCSF-544 NCSF-546 NCSF-546 NCSF-547 NCSF-548 NCSF-550 NCSF-551 NCSF-551 NCSF-552 NCSF-553 NCSF-553 NCSF-555 NCSF-555 NCSF-555	Conduct risk assessments at three levels: organization, mission/business process, and information systems level Contex acquisition: contracts for information systems including security functional, strength, and assurance realize accurity related documentation requirements and requirements for protecting such documentation in al information system acquisition contracts include a description of information system acquisition contracts include accurity requirements in all information system acquisitions contracts. Exability agreements with third parties of management reprosmalities for contenting the transmission, disatch, and receipt requirements in all information system acquisitions contracts. Exability agreements with third parties of the minimum packing, labeling, and transmission, disatch, and receipt with the diparties of necessary protection measures for transferred business information (i.e., contacquisition) of the ensures of transferred business information (i.e., contacquisition).	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational
NCSF-543 NCSF-544 NCSF-546 NCSF-546 NCSF-547 NCSF-548 NCSF-550 NCSF-551 NCSF-551 NCSF-552 NCSF-553 NCSF-553 NCSF-555 NCSF-555 NCSF-555	Conduct risk assessments at three levels: organization, mission/business process, and information systems level Costex acquitation contracts for information systems including security functional, strength, and assurance reasonershi. Include a description of information system development environments in al information system acquitation contracts. Include a description of information system development environments in al information system acquitation contracts. Include description of information system development environments in al information system acquitation contracts. Exabiling agreements with hird parties of management reprosmolities for controlling the transmission, dudgets, and receipt requirements and information system. Exabiling agreements with hird parties of necessary protocion measures for transferred business information (e.e., crystograph). Exabiling agreements taking for personnel interacting with hird party personnel regarding apoppisate information (e.e., crystograph). Exabiling agreements taking for personnel interacting with hird party personnel regarding apoppisate information (e.e., crystograph). Exabiling agreements taking for personnel interacting with hird party sectores. Exabiling agreements taking for personnel interacting with hird party sectores.	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational
NCSF-543 NCSF-544 NCSF-545 NCSF-546 NCSF-547 NCSF-547 NCSF-549 NCSF-550 NCSF-551 NCSF-552 NCSF-553 NCSF-553 NCSF-555 NCSF-555 NCSF-555 NCSF-556 NCSF-557	Conduct risk assessments at three levels: organization, mission/business process, and information systems level. Constructions and the constructs for information systems including security functional, strength, and assurance constructions and the constructs for information system sincluding security functional, attempts and assurance include according on information system development environments in all information systems advalations: contracts. Include is according environments in all information systems acquisition contracts. Exability agreements with third partice of management proposabilities for controling the transmission, display agreements with third partice of the management transmittion of transformed business information of transformed business information of transformed business information information systems acquisition contracts. Exability agreements with third partice of the minimum packing, bubling, and transmission, display and the system information in the example systems the systems and advalation transformed business information information systems acquisition measures for transformed business ficability agreements variability implement agreements training for personnel interacting with third party personnel regarding appropriate business ficability in agreements training for personnel interacting with third party personnel regarding appropriate business includent includent management requirements and training with third parts includent includent management requirements and training market to currentices, systems, Manage and re-assessional advancessional advancessional advancessional advancessional advancessionadvancessionadvancessionadvancessionadvancessionadvancessionad	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational
NCSF-543 NCSF-544 NCSF-545 NCSF-546 NCSF-547 NCSF-547 NCSF-549 NCSF-550 NCSF-551 NCSF-552 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-556 NCSF-557 NCSF-558	Conduct risk assessments at three levels: organization, mission/business process, and information systems level. Contra acquires constructs for information systems including security functional, strength, and aurance and a security related documentation requirements and requirements for protecting such documentation in all information systems acquires on contracts. Include a accuration of information system development environments in all information system acquires accurates on the security of the systems acquires on the system acquires accurates on the size of the system acquires on the system acquires on the system acquires on the system acquires on contracts. Establish agreements with their parties of management reponsibilities for controlling the transmission, disades, and records the channels on the system acquires on the system acquires on transformed business information constructed business information on the system acquires on the system acquires on transformed business information. Establish agreements, with their parties of the messary protection measures for transformed business information business information. Establish document, and implement legal regulatory requirements with their parties (e.g., intellectual protector y data): Implement acquires to acquerements and transmission durates to the index of the system in the system acquires on the system acquires on the system in colons in management requirements and transmission standards for transformed business information. Establish document, and implement legal regulatory requirements with their parties (e.g., intellectual protector y data): Implement agreements with their parties and all processes and controls in applement advectors to the system is the system and the system acquires on the system information makes to accurate system. The system is the system acquires on the system acq	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational
INCSF-543 INCSF-544 INCSF-545 INCSF-546 INCSF-547 INCSF-549 INCSF-550 INCSF-551 INCSF-552 INCSF-553 INCSF-555 INCSF-555 INCSF-556 INCSF-557 INCSF-558 INCSF-559	Conduct risk assessments at three levels: organization, mission/business process, and information systems level. Center acquintion contracts for information systems including security functional, strength, and assurance reautometers. Include a description of information system acquinements for protecting such documentation in al information system acquintion contracts. Include a description of information system acquintion contracts. Include security accurity requirements in al information system acquintion contracts biological activity and assurance information system acquintion contracts. Include security accurity requirements in al information system acquintion contracts. Exability agreements with third parties of management repressibilities for controlling the traumission, dutatch, and receips formation. Exability agreements with third parties of management repressibilities for controlling the traumission, dutatch, and receips training for personnel interacting with third parties information (e.e., crystomation). Exability agreements training for personnel interacting with third parties information (e.e., crystomation). Exability agreements training for personnel interacting with third parties for controlling appropriate backness training for personnel interacting with third parties. Implement aurone a personnel interacting with third parties. Implement states training for personnel interacting with third parties. Implement and and the partenets the training with third parties. Implement advectors intra account of parties to advised and training with third parties. Takatas en volvance and the partenets on training with third parties. Takatas environ the partenets the training the personnel regarding appropriate Manage on volvance intra account parties and part	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational
INCSF-543 INCSF-544 INCSF-545 INCSF-546 INCSF-547 INCSF-549 INCSF-550 INCSF-551 INCSF-552 INCSF-553 INCSF-555 INCSF-555 INCSF-556 INCSF-557 INCSF-558 INCSF-559	Conduct risk assessments at three levels: organization, mission/business process, and information systems level. Contra acquires constructs for information systems including security functional, strength, and aurance and a security related documentation requirements and requirements for protecting such documentation in all information systems acquires on contracts. Include a accuration of information system development environments in all information system acquires accurates on the security of the systems acquires on the system acquires accurates on the size of the system acquires on the system acquires on the system acquires on the system acquires on contracts. Establish agreements with their parties of management reponsibilities for controlling the transmission, disades, and records the channels on the system acquires on the system acquires on transformed business information constructed business information on the system acquires on the system acquires on transformed business information. Establish agreements, with their parties of the messary protection measures for transformed business information business information. Establish document, and implement legal regulatory requirements with their parties (e.g., intellectual protector y data): Implement acquires to acquerements and transmission durates to the index of the system in the system acquires on the system acquires on the system in colons in management requirements and transmission standards for transformed business information. Establish document, and implement legal regulatory requirements with their parties (e.g., intellectual protector y data): Implement agreements with their parties and all processes and controls in applement advectors to the system is the system and the system acquires on the system information makes to accurate system. The system is the system acquires on the system acq	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational
INCSF-543 INCSF-544 INCSF-545 INCSF-546 INCSF-547 INCSF-549 INCSF-549 INCSF-550 INCSF-551 INCSF-551 INCSF-553 INCSF-553 INCSF-553 INCSF-555 INCSF-556 INCSF-557 INCSF-558 INCSF-558 INCSF-558 INCSF-559 INCSF-560	Conduct risk assessments at three levels: organization, mission/business process, and information systems level. Conservations: Constructs for information systems including security functional, strength, and aurance and a security related documentation requirements and requirements for protecting such documentation is all information systems acquisition constructs. Include accurity related documentation requirements and requirements in all information system acquisition constructs. Include accurity requirements in all information system acquisition constructs. Tables and a security requirements in all information system acquisition constructs. Exabilish agreements, with hird parties of macagement traponosibilities for constructing the transmission, catabilish agreements with hird parties of procedures to ensure traceability and non-regulation of transformed basiness information. Exabilish agreements with hird parties of proceedures to ensure traceability and non-regulation of transformed basiness information. Exabilish agreements with hird parties of proceedures to ensure traceability and non-regulation of transformation (accurry organization). Exabilish agreements with hird parties of proceedures to ensure traceability and non-regulation for adverse basiness information. Examples agreements that hird parties of proceedures to ensure that transmission, displant transformed and informant legal regulatory requirements with hird parties of ensures and transformed to agreement legal regulatory requirements and control Manage and re-assession adverse to audvisit all processes and controls. Manage and re-assession agreement requirements and controls Manage and re-assession adverse to audvisit all processes and controls and graves and procession. Exploring control agreements with hird parties and re-assess any new risks a spoporties and procession. Explores that baseling scheme that hird parties and re-assess any new risks as appropriate displants and procesion.	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational
NCSF-543 NCSF-545 NCSF-545 NCSF-545 NCSF-545 NCSF-554 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-555	Conduct risk assessments at three levels: organization, mission/business process, and information systems level accounts constructs for information systems including security functional, strength, and aurance active accounts of the mission system sincluding security functional, strength, and aurance information systems acquisition constructs. Include a description of information system development environments in all information system acquisitions constructs. Include accounts of the one of the one acquisitions constructs. Exability agreements with third parties of management reprovabilities for contenting the transmission, duals duals, and receive the observation of the one of the one of the one of the one transformed bases information Exability agreements with third parties of the minimum packing, labeling, and transmission standards for transformed basiness information Exability agreements with the parties of the ensure transmission standards for transformed bases information to the one of the one of the one of the one information of the one of the one of the one of the one of the one information of the one of the one information of the one of the one of the one of the one of the one information of the one of the one of the one of the one of the one information of the one of the one of the one of the one of the one information of the one of the one of the one of the one of the one information of the one of the one of the one of the one of the one information of the one of the one of the one of the one of the one information of the one of the one of the one of the one of the one information of the one of the one of the one of the one of the one information of the one of the one information of the one of the one information of the one of the one of the one of the one of the one information of the one of the one of t	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational
NCSF-543 NCSF-545 NCSF-545 NCSF-545 NCSF-547 NCSF-548 NCSF-559 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-556 NCSF-556	Conduct risk assessments at three levels: organization, mission/business process, and Information systems level. Center acquints contracts for information systems including security functional, strength, and assurance reasons and a security of accumentation requirements and requirements for protecting such documentation in all information system development environments in all information system acquination contracts. Include settledise exercision requirements and information system acquination contracts. Include settledise exercision requirements and information system acquination contracts. Exabilin agreements with hird parties of information system acquinotion contracts. Exabilin agreements with hird parties of neargament reproposibilities for controlling the transmission, durated, and receipt requirements in all information system acquination contracts with hird parties of neargament reproposibilities for controlling the transmission facilities information in the system of the system acquirements with hird parties of transformed business information. Exabiling agreements with hird parties of neargament protection measures for transformed business information (<i>e.g.</i> , crystograph)). Insplement includent management requirements and training with hird parties (<i>e.g.</i> , intellectual protection). Exabiling agreements with hird parties to add all process and controls Manage and re-assess risks associated with any changes the organization makes to current services, sptems, <i>explores</i> regulaters. Manage and re-assess risks sanceidade with any changes the organization makes to current services, sptems, and and associated and the parties of a transformed business information applicated and controls of filter business information. Require current services strates business functions. Require current development to the information of a transported filter services, sptems, <i>analosis</i> and <i>approcel</i> justification for the current week of a disconse and control efficiency verification filter applicates, correction, associate	Foundational Foundational
NCSF-543 NCSF-545 NCSF-545 NCSF-545 NCSF-545 NCSF-554 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-555	Conduct risk assessments at three levels: organization, mission/business process, and Information systems level. Constructions of the constructs for information systems including security functional, strength, and aurance and a security related documentation requirements and requirements for protecting such documentation is all information systems documentations and information systems acuitation contracts. Totale according to information system documents and information system acuitation contracts. Totale according to information system documents and information system acuitation contracts. Tabulaki agreements with hird parties of management requirements for protecting the transmission, displays and the all information system documents to a system acuitation contracts. Tabulaki agreements with hird parties of the magement requirements and information system acuitation contracts with the parties of the magement requirements and the action transformed business information. Tabulaki agreements with hird parties of the messary protection measures for transformed business therability agreements with hird parties of the messary protection measures for transformed business therability agreements with hird parties of the messary protection measures for transformed business transformed business information. Tabulaki, document, and memory tagel interacting with hird parties transformed business transformed business information acuitation acut acut acuts the parties includent transagement requirements and transmission administion agreement and parties the size acut acuts with hird parties and a substance and transmission, administion and parties in tabulation agreements and transmission administion acuts and parties in tabulation the substance and transmission administion application agreement to adverse the there are a substance and transmission administion application agreement adverse to the information applicable laws and control efficiency verification and the adverse to agreements inductions for the acontrubut and	Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational Foundational
NCSF-543 NCSF-545 NCSF-545 NCSF-545 NCSF-547 NCSF-548 NCSF-548 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-556 NCSF-556 NCSF-556 NCSF-556 NCSF-556	Conduct risk assessments at three levels: organization, mission/business process, and information systems includes acquires contracts for information systems including security functional, strength, and assumance regularismotic. Include a description of information system acquirements and requirements for protecting such documentation is al information system acquires contracts. Include additional execution contracts. Include additional execution contracts. Exabiling agreements with hird parties of management reproprohilities for controlling the transmission, durates, and execution contracts information system acquires controlling the transmission, durates, and execution contracts. Exabiling agreements with hird parties of management reproprohilities for controlling the transmission, durates, and execution formations of the minimum packing, labeling, and transmission, advanced for transferred basiness information acquires basiness information on the minimum packing, labeling, and transmission acquires information (e.e., crystograph). Implement aurencess training for personnel interacting with hird parties for controlling the transmission acquires basiness information on the minimum packing, labeling, and transmission acquires information (e.e., crystograph). Implement aurencess training for personnel interacting with hird parties (e.g., intellectual property relation). Implement acquires training that the durates and the garties to controlls Manage and changes index acquires and the same were shifted and parties (e.g., intellectual manage and changes index acquires and the same stress required in information acquired a subscience in the acquires the organization makes to current envices, systems, originates acquires, controls, and environal subscience in the actual stress required in information acquires acquires, controls, and environal subscience information interaction facilities that accurred developes to terma compliant with bapilicable laws and control efficiency verification Provide documented and approv	Foundational Found
NCSF-543 NCSF-545 NCSF-545 NCSF-546 NCSF-547 NCSF-547 NCSF-553 NCSF-553 NCSF-553 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-556 NCSF-557 NCSF-556 NCSF-556 NCSF-556 NCSF-556 NCSF-557 NCSF-556 NCSF-557 NCSF-556 NCSF-557 NCSF-556 NCSF-557 NCSF-556 NCSF-557 NCSF-556 NCSF-557 NCSF-556 NCSF-557 NCSF-556 NCSF-557 NCSF-556 NCSF-557 NCSF-556 NCSF-557 NCSF-556 NCSF-557 NCSF-556 NCSF-557 NCSF-556 NCSF-556 NCSF-557 NCSF-556 NCSF-557 NCSF-556 NCS	Conduct risk assessments at three levels: organization, mission/business process, and Information systems includes assessments at three levels: organization, mission/business process, and Information systems and constructs for information systems including security functional, strength, and aurance and assessments and the magnituments and requirements for protecting such documentation is all information systems may advance on constructs. Include advances of information system development environments in all information system advances of information system development environments in all information system advances of information system advances on constructs. Tables in a landom termination in the system advances of the system advances of the system advances on the system advances of the system advances of the system advances of the system advances of the system advances of the system advances of the system advances of the system advances of the system advances of the system advances of the system advances of the system advances information information (see, constructs). Intellenter advances information advances of the system advances of the system advances information information (see, constructs). Intellenter advances information advances of the system advances of the advances information (see, constructs). Intellenter advances information information (see, constructs). Manage and re-assess information advances of advances the big regulatory requirements with third parties (see, intellectual constructs). Manage and re-assess in advances to advances to controls Manage and re-assess advances to advances in the system advances to controls Manage and re-assess advances to advances of the information avances opporting childra during constructs and control efficiency verification avances opporting childra during construction in the construct advances advances to advances opporting childra during construction in the information service information security constructs and controls efficiency verification information	Foundational Foundational
NCSF-543 NCSF-545 NCSF-545 NCSF-545 NCSF-547 NCSF-548 NCSF-548 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-555 NCSF-556 NCSF-556 NCSF-556 NCSF-556 NCSF-556	Conduct risk assessments at three levels: organization, mission/business process, and information systems level. Contra acquisition contracts for information systems including security functional, strength, and aurance and activation contracts for information systems including security functional, strength, and aurance and a decorption of information system development environments in all information systems acquisition contracts. Unclude activities contracts. Establish agreements with third parties of management regionabilities for controlling the transmission, disease and the system activities contracts. Establish agreements with third parties of message protoching and transmission diseases, and receive the observation of the system acquisition contracts. Establish agreements with third parties of message protoching that the system acquisition contracts. Establish agreements with third parties of message protoching and transmission diseases information. Establish document, with third parties of message protoching with third parties (e.g., intellectual protoching the system strength and the system strength agreement with third parties incoment with the parties of the development with third parties (e.g., intellectual protoching the system strength and the system strength and the parties (e.g., intellectual protoching the system strength and the system strength and the parties (e.g., intellectual protoching the system strength and the system strength agreements with the system insplement agreements with the parties and ensuits and control efficiency werification to agreement strengths functions functions and control efficiency werification protoching the system strength and the system strength and control efficiency werification transformed and approved justification (relates used on supported system components that allow the protoching the system strength and control efficiency werification to approve document to active assisted with the intercenting used the system strength in formation system strength and th	Foundational Found

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		
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		
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
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		
JNCSF-568	Obtain legal opinion with regard to information system monitoring activities as appropriate	Foundational		
JNCSF-569	Provide information system monitoring information to defined personnel as needed	Foundational		
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

 7.2.1
 MANAGEMENT RESPONSIBILITIES

 7.2.2
 INFORMATION SECURITY AWARENESS. EDUCATION AND TRAINING

 7.2.2
 INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING

SCREENING SCREENING SECURE DEVELOPMENT ENVIRONMENT 8.1.4 RETURN OF ASSETS
 13.2.4 CONFIDENTIALITY OR NONDISCLOSURE AGREEMENTS

CONFIDENTIALITY OR NONDISCLOSURE AGREEMENTS

CONFIDENTIALITY OR NONDISCLOSURE AGREEMENTS CONFIDENTIALITY OR NONDISCLOSURE AGREEMENTS CONFIDENTIALITY OR NONDISCLOSURE AGREEMENTS

13.2.4 CONFIDENTIALITY OR NONDISCLOSURE AGREEMENTS 7.1.2 TERMS AND CONDITIONS OF EMPLOYMENT

DISCIPLINARY PROCESS

SCREENING

 8.1.3
 ACCEPTABLE USE OF ASSETS

 15.1.2
 ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS

TERMS AND CONDITIONS OF EMPLOYMENT TERMS AND CONDITIONS OF EMPLOYMENT TERMS AND CONDITIONS OF EMPLOYMENT TERMS AND CONDITIONS OF EMPLOYMENT

6.1.5 INFORMATION SECURITY IN PROJECT MANAGEMENT

 10.1.1
 POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS

 112.6
 SECURITY OF EQUIPMENT AND ASSETS OFF-PREMISES

 142.2
 SYSTEM CHANGE CONTROL PROCEDURES

 11.1
 PHYSICAL SECURITY PERIMETER

13.2.2 AGREEMENTS ON INFORMATION TRANSFER 15.1.1 INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS

 14.1.1
 INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION

 15.1.1
 INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS

TERMINATION OR CHANGE OF EMPLOYMENT RESPONSIBILITIES

TERMINATION OR CHANGE OF EMPLOYMENT RESPONSIBILITIES

MANAGEMENT RESPONSIBILITIES

7.2.1

7.1.1 7.1.1 14.2.6

13.2.4

13.2.4 13.2.4 13.2.4 7.3.1

7.3.1

7.2.3 7.1.1 SCREENING 7.1.1

7.1.2 7.1.2 7.1.2 7.1.2

 BACSE-527
 Require compliance with mandatory or discretionary methods of access by federal authorities to encrypted information
 Foundational Results

 ACSE-537
 Design ad adve through access by the phone to adve through access by the advectory of access by the advectory of the table test and test on the table test on the table test of the advectory of Results
 Foundational Results

 ACSE-537
 Design advect through access by the advectory of the advectory of the advectory of Results
 Foundational Results

 ACSE-537
 Design facilities and cascible to unanatored personnel
 Foundational Results

 ACSE-537
 Design facilities and cascible to unanatored personnel
 Foundational Results

 ACSE-537
 Design facilities and cascible to unanatored personnel
 Foundational Results

 18.1.5
 REGULATION OF CRYPTOGRAPHIC CONTROLS

 11.1.4
 PROTECTING AGAINST EXTERNAL AND ENVIRONMENTAL THEFATS

 11.1.3
 SECURING OFFICES, ROOMS AND FACUTIES

 11.1.3
 SECURING OFFICES, ROOMS AND FACUTIES

PL-4	RULES OF BEHAVIOR
PL-4 Pl-4	RULES OF BEHAVIOR RULES OF BEHAVIOR
PS-2	POSITION RISK DESIGNATION
PS-2	POSITION BISK DESIGNATION
PS-3	PERSONNEL SCREENING
SA-21 PS-3	DEVELOPER SCREENING PERSONNEL SCREENING
PS-4	PERSONNEL TERMINATION
PS-4	PERSONNEL TERMINATION
PS-4	PERSONNEL TERMINATION
PS-5	
	PERSONNEL TRANSFER
PS-6	ACCESS AGREEMENTS
PS-7	THIRD-PARTY PERSONNEL SECURITY
PS-7	THIRD-PARTY PERSONNEL SECURITY
PS-7	THIRD-PARTY PERSONNEL SECURITY
PS-8	PERSONNEL SANCTIONS
PS-8	PERSONNEL SANCTIONS
PS-6	ACCESS AGREEMENTS
PS-6	ACCESS AGREEMENTS
PS-6 RA-2	ACCESS AGREEMENTS
RA-2	SECURITY CATEGORIZATION
RA-2 RA-2 RA-3 RA-3	SECURITY CATEGORIZATION SECURITY CATEGORIZATION RISK ASSESSMENT
RA-2 RA-2 RA-3	SECURITY CATEGORIZATION SECURITY CATEGORIZATION RISK ASSESSMENT RISK ASSESSMENT RISK ASSESSMENT
RA-2 RA-2 RA-3 RA-3 RA-3	SECURITY CATEGORIZATION SECURITY CATEGORIZATION RISK ASSESSMENT
RA-2 RA-2 RA-3 RA-3 RA-3	SECURITY CATEGORIZATION SECURITY CATEGORIZATION RISK ASSESSMENT RISK ASSESSMENT RISK ASSESSMENT
RA-2 RA-2 RA-3 RA-3 RA-3	SECURITY CATEGORIZATION SECURITY CATEGORIZATION RISK ASSESSMENT RISK ASSESSMENT RISK ASSESSMENT
RA-2 RA-2 RA-3 RA-3 RA-3 RA-3	SECURITY CATEGORIZATION SECURITY CATEGORIZATION RISK ASSESSMENT RISK ASSESSMENT RISK ASSESSMENT RISK ASSESSMENT
RA-2 RA-3 RA-3 RA-3 RA-3 RA-3	SECURITY CATEGORIZATION SECURITY CATEGORIZATION RISK ASSESSMENT RISK ASSESSMENT RISK ASSESSMENT
RA-2 RA-2 RA-3 RA-3 RA-3 RA-3 SA-4	SECURITY CATEGORIZATION SECURITY CATEGORIZATION RISK ASSESSMENT RISK ASSESSMENT RISK ASSESSMENT RISK ASSESSMENT RISK ASSESSMENT
RA-2 RA-2 RA-3 RA-3 RA-3 RA-3 SA-4 SA-4	SECURITY CATEGORIZATION SECURITY CATEGORIZATION RIKK ASSESSMENT RIKK ASSESSMENT RIKK ASSESSMENT RIKK ASSESSMENT ACQUISITION PROCESS ACQUISITION PROCESS
RA-2 RA-3 RA-3 RA-3 RA-3 RA-3 RA-3 SA-4 SA-4 SA-4	SECURITY CATEGORIZATION SECURITY CATEGORIZATION RISK ASSESSMENT RISK ASSESSMENT RISK ASSESSMENT RISK ASSESSMENT ACQUISTION PROCESS ACQUISTION PROCESS ACQUISTION PROCESS
RA-2 RA-3 RA-3 RA-3 RA-3 RA-3 RA-3 SA-4 SA-4 SA-4 SA-4	SECURITY CATEGORIZATION SECURITY CATEGORIZATION RIKK ASSESSMENT RIKK ASSESSMENT RIKK ASSESSMENT RIKK ASSESSMENT ACQUISITION PROCESS ACQUISITION PROCESS
RA-2 RA-3 RA-3 RA-3 RA-3 RA-3 RA-3 SA-4 SA-4 SA-4 SA-4	SECURITY CATEGORIZATION SECURITY CATEGORIZATION RIKK ASSESSMENT RIKK ASSESSMENT RIKK ASSESSMENT RIKK ASSESSMENT ACQUISITION PROCESS ACQUISITION PROCESS
RA-2 RA-3 RA-3 RA-3 RA-3 RA-3 RA-3 SA-4 SA-4 SA-4 SA-4	SECURITY CATEGORIZATION SECURITY CATEGORIZATION RIKK ASSESSMENT RIKK ASSESSMENT RIKK ASSESSMENT RIKK ASSESSMENT ACQUISITION PROCESS ACQUISITION PROCESS
RA-2 RA-3 RA-3 RA-3 RA-3 RA-3 RA-3 SA-4 SA-4 SA-4 SA-4	SECURITY CATEGORIZATION SECURITY CATEGORIZATION RIKK ASSESSMENT RIKK ASSESSMENT RIKK ASSESSMENT RIKK ASSESSMENT ACQUISITION PROCESS ACQUISITION PROCESS

SA-13	TRUSTWORTHINESS
\$4.72	LINSUPPORTED SYSTEM COMPONENTS
5A-22	UNSUPPORTED SYSTEM COMPONENTS
SC-13	CRYPTOGRAPHIC PROTECTION
\$1-2	
SI-2 SI-4	FLAW REMEDIATION
51-4	INFORMATION SYSTEM MONITORING
51-4	INFORMATION SYSTEM MONITORING
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
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