SR-23-002

Range Commanders Council
CYBERSECURITY GROUP

RESEARCH, DEVELOPMENT, TEST, AND EVALUATION OVERLAY

ABERDEEN TEST CENTER
DUGWAY PROVING GROUND
ELECTRONIC PROVING GROUND
REAGAN TEST SITE
REDSTONE TEST CENTER
WHITE SANDS TEST CENTER
YUMA PROVING GROUND

NAVAL AIR WARFARE CENTER AIRCRAFT DIVISION PATUXENT RIVER
NAVAL AIR WARFARE CENTER WEAPONS DIVISION CHINA LAKE
NAVAL AIR WARFARE CENTER WEAPONS DIVISION POINT MUGU
NAVAL SURFACE WARFARE CENTER DAHLGREN DIVISION
NAVAL UNDERSEA WARFARE CENTER DIVISION KEYPORT
NAVAL UNDERSEA WARFARE CENTER DIVISION NEWPORT
PACIFIC MISSILE RANGE FACILITY

96th TEST WING
412th TEST WING
ARNOLD ENGINEERING DEVELOPMENT COMPLEX

SPACE LAUNCH DELTA 30
SPACE LAUNCH DELTA 45

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

This page intentionally left blank.

SR-23-002

RESEARCH, DEVELOPMENT, TEST, AND EVALUATION OVERLAY

June 2024

Prepared by

CYBERSECURITY GROUP

Published by

Secretariat
Range Commanders Council
White Sands Missile Range
New Mexico 88002-5110

This page intentionally left blank.

Table of Contents

Table of Tables

This page intentionally left blank.

Preface

Range RDT&E IT systems have become extremely challenging to authorize under the Risk Management Framework (RMF) due to the dynamic nature of the systems; continued configuration modification due to test capability and system under test improvements; and resources becoming more constrained. Ranges need to identify key controls applicable to common RDT&E system types to streamline the authorization process and provide guidance for addressing security controls. This RMF overlay provides security control value definitions, guidance, and tailoring justifications for RDT&E systems creating efficiencies for cybersecurity professionals.

For information about this document, please contact the RCC Secretariat office.

Secretariat, Range Commanders Council
ATTN: TEWS-EDR
1510 Headquarters Avenue
White Sands Missile Range, New Mexico 88002-5110
Telephone: (575) 678-1107, DSN 258-1107
E-mail: rcc-feedback@trmc.osd.mil

This page intentionally left blank.

Acronyms

† AO	authorizing official
† BIOS	basic input/output system
CCI	control correlation identifier
CNSSI	Committee on National Security Systems Instruction
CSSP	Cybersecurity Service Provider
DNS	domain name system
DoD	Department of Defense
† FICAM	federal identity, credential, and access management
† FIPS	Federal Information Processing Standards
† GSM	Global System for Mobile Communication
IAW	in accordance with
† IPSec	Internet Protocol Security
IRP	incident response plan
IS	information system
ISO	information system owner
ISOL	Isolated
ISOL-ET	Isolated with Encrypted Transport
ISSM	information systems security manager
ISSO	information systems security officer
KS	Knowledge Service
† LDAP	lightweight directory access protocol
N/A	not applicable
NIST	National Institute of Standards and Technology
No Gen	No General Users
† NSS	National Security System
PKI/PKE	Public Key Infrastructure/Enabling
† RADIUS	Remote Authentication Dial-in User Service
† RDP	Remote Desktop Protocol
RDT&E	research, development, test, and evaluation
RMF	Risk Management Framework
SP	Special Publication
† SSH	Secure Shell
SRG	security requirements guide
† SSP	system security plan
STD	standard
STIG	Security Technical Information Guide
† TLS	transport layer security
† UHF	ultra-high frequency
† VHF	very high frequency

† Not spelled out in document.

This page intentionally left blank.

RDT&E Overlay

1. Identification

The Research, Development, Test, & Evaluation (RDT&E) overlay identifies security control specifications related to RDT&E systems. Versioning for this document is by date. The date of this overlay is June 2024.

The following resources were used to create this overlay.

- *Security Categorization and Control Selection for National Security Systems*, CNSSI 1253[1]
- *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53 Revision 4[2]
- DoD Risk Management Framework Knowledge Service (RMF KS) web site[3]

This overlay should be evaluated for revision when there has been an update to the security controls in NIST SP 800-53, a change to CNSSI 1253 baselines, or when new threats or vulnerabilities have been identified that change the security protection needs for information systems (ISs).

2. Overlay Characteristics

This Overlay will identify control specifications for the different types of RDT&E systems.

An RDT&E system is one that performs, supports, tests, or evaluates the results of one or more of the following activities: basic research; applied research; advanced technology development; advanced component development and prototypes; system development and demonstration; RDT&E management support; operation system development.

2.1 Standard (STD): This type of system has no specific characteristics other than being an RDT&E system. An STD system is often connected to other RDT&E authorization boundaries (e.g., RDT&E systems, Defense Research and Engineering Network [DREN], Secret Defense Research & Engineering Network [SDREN]) for data sharing.

2.2 Isolated (ISOL): This type of system has no connectivity to any other system. This could be a local area network or a standalone computer.

2.3 Isolated with Encrypted Transport (ISOL-ET): This type of system uses encrypted transport to connect one or more geographically separated components within the same authorization boundary. The Encrypted Transport shall be via National Security Agency Type-1 encryption, or IPSec virtual private network tunnel. The ISOL-ET system and the transport

[1] Committee on National Security Systems. *Security Categorization and Control Selection for National Security Systems*. CNSSI 1253. 27 March 2014. May be superseded by update. Retrieved 4 June 2024. Available at https://www.dcsa.mil/portals/91/documents/ctp/nao/CNSSI_No1253.pdf.

[2] National Institute of Standards and Technology. *Security and Privacy Controls for Federal Information Systems and Organizations*. SP 800-53. April 2013. Updated 22 January 2015. Superseded by SP 800-53 Rev. 5, 23 September 2020. Superseding document retrieved 16 August 2021. Available at https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[3] DoD Risk Management Framework Knowledge Service. https://rmfks.osd.mil/rmf/Pages/default.aspx

network will not have any ability to see or share data between the systems. There shall be no ability for system users to remotely connect from the transport system to the connected systems, or vice versa.

2.4 No General Users (No Gen): This type of system has one main characteristic: no general users (non-privileged users) are allowed to have accounts on, or access the system. Privileged users are the only type of users that will be allowed to have accounts on, and access the system. Since this type of system has no general users, that entire risk vector has been eliminated. Examples of No Gen systems include, but are not limited to, the following: systems specific to network monitoring; systems that only perform anti-virus scanning; some Platform Information Technology systems; some Sensor systems; and some Data Transfer systems.

2.5 No Wireless: The No Wireless designation allows for the removal of a group of controls that are deemed not applicable (N/A) due to the lack of wireless capabilities. Wireless technology examples include, but are not limited, to the following: cell phone transmissions (GSM, Long-term Evolution, 3/4/5 G); Wi-Fi transmissions (2.4/5 GHz [802.11 a/b/g/n]); Bluetooth; Zigbee; packet radio (UHF/VHF); and Near Field Communication.

2.6 No Mobile Devices (No Mobile): The No Mobile designation allows for the removal of a group of controls that are deemed N/A due to the lack of mobile devices within the authorization boundary. Mobile Device examples include, but are not limited, to the following: laptops; tablets; smart phones; and E-readers.

* No Gen and/or No Wireless and/or No Mobile may be used in combination with any of the base system types (STD, ISOL, ISOL-ET).
** Only one base system type (STD, ISOL, ISOL-ET) may be selected.
** This overlay is independent of system categorization and/or other overlays.

3. Applicability

Use questions 3.1 through 3.7, in order, to determine the applicable RDT&E system type(s).

3.1 Will this be an RDT&E system?

If the answer is yes, continue with question 3.2.

If the answer is no, this Overlay does not apply.

3.2 Is this an Isolated system (see Section 2.2)?

If the answer is yes, apply the ISOL column from the chart in Section 4, and continue with questions 3.5, 3.6. and 3.7.

If the answer is no, continue to question 3.4.

3.3 Is this an Isolated with Encrypted Transport system (see Section 2.3)?

If the answer is yes, apply the ISOL-ET column from the chart in Section 4, and continue with questions 3.5, 3.6, and 3.7.

If the answer is no, continue to question 3.5.

3.4 If the answer to both questions 3.2 and 3.3 is no, then it is a Standard system.

Apply the STD column from the chart in Section 4, and continue with questions 3.5, 3.6, and 3.7.

3.5 Is this system without General Users (see Section 2.4)?

If the answer is yes, apply the No Gen column from the chart in Section 4, and continue with questions 3.6 and 3.7.

If the answer is no, continue to question 3.6.

3.6 Does the system have any wireless capabilities/technologies (see 2.5)?

If the answer is no, apply the No Wireless column from the chart in Section 4, and continue with question 3.7.

If the answer is yes, continue with question 3.7.

3.7 Does the system include any mobile devices (see 2.6)?

If the answer is no, apply the No Mobile column from the chart in Section 4.

If the answer is yes, continue to sections 4 and 5.

Apply other/additional Overlays as appropriate (e.g., Privacy, Classified).

4. Overlay Summary

Table 1 contains a summary of the security control specifications as they apply in this overlay. The symbols used in the table are as follows.

- A plus sign ("+") indicates the control should be selected.
- Two dashes ("- -") indicate the control should not be selected.
- The letter "G" indicates there is supplemental guidance, including specific tailoring guidance if applicable, for the control.
- The letter "V" indicates this overlay defines a value for an organizational-defined parameter for the control.

Table 1. Security Controls for the RDT&E Overlay

Control ID	Control Name	STD	ISOL	ISOL-ET	No Gen	No Wireless	No Mobile
AC-2 a	ACCOUNT MANAGEMENT	V	V	V	V		
AC-2 f	ACCOUNT MANAGEMENT	V	V	V	V		
AC-2(3)	ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS						
AC-2(5)	ACCOUNT MANAGEMENT | INACTIVITY LOGOUT	V	V	V	V		
AC-2(9)	ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED GROUPS/ ACCOUNTS	V	V	V	V		
AC-2(12) a	ACCOUNT MANAGEMENT | ACCOUNT MONITORING/ATYPICAL USAGE	V	V	V	V		
AC-3(4)	ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL	V	V	V	V		
AC-4	INFORMATION FLOW ENFORCEMENT	V	V	V	V		
AC-5 a	SEPARATION OF DUTIES	V	V	V			
AC-6(1)	LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS	G	G	G	G		
AC-6(2)	LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS				- -		
AC-6(5)	LEAST PRIVILEGE | PRIVILEGED ACCOUNTS	V, G	V. G	V, G	V. G		
AC-6(8)	PRIVILEGE LEVELS FOR CODE EXECUTION	G	G	G	G		
AC-6(10)	LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS				- -		
AC-10	CONCURRENT SESSION CONTROL	V	V	V	V		
AC-12	SESSION TERMINATION	G	G	G	G		
AC-14 a	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	G	G	G	G		
AC-17	REMOTE ACCESS	G	- -	- -	G		
AC-17(1)	REMOTE ACCESS | AUTOMATED MONITORING/CONTROL	G	- -	- -	G		
AC-17(2)	REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY/INTEGRITY USING ENCRYPTION	G	- -	- -	G		
AC-17(3)	REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS	G	- -	- -	G		
AC-17(4)	REMOTE ACCESS | PRIVILEGED COMMANDS/ACCESS	G	- -	- -	G		
AC-17(6)	REMOTE ACCESS | PROTECTION OF INFORMATION	G	- -	- -	G		
AC-17(9)	REMOTE ACCESS | DISCONNECT/DISABLE ACCESS	G	- -	- -	G		
AC-18	WIRELESS ACCESS					- -	
AC-18 (1)	WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION					- -	
AC-18 (3)	WIRELESS ACCESS | DISABLE WIRELESS NETWORKING					- -	
AC-18 (4)	WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS					- -	
AC-19	ACCESS CONTROL FOR MOBILE DEVICES						- -
AC-19(5)	ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE/CONTAINER-BASED ENCRYPTION						- -

Table 1. Security Controls for the RDT&E Overlay

Control ID	Control Name	STD	ISOL	ISOL-ET	No Gen	No Wireless	No Mobile
AC-23	DATA MINING PROTECTION	V	V	V	V		
AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	G	G	G	G		
AT-3(2)	SECURITY TRAINING | PHYSICAL SECURITY CONTROLS	V	V	V	V		
AT-3(4)	SECURITY TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR	G	G	G	G		
AU-3(1)	CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION	- -	- -	- -	- -		
AU-4	AUDIT STORAGE CAPACITY	G	G	G	G		
AU-5 b	RESPONSE TO AUDIT PROCESSING FAILURES	V, G	V, G	V. G	V, G		
AU-6 a	AUDIT REVIEW, ANALYSIS, AND REPORTING	V	V	V	V		
AU-6(1)	PROCESS INTEGRATION	G	G	G	G		
AU-6(4)	AUDIT REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS	G	G	G	G		
AU-7	AUDIT REDUCTION AND REPORT GENERATION	G	G	G	G		
AU-9(4)	PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS	G	G	G	G		
AU-11(1)	AUDIT RECORD RETENTION | LONG-TERM RETRIEVAL CAPABILITY	V	V	V	V		
AU-12(1)	TIME-CORRELATED AUDIT TRAIL	V	V	V	V		
AU-12(3)	AUDIT GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS	V	V	V	V		
CA-2(1)	SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS	V	V, G	V, G	V, G		
CA-3	SYSTEM INTERCONNECTIONS		- -				
CA-3(1)	CA-3(1). SYSTEM INTERCONNECTIONS | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	V	- -	V	V		
CA-7	CONTINUOUS MONITORING	G	G	G	G		
CA-7(1)	CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT		G	G	G		
CA-9 a	INTERNAL SYSTEM CONNECTIONS	V	V	V	V		
CM-2(7)	BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS	- -	- -	- -	- -		
CM-3 e, g	CONFIGURATION CHANGE CONTROL	V	V	V	V		
CM-4(1)	SECURITY IMPACT ANALYSIS | SEPARATE TEST ENVIRONMENTS	G	G	G	G		
CM-6(1)	CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT/ APPLICATION/VERIFICATION	V	V	V	V		
CM-7(1) b	LEAST FUNCTIONALITY | PERIODIC REVIEW	V	V	V	V		
CM-7(2)	LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION	V, G	V, G	V, G	V, G		
CM-7(5) a	LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE/WHITELISTING	- -	- -	- -	- -		

Table 1. Security Controls for the RDT&E Overlay

Control ID	Control Name	STD	ISOL	ISOL-ET	No Gen	No Wireless	No Mobile
CM-8(2)	INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE	G	G	G	G		
CM-8(3)	INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION	G	G	G	G		
CM-11 a, b	USER-INSTALLED SOFTWARE	V	V	V	V		
CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES	G	G	G	G		
CP-4	CONTINGENCY PLAN TESTING	V	V	V	V		
CP-7	ALTERNATE PROCESSING SITE	G	G	G	G		
CP-7(1)	ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE	G	G	G	G		
CP-7(2)	ALTERNATE PROCESSING SITE | ACCESSIBILITY	G	G	G	G		
CP-7(3)	ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE	G	G	G	G		
CP-8	TELECOMMUNICATIONS SERVICES	G	V	G	G		
CP-8(1)	TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS	G	G	G	G		
CP-8(2)	TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE	G	G	G	G		
IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	G	G	G	G		
IA-2(2)	IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS				- -		
IA-2(4)	IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS				- -		
IA-2(8)	IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT	G	G	G	G		
IA-2(9)	IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT	G	G	G	- -		
IA-4 (e)	IDENTIFIER MANAGEMENT	G	G	G	G		
IA-5(13)	AUTHENTICATOR MANAGEMENT | EXPIRATION OF CACHED AUTHENTICATORS	G	G	G	G		
IA-8(2)	IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-APPROVED PRODUCTS	G	G	G	G		
IA-8(3)	IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-APPROVED PRODUCTS	G	G	G	G		
IA-8(4)	IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-APPROVED PRODUCTS	G	G	G	G		
IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	G	G	G	G		
IR-3	IR-3. INCIDENT RESPONSE TESTING	G	G	G	G		
IR-6(1)	INCIDENT REPORTING | AUTOMATED REPORTING	G	- -	- -	G		

Table 1. Security Controls for the RDT&E Overlay

Control ID	Control Name	STD	ISOL	ISOL-ET	No Gen	No Wireless	No Mobile
IR-7(1)	INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION/SUPPORT		- -	- -			
IR-10	INTEGRATED INFORMATION SECURITY ANALYSIS TEAM	G	G	G	G		
MA-2 c, f	CONTROLLED MAINTENANCE	V	V	V	V		
MP-1	MEDIA PROTECTION POLICY AND PROCEDURES	G	G	G	G		
PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	G	G	G	G		
PE-17	ALTERNATE WORK SITE	- -	- -	- -	- -		
PL-1	SECURITY PLANNING POLICY AND PROCEDURES	G	G	G	G		
PL-2(3)	SYSTEM SECURITY PLAN | PLAN/COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	V	V	V	V		
PL-8	INFORMATION SECURITY ARCHITECTURE	G	G	G	G		
PL-8(1) a	INFORMATION SECURITY ARCHITECTURE | DEFENSE-IN-DEPTH	V	V	V	V		
PL-8(2)	INFORMATION SECURITY ARCHITECTURE | SUPPLIER DIVERSITY	V	V	V	V		
PM-1	INFORMATION SECURITY PROGRAM PLAN	G	G	G	G		
PM-2	SENIOR INFORMATION SECURITY OFFICER	G	G	G	G		
PM-7	ENTERPRISE ARCHITECTURE	G	G	G	G		
PM-8	CRITICAL INFRASTRUCTURE PLAN	G	G	G	G		
PM-9	RISK MANAGEMENT STRATEGY	G	G	G	G		
PM-10	SECURITY AUTHORIZATION PROCESS	G	G	G	G		
PM-13	INFORMATION SECURITY WORKFORCE	G	G	G	G		
PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	G	G	G	G		
PS-4 c	PERSONNEL TERMINATION	V	V	V	V		
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	G	G	G	G		
RA-5 a, d	VULNERABILITY SCANNING	G	G	G	G		
RA-5(4)	VULNERABILITY SCANNING | DISCOVERABLE INFORMATION	V	V	V	V		
RA-5(5)	VULNERABILITY SCANNING | PRIVILEGED ACCESS	V	V	V	V		
SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	G	G	G	G		
SA-2	ALLOCATION OF RESOURCES	G	G	G	G		
SA-3 a	SYSTEM DEVELOPMENT LIFE CYCLE	G	G	G	G		
SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	G	G	G	G		
SC-5	DENIAL OF SERVICE PROTECTION	V	G	G	V		
SC-5(1)	DENIAL OF SERVICE PROTECTION | RESTRICT INTERNAL USERS	V	- -	- -	V		
SC-7 b	BOUNDARY PROTECTION		- -	- -			
SC-7(3)	BOUNDARY PROTECTION | ACCESS POINTS		- -	- -			
SC-7(4)	BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES		- -	- -			

Table 1. Security Controls for the RDT&E Overlay

Control ID	Control Name	STD	ISOL	ISOL-ET	No Gen	No Wireless	No Mobile
SC-7(5)	BOUNDARY PROTECTION | DENY BY DEFAULT/ALLOW BY EXCEPTION		- -	- -			
SC-7(7)	BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES		- -	- -			
SC-7(8)	BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS		- -	- -			
SC-7(9)	BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC		- -	- -			
SC-7(10)	BOUNDARY PROTECTION | PREVENT UNAUTHORIZED EXFILTRATION		- -	- -			
SC-7(11)	BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC	V	- -	- -	V		
SC-7(13)	BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS/MECHANISMS/ SUPPORT COMPONENTS	G	G	G	G		
SC-7(14)	BOUNDARY PROTECTION | PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTION	G	G	G	G		
SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	V	V	V	V		
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	G	- -	- -	G		
SC-18(1)	MOBILE CODE | IDENTIFY UNACCEPTABLE CODE/TAKE CORRECTIVE ACTIONS	V	V	V	V		
SC-18(3)	MOBILE CODE | PREVENT DOWNLOADING/EXECUTION	V	V, G	V, G	V		
SC-20	SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)		- -	- -			
SC-21	SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	G	- -	- -	G		
SC-23(3)	SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION	V	V	V	V		
SC-23(5)	SESSION AUTHENTICITY | ALLOWED CERTIFICATE AUTHORITIES	G	- -	- -	G		
SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	G	G	G	G		
SI-2(2)	FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS	G	G	G	G		
SI-3(1)	MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT	G	G	G	G		
SI-3(2)	MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES	G	G	G	G		
SI-4 b, g	INFORMATION SYSTEM MONITORING	V	V	V	V		
SI-4(1)	INFORMATION SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM	G	G	G	G		
SI-4(14)	INFORMATION SYSTEM MONITORING | WIRELESS INTRUSION DETECTION					- -	

Table 1. Security Controls for the RDT&E Overlay							
Control ID	**Control Name**	**STD**	**ISOL**	**ISOL-ET**	**No Gen**	**No Wireless**	**No Mobile**
SI-4(15)	INFORMATION SYSTEM MONITORING | WIRELESS TO WIRELINE COMMUNICATIONS					- -	
SI-4(19)	INFORMATION SYSTEM MONITORING | INDIVIDUALS POSING GREATER RISK	V	V	V	V		
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	V	V	V	V		
SI-8	SPAM PROTECTION	- -	- -	- -	- -		
SI-8(1)	SPAM PROTECTION | CENTRAL MANAGEMENT	- -	- -	- -	- -		
SI-16	MEMORY PROTECTION	V	V	V	V		

5. Detailed Overlay Control Specifications

The information provided in this section elaborates on the guidance provided in NIST SP 800-53 and on the DoD RMF KS web site. Values defined by this Overlay are within squared brackets and underlined "[example value definition]"; DoD-defined values are within brackets, but NOT underlined.

AC-2 a. ACCOUNT MANAGEMENT

Value Definition: Identifies and selects the following types of IS accounts to support organizational missions/business functions: [General and Privileged user accounts].

AC-2 f. ACCOUNT MANAGEMENT

Value Definition: Creates, enables, modifies, disables, and removes IS accounts in accordance with (IAW) [direction identified in the account request form (DD 2875 or similar)];

AC-2(3): ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS

Guidance: The DoD value is 35 days of inactivity. Due to the nature of system usage within the RDT&E environment, 90 days may be a more suitable time frame. This could be accomplished by tailoring (modifying) the control value from 35 to 90 days.

AC-2(5). ACCOUNT MANAGEMENT | INACTIVITY LOGOUT

Value Definition: The organization requires that users log out when [the user's work day has ended or at the conclusion of the test event].

AC-2(9). ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED GROUPS/ ACCOUNTS

Value Definition: The organization only permits the use of shared/group accounts that meet [AO/delegated AO approved conditions, are required to meet mission objectives, and are documented in the SSP].

AC-2(12) a. ACCOUNT MANAGEMENT | ACCOUNT MONITORING/ATYPICAL USAGE

Value Definition: Monitors IS accounts for [atypical usage, including but not limited to the following: during "non-standard" work hours; from "non-standard" locations; during scheduled out-of-office periods; logging into multiple workstations concurrently; attempted use of unauthorized applications; and attempted input/output port usage];

AC-3(4). ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL

Value Definition: The IS enforces [user/identity-based discretionary access control policy] over defined subjects and objects where the policy specifies that a subject that has been granted access to information can do one or more of the following:

AC-4. INFORMATION FLOW ENFORCEMENT

Value Definition: The IS enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [the identified Ports, Protocols, and Services as documented in the SSP].

AC-5 a. SEPARATION OF DUTIES

Value Definition: The Organization a: separates [at a minimum, the duties of general users and system administrators];

AC-6(1). LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

Guidance: Some examples of security-relevant functions are: auditing tools/data; security configuration settings (local/group policies); backup settings/data; installing software; BIOS access; and input/output port controls.

AC-6(2). LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

Tailoring Justification: This control is not applicable to the No Gen system type since the system is only used by administrative personnel, and those personnel are always performing administrative (privileged) functions when using the system.

AC-6(5). LEAST PRIVILEGE | PRIVILEGED ACCOUNTS

Value Definition: The organization restricts privileged accounts on the IS to [the minimum number of privileged users required to manage the system].

Guidance: The minimum number of privileged users will also need to include redundant personnel to cover for non-availability of primary personnel performing each privileged function.

AC-6(8). PRIVILEGE LEVELS FOR CODE EXECUTION

Guidance: Configure the system/components IAW applicable STIG/security requirements guide (SRG) requirements to restrict software execution levels to those users executing the software.

AC-6(10). LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

Tailoring Justification: This control is not applicable to the No Gen system type since there are only privileged users on the system.

AC-10. CONCURRENT SESSION CONTROL

Value Definition: The IS limits the number of concurrent sessions for [all account types and/or accounts] to [be in compliance with applicable STIGs/SRGs].

AC-12. SESSION TERMINATION

Guidance: User session termination settings should be IAW applicable STIGS/SRGs or mission requirements.

AC-14 a. PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Guidance: In most circumstances, no actions would be allowed without Identification and Authorization. An example of when it may be appropriate to use a device without Identification and Authorization would be when the device's capabilities have ben administratively restricted such that it is limited in use to only acting as a kiosk or proxy machine and where appropriate Identification and Authorization take place on a destination system.

AC-17. REMOTE ACCESS

Guidance: The RDT&E community defines remote access as connecting to and accessing an IS directly from another IS that is outside of the authorization boundary of the initial IS. For example, if an IS has two sites transporting data between them via an encrypted tunnel over another network, access between the sites would NOT be considered remote access since both sites and all devices and the encrypted connectivity are part of the authorization boundary and organizationally controlled. Conversely, access to an IS from an asset that is not managed by and/or part of the authorization boundary would be considered remote access. The encrypted tunnel between sites must be AO-approved.

Tailoring Justification: This control is tailored out for ISOL and ISOL-ET systems since these system types do not have communication capabilities/remote access capabilities with any other network.

Guidance: This control may be tailored out for STD and No Gen systems if these system types do not have remote access capabilities from any external network.

AC-17(1). REMOTE ACCESS | AUTOMATED MONITORING/CONTROL

Tailoring Justification: This control is tailored out for ISOL and ISOL-ET systems since these system types do not have communication capabilities/remote access capabilities with any other network.

Guidance: This control may be tailored out for STD and No Gen systems if these system types do not have remote access capabilities from any external network.

AC-17(2). REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY/INTEGRITY USING ENCRYPTION

Tailoring Justification: This control is tailored out for ISOL and ISOL-ET systems since these system types do not have communication capabilities/remote access capabilities with any other network.

Guidance: This control may be tailored out for STD and No Gen systems if these system types do not have remote access capabilities from any external network.

AC-17(3). REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS

Tailoring Justification: This control is tailored out for ISOL and ISOL-ET systems since these system types do not have communication capabilities/remote access capabilities with any other network.

Guidance: This control may be tailored out for STD and No Gen systems if these system types do not have remote access capabilities from any external network.

AC-17(4). REMOTE ACCESS | PRIVILEGED COMMANDS/ACCESS

Tailoring Justification: This control is tailored out for ISOL and ISOL-ET systems since these system types do not have communication capabilities/remote access capabilities with any other network.

Guidance: This control may be tailored out for STD and No Gen systems if these system types do not have remote access capabilities from any external network.

AC-17(6). REMOTE ACCESS | PROTECTION OF INFORMATION

Tailoring Justification: This control is tailored out for ISOL and ISOL-ET systems since these system types do not have communication capabilities/remote access capabilities with any other network.

Guidance: This control may be tailored out for STD and No Gen systems if these system types do not have remote access capabilities from any external network.

AC-17(9). REMOTE ACCESS | DISCONNECT/DISABLE ACCESS

Tailoring Justification: This control is tailored out for ISOL and ISOL-ET systems since these system types do not have communication capabilities/remote access capabilities with any other network.

Guidance: This control may be tailored out for STD and No Gen systems if these system types do not have remote access capabilities from any external network.

AC-18. WIRELESS ACCESS

Tailoring Justification: For systems without wireless communication technologies (see 2.5), this control is not applicable and can be tailored out.

AC-18(1). WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION

Tailoring Justification: For systems without wireless communication technologies (see 2.5), this control is not applicable and can be tailored out.

AC-18(3). WIRELESS ACCESS | DISABLE WIRELESS NETWORKING

Tailoring Justification: For systems without wireless communication technologies (see 2.5), this control is not applicable and can be tailored out.

AC-18(4). WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS

Tailoring Justification: For systems without wireless communication technologies (see 2.5), this control is not applicable and can be tailored out.

AC-19. ACCESS CONTROL FOR MOBILE DEVICES

Tailoring Justification: For systems without mobile devices (see 2.6), this control is not applicable and can be tailored out.

AC-19(5). ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE/CONTAINER-BASED ENCRYPTION

Tailoring Justification: For systems without mobile devices (see 2.6), this control is not applicable and can be tailored out.

AC-23. DATA MINING PROTECTION

Value Definition: The organization employs [auditing of failed access attempts] for [all data storage objects] to adequately detect and protect against data mining.

AT-1. SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Guidance: This control is fully inherited due to all control correlation identifiers (CCIs) being accomplished at the DoD/Organizational level (per the RMF KS).

AT-3(2). SECURITY TRAINING | PHYSICAL SECURITY CONTROLS

Value Definition: The organization provides [personnel with specific roles and responsibilities associated with physical security controls] with initial and [annual] training in the employment and operation of physical security controls.

AT-3(4). SECURITY TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR

Guidance: This control is specific to each organization/system; therefore, each Organization will need to define their own value for the training requirements. One example of a value could be the following: “suspicious emails, opening suspicious attachments, clicking on suspicious links/URLs, phishing attempts, and anti-virus/malware”.

AU-3(1). CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION

Tailoring Justification: RDT&E systems that have implemented all STIG/SRG audit settings do not require any additional audit information to be captured.

AU-4. AUDIT STORAGE CAPACITY

Guidance: System personnel will determine the audit storage capacity that is determined in part by the volume of audit logs combined with the time the audit logs must be kept on the system.

AU-5 b. RESPONSE TO AUDIT PROCESSING FAILURES

Value Definition: Takes the following additional actions: [records any audit processing failures and if mission requirements allow, shuts down the failing component until auditing can be re-enabled].

Guidance: When a determination is required regarding allowing a component to remain operational during an audit processing failure, the information systems security manager (ISSM) (or designee) will make the decision to allow or not allow the component to operate.

AU-6 a. AUDIT REVIEW, ANALYSIS, AND REPORTING

Value Definition: Reviews and analyzes IS audit records [every seven days or more frequently if required by an alarm, event, or anomaly] for indications of [any inappropriate or unusual activity];

AU-6(1). PROCESS INTEGRATION

Guidance: This control is often tailored from automated to manual on small and/or isolated RDT&E systems.

AU-6(4). AUDIT REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS

Guidance: This control is often tailored from centralized to de-centralized on small and/or isolated RDT&E systems.

AU-7. AUDIT REDUCTION AND REPORT GENERATION

Guidance: This control is often tailored out on small and/or isolated RDT&E systems, as it may not be practical to implement an audit reduction and reporting capability.

AU-9(4). PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS

Guidance: Access to the management of audit functionality and logs should be limited to the minimum number of individuals possible. When possible, two individuals with such access is preferable to one in order to minimize the potential of insider threat. Additionally, role separation should be implemented if possible, meaning that, when avoidable, the system and network administrators whose actions are being audited should not be the same individuals as those with access to the management of audit functionality and logs.

AU-11(1). AUDIT RECORD RETENTION | LONG-TERM RETRIEVAL CAPABILITY

Value Definition: The organization employs [a retention technology that will enable access to the audit records for the duration of the required retention period (AU-11)] to ensure that long-term audit records generated by the IS can be retrieved.

AU-12(1). TIME-CORRELATED AUDIT TRAIL

Value Definition: The IS compiles audit records from [all information system components that have the capability to generate audit logs] into a system-wide (logical or physical) audit trail that is time-correlated to within [the tolerance defined in AU-8].

AU-12(3). AUDIT GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS

Value Definition: The IS provides the capability for [designated privileged users] to change the auditing to be performed on [all information system components that have the capability to generate audit logs] based on [the organization's change management process] within [the timeframes identified in the change management process].

CA-2(1). SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS

Guidance: Due to the lack of data sharing capabilities outside of the authorization boundary, ISOL and ISOL-ET systems would likely not need independent/external assessors. Due to no General Users being on the system, No Gen systems would likely not need independent/external assessors.

CA-3. SYSTEM INTERCONNECTIONS

Tailoring Justification: ISOL systems do not connect to any systems outside of the authorization boundary; therefore, Interconnection Security Agreements are N/A.

CA-3(1). SYSTEM INTERCONNECTIONS | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS

Value Definition: The organization prohibits the direct connection of [all unclassified NSS] to an external network without the use of [an AO-approved Controlled Interface/boundary protection device]. ** CNSSI 4009[4] defines a controlled interface **

Tailoring Justification: ISOL systems do not connect to any systems outside of the Authorization Boundary.

CA-7. CONTINUOUS MONITORING

Guidance: Continuous monitoring frequencies are defined in CA-2, and reads in part "DoD has defined the frequency as annually for technical controls, annually for a portion of management and operational controls, such that all are reviewed in a 3-year period, except for those requiring more frequent review as defined in other site or overarching policy. (NOTE: Technical, Management and Operational is IAW NIST SP 800-53 Table 1-1)." (Risk Management Framework Knowledge Service website).

CA-7(1). CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT

Guidance: Due to the lack of data sharing capabilities outside of the authorization boundary, ISOL and ISOL-ET systems would likely not need independent/external assessors. Due to no General Users being on the system, No Gen systems would likely not need independent/external assessors.

CA-9 a. INTERNAL SYSTEM CONNECTIONS

Value Definition: The organization: a. Authorizes internal connections of [all IS devices identified in the network diagram and included in the hardware list] to the IS;

CM-2(7). BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS

Tailoring Justification: RDT&E systems do not travel to high-risk areas, so this control is N/A.

[4] Committee on National Security Systems. *Committee on National Security Systems (CNSS) Glossary*. CNSSI 4009. 6 April 2015. May be superseded by update. Retrieved 4 June 2024. Available at https://www.cnss.gov/cnss/.

CM-3 e, g. CONFIGURATION CHANGE CONTROL

Value Definition: e. Retains records of configuration-controlled changes to the IS for [the duration of the Authorization to Operate period];

Value Definition: g. Coordinates and provides oversight for configuration change control activities through [the Configuration Control Board] that convenes [as required to meet the needs for evaluating qualifying proposed system changes].

CM-4(1). SECURITY IMPACT ANALYSIS | SEPARATE TEST ENVIRONMENTS

Guidance: This control is sometimes tailored out for RDT&E systems since the very nature of them is to support testing and evaluation. The need for a separate test environment should track to the RMF availability level. Some RDT&E environments may require a high level of configuration control. These environments should be considered similar to production environments and may require the application of a separate test environment to validate changes.

CM-6(1). CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT/ APPLICATION/VERIFICATION

Value Definition: The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [all IS components].

CM-7(1) b. LEAST FUNCTIONALITY | PERIODIC REVIEW

Value Definition: Disables [all functions, ports, protocols, and services within the IS deemed to be unnecessary].

CM-7(2). LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION

Value Definition: The information system prevents program execution in accordance with [applicable SRGs/STIGs].

Guidance: For example program execution shall only occur in specifically identified program folders (e.g., C:\Program Files(x85)\McAfee\VirusScan Enterprise) and shall not occur in temporary locations, home directories, or on removable media.

CM-7(5) a. LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE/WHITELISTING

Value Definition: The organization:

(a) Identifies [and maintains a list of software programs authorized to execute on the IS (commonly referred to as whitelisting)];

CM-8(2). INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE

Guidance: This control is often tailored from automated to manual on small and/or isolated RDT&E systems.

CM-8(3). INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION

Guidance: This control is often tailored from automated to manual on small and/or isolated RDT&E systems.

CM-11. USER-INSTALLED SOFTWARE

Value Definition: The organization:

a. Establishes [policies prohibiting general users from installing software];

b. Enforces software installation policies through [permission-based technical controls implemented on the system];

CP-1. CONTINGENCY PLANNING POLICY AND PROCEDURES

Guidance: This control is fully inherited due to all CCIs being accomplished at the DoD/ Organizational level (per the RMF KS).

CP-4. CONTINGENCY PLAN TESTING

Value Definition: The organization:

a. Tests the contingency plan for the IS [at least annually] using [at the minimum table top exercises as defined in the contingency plan] to determine the effectiveness of the plan and the organizational readiness to execute the plan;

CP-7. ALTERNATE PROCESSING SITE

Guidance: This control is often tailored out on systems that do not support mission-essential functions or essential business functions.

CP-7(1). ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE

Guidance: This control is often tailored out on systems that do not support mission-essential functions or essential business functions.

CP-7(2). ALTERNATE PROCESSING SITE | ACCESSIBILITY

Guidance: This control is often tailored out on systems that do not support mission-essential functions or essential business functions.

CP-7(3). ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE

Guidance: This control is often tailored out on systems that do not support mission-essential functions or essential business functions.

CP-8. TELECOMMUNICATIONS SERVICES

Guidance:

a. This control is often tailored out on systems that do not support mission-essential functions or essential business functions.

b. For ISOL systems, this control may be tailored out.

CP-8(1). TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS

Guidance: This control is often tailored out on systems that do not support mission-essential functions or essential business functions.

CP-8(2). TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE

Guidance: This control is often tailored out on systems that do not support mission-essential functions or essential business functions.

IA-1. IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Guidance: This control is fully inherited due to all CCIs being accomplished at the DoD/ Organizational level (per the RMF KS).

IA-2(2). IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS

Tailoring Justification: This control is tailored out for No Gen systems since they do not have any non-privileged accounts.

IA-2(4). IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS

Tailoring Justification: This control is tailored out for No Gen systems since they do not have any non-privileged accounts.

IA-2(8). IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT

Guidance: The intent of the control is to implement either time-based and/or encryption-based methods to prevent replay. Replay-resistant mechanisms include but are not limited to the following: Kerberos, LDAP with TLS, RADIUS with FIPS mode, RDP with TLS, and SSH with TLS.

IA-2(9). IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT

Tailoring Justification: This control is tailored out for No Gen systems since they do not have any non-privileged accounts.

Guidance: The intent of the control is to implement either time-based and/or encryption-based methods to prevent replay. Replay -resistant mechanisms include but are not limited to the following: Kerberos, LDAP with TLS, RADIUS with FIPS mode, RDP with TLS, and SSH with TLS.

IA-4 (e). IDENTIFIER MANAGEMENT

Guidance: The DoD value is 35 days of inactivity. Due to the nature of system usage within the RDT&E environment, a longer timeframe may be more suitable. This could be accomplished by tailoring (modifying) the control value.

IA-5(13). AUTHENTICATOR MANAGEMENT | EXPIRATION OF CACHED AUTHENTICATORS

Guidance: If the device/application doesn’t have a technical method to implement this control, this may be tailored out.

IA-8(2). IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF THIRD-PARTY CREDENTIALS

Guidance: If a system is not publicly accessible, this control may be tailored out.

IA-8(3). IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-APPROVED PRODUCTS

Guidance: If a system is not publicly accessible, this control may be tailored out.

IA-8(4). IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-ISSUED PROFILES

Guidance: If a system is not publicly accessible, this control may be tailored out.

IR-1. IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Guidance: This control is fully inherited due to all CCIs being accomplished at the DoD/ Organizational level (per the RMF KS).

IR-3. INCIDENT RESPONSE TESTING

Guidance: For RDT&E systems, testing can be accomplished via table top exercises, simulated events, or by completing an After Action Report following a real event or incident.

IR-6(1). INCIDENT REPORTING | AUTOMATED REPORTING

Tailoring Justification: Due to the lack of connectivity for ISOL and ISOL-ET systems, automated incident reporting is not implementable.

Guidance: This control is specific to JIMS reporting, which is accomplished by the Cybersecurity Service Provider (CSSP). RDT&E systems would likely inherit this control from their CSSP.

IR-7(1). INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION/SUPPORT

Tailoring Justification: Due to the lack of connectivity for ISOL and ISOL-ET systems, automated incident reporting is not implementable.

IR-10. INTEGRATED INFORMATION SECURITY ANALYSIS TEAM

Guidance: This control is often inherited from the CSSP or higher-level organization.

MA-2 c, f. CONTROLLED MAINTENANCE

Value Definition: c. Requires that [at a minimum, the ISSM] explicitly approve the removal of the IS or system components from organizational facilities for off-site maintenance or repairs;

f. Includes [date and time of maintenance, name of the company and point of contact performing the maintenance, name of escort (if applicable), a description of the maintenance performed, and a list of equipment removed or replaced (including at a minimum make, model, serial number, and general description)] in organizational maintenance records.

MP-1. MEDIA PROTECTION POLICY AND PROCEDURES

Guidance: This control is fully inherited due to all CCIs being accomplished at the DoD/ Organizational level (per the RMF KS).

PE-1. IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Guidance: This control is fully inherited due to all CCIs being accomplished at the DoD/ Organizational level (per the RMF KS).

PE-17. ALTERNATE WORK SITE

Tailoring Justification: Due to RDT&E systems requiring access/connectivity to site-specific testing equipment, this control is not required.

PL-1. IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Guidance: This control is fully inherited due to all CCIs being accomplished at the DoD/ Organizational level (per the RMF KS).

PL-2(3). SYSTEM SECURITY PLAN | PLAN/COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES

Value Definition: The organization plans and coordinates security-related activities affecting the IS with [all applicable organizational personnel (e.g., Information System Owner [ISO], Information Owner, Contractor Program Security Officer/Government Program Security Officer, ISSM/ISSO, COOP lead)] before conducting such activities in order to reduce the impact on other organizational entities.

PL-8. INFORMATION SECURITY ARCHITECTURE

Guidance: All aspects of Information Security Architecture can be accomplished in the SSP, thereby reducing the need for a separate document for this control.

PL-8(1) a. INFORMATION SECURITY ARCHITECTURE | DEFENSE-IN-DEPTH

Value Definition: (a) Allocates [sufficient technical and procedural security safeguards] to [provide a layered security approach comprising of procedural and technical security measures to safeguard the IS and environment]; and

PL-8(2). INFORMATION SECURITY ARCHITECTURE | SUPPLIER DIVERSITY

Value Definition: The organization requires that [technical security safeguards, as identified in PL-8(1)] allocated to [Assignment: organization-defined locations and architectural layers] are obtained from different suppliers.

PM-1. INFORMATION SECURITY PROGRAM PLAN

Guidance: This control is fully inherited due to all CCIs being accomplished at the DoD/ Organizational level (per the RMF KS).

PM-2. SENIOR INFORMATION SECURITY OFFICER

Guidance: This control is fully inherited due to all CCIs being accomplished at the DoD/ Organizational level (per the RMF KS).

PM-7. ENTERPRISE ARCHITECTURE

Guidance: This control is fully inherited due to all CCIs being accomplished at the DoD/ Organizational level (per the RMF KS).

PM-8. CRITICAL INFRASTRUCTURE PLAN

Guidance: This control is fully inherited due to all CCIs being accomplished at the DoD/ Organizational level (per the RMF KS).

PM-9. RISK MANAGEMENT STRATEGY

Guidance: This control is fully inherited due to all CCIs being accomplished at the DoD/ Organizational level (per the RMF KS).

PM-10. SECURITY AUTHORIZATION PROCESS

Guidance: This control is fully inherited due to all CCIs being accomplished at the DoD/ Organizational level (per the RMF KS).

PM-13. INFORMATION SECURITY WORKFORCE

Guidance: This control is fully inherited due to all CCIs being accomplished at the DoD/ Organizational level (per the RMF KS).

PS-1. PERSONNEL SECURITY POLICY AND PROCEDURES

Guidance: This control is fully inherited due to all CCIs being accomplished at the DoD/ Organizational level (per the RMF KS).

PS-4 c. PERSONNEL TERMINATION

Value Definition: Conducts exit interviews that include a discussion of [the continued need to protect organizational and/or classified information following separation from the organization];

RA-1. RISK ASSESSMENT POLICY AND PROCEDURES

Guidance: This control is fully inherited due to all CCIs being accomplished at the DoD/ Organizational level (per the RMF KS).

RA-5 a, d. VULNERABILITY SCANNING

Guidance: Vulnerability scanning (a) and remediation (d) may not be able to be accomplished according to identified timeframes (e.g., 30 days) due to systems needing to be in a static state throughout the duration of a given test event.

RA-5(4). VULNERABILITY SCANNING | DISCOVERABLE INFORMATION

Value Definition: The organization determines what information about the IS is discoverable by adversaries and subsequently takes [the following action: notifies the ISO/PM and AO].

RA-5(5). VULNERABILITY SCANNING | PRIVILEGED ACCESS

Value Definition: The IS implements privileged access authorization to [all ISs and infrastructure components] for [all vulnerability scanning activities that require privileged access].

SA-1. SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Guidance: This control is fully inherited due to all CCIs being accomplished at the DoD/ Organizational level (per the RMF KS).

SA-2. ALLOCATION OF RESOURCES

Guidance: Some of the CCIs for this control may be inherited from the Organization/ Component.

SA-3 a. SYSTEM DEVELOPMENT LIFE CYCLE

Guidance: Based upon DoD implementation guidance statements and refers to DoDI 8580.1, this control is primarily applicable to acquisition systems.

SC-1. SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Guidance: This control is fully inherited due to all CCIs being accomplished at the DoD/ Organizational level (per the RMF KS).

SC-5. DENIAL OF SERVICE PROTECTION

Guidance: This may be tailored out for ISOL and ISOL-ET systems due to the lack of connectivity with other systems.

Value Definition: The IS protects against or limits the effects of the following types of denial-of-service attacks: [internal and external denial of service attacks] by employing [settings identified in the applicable STIGs].

SC-5(1). DENIAL OF SERVICE PROTECTION | RESTRICT INTERNAL USERS

Tailoring Justification: Due to the lack of direct connectivity with other systems, this control is tailored out for ISOL and ISOL-ET system types.

Value Definition: The IS restricts the ability of individuals to launch [internally generated denial of service attacks] against other ISs.

SC-7 b. BOUNDARY PROTECTION

Tailoring Justification: Due to the lack of direct connectivity with other systems, this control is tailored out for ISOL and ISOL-ET system types.

SC-7(3). BOUNDARY PROTECTION | ACCESS POINTS

Tailoring Justification: Due to the lack of direct connectivity with other systems, this control is tailored out for ISOL and ISOL-ET system types.

SC-7(4). BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES

Tailoring Justification: Due to the lack of direct connectivity with other systems, this control is tailored out for ISOL and ISOL-ET system types.

SC-7(5). BOUNDARY PROTECTION | DENY BY DEFAULT/ALLOW BY EXCEPTION

Tailoring Justification: Due to the lack of direct connectivity with other systems, this control is tailored out for ISOL and ISOL-ET system types.

SC-7(7). BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES

Tailoring Justification: Due to the lack of direct connectivity with other systems, this control is tailored out for ISOL and ISOL-ET system types.

SC-7(8). BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS

Tailoring Justification: Due to lack of connectivity with other systems, this control is tailored out for ISOL and ISOL-ET systems.

SC-7(9). BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC

Tailoring Justification: Due to the lack of direct connectivity with other systems, this control is tailored out for ISOL and ISOL-ET system types.

SC-7(10). BOUNDARY PROTECTION | PREVENT UNAUTHORIZED EXFILTRATION

Tailoring Justification: Due to the lack of direct connectivity with other systems, this control is tailored out for ISOL and ISOL-ET system types.

SC-7(11). BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC

Tailoring Justification: Due to the lack of direct connectivity with other systems, this control is tailored out for ISOL and ISOL-ET system types.

Value Definition: The IS only allows incoming communications from [authorized sources as identified in the Ports, Protocols, and Services list] routed to [authorized destinations as identified in the Ports, Protocols, and Services list].

SC-7(13). BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS/ MECHANISMS/SUPPORT COMPONENTS

Guidance: This control is often tailored from physical isolation to virtual isolation, or tailored out on small and/or isolated RDT&E systems.

SC-7(14). BOUNDARY PROTECTION | PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTION

Guidance: The DoD has identified limited circumstances in which this control applies. When defining values and developing implementation strategies, all instances where incorrect connections between Information Systems operating at different levels (i.e., different classification levels and/or different compartments/caveats) could occur should be considered (i.e., any occasion when components of two or more systems under different authorization boundaries are in close enough proximity to allow for the possibility of inadvertent cross connections between them).

SC-8. TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Value Definition: The IS protects the [confidentiality and integrity] of transmitted information.

SC-17. PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Tailoring Justification: Due to lack of direct connectivity with other systems, this control is tailored out for ISOL and ISOL-ET systems.

Guidance: Public Key Infrastructure/Enabling (PKI/PKE) requirements may be tailored out for STD and No Gen systems if there is a lack of required connectivity to authoritative PKI/PKE sources.

SC-18(1). MOBILE CODE | IDENTIFY UNACCEPTABLE CODE/TAKE CORRECTIVE ACTIONS

Value Definition: The IS identifies [unacceptable mobile code defined in SC-18] and [blocks the unacceptable mobile code and all associated actions].

SC-18(3). MOBILE CODE | PREVENT DOWNLOADING/EXECUTION.

Value Definition: The IS prevents the download and execution of [any mobile code not identified in the software list].

Guidance: ISOL and ISOL-ET systems may tailor out the CCI relating to downloading (CCI 001169) due to the lack of direct connectivity with other systems.

SC-20. SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Tailoring Justification: Due to the lack of connectivity with authoritative domain name system (DNS) sources, this control is tailored out for ISOL and ISOL-ET system types.

SC-21. SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Tailoring Justification: Due to the lack of connectivity with authoritative DNS sources, this control is tailored out for ISOL and ISOL-ET system types.

Guidance: Secure DNS requirements are often tailored out for RDT&E systems if they lack connectivity with authoritative DNS sources.

SC-23(3). SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION

Value Definition: The IS generates a unique session identifier for each session with [configuration settings in accordance with applicable STIGs] and recognizes only session identifiers that are system-generated.

SC-23(5). SESSION AUTHENTICITY | ALLOWED CERTIFICATE AUTHORITIES

Tailoring Justification: Due to the lack of connectivity with a DoD PKI certificate authority, this control is tailored out for ISOL and ISOL-ET system types.

Guidance: Due to lack of required connectivity to DoD PKI certificate authorities, PKI certificate requirements are often tailored out.

SI-1. SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Guidance: This control is fully inherited due to all CCIs being accomplished at the DoD/ Organizational level (per the RMF KS).

SI-2(2). FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS

Guidance: This control is often tailored from automated to manual on small and/or isolated RDT&E systems.

SI-3(1). MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT

Guidance: This control is often tailored from automated to manual on small and/or isolated RDT&E systems.

SI-3(2). MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES

Guidance: This control is often tailored out on isolated RDT&E systems.

SI-4 b, g. INFORMATION SYSTEM MONITORING

Value Definitions:

b. Identifies unauthorized use of the IS through [review of all logs containing security-relevant information]

g. Provides [all relevant IS monitoring information] to [the AO, ISO, and ISSM] as needed; and [to support the investigation of suspected IS attacks, unauthorized usage, and unauthorized connections].

SI-4(1). INFORMATION SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM

Guidance: This control is often tailored out on small and/or isolated RDT&E systems.

SI-4(14). INFORMATION SYSTEM MONITORING | WIRELESS INTRUSION DETECTION

Tailoring Justification: For systems without wireless communication technologies (see 2.5), this control can be tailored out.

SI-4 (15). INFORMATION SYSTEM MONITORING | WIRELESS TO WIRELINE COMMUNICATIONS

Tailoring Justification: For systems without wireless communication technologies (see 2.5), this control can be tailored out.

SI-4(19). INFORMATION SYSTEM MONITORING | INDIVIDUALS POSING GREATER RISK

Guidance: If a senior official (e.g., AL, ISO, and Program Security Officer) has determined that there is a need for an elevated level of monitoring for an individual posing increased risk, a decision will also need to be made as to what the elevated monitoring will involve. This monitoring should be closely coordinated with management, legal, security, and human resources individuals.

SI-7. SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Value Definition: The organization employs integrity verification tools to detect unauthorized changes to [all security-relevant software, firmware, and settings].

SI-8. SPAM PROTECTION

Tailoring Justification: Spam protection is not applicable to RDT&E systems due to their relative isolation from email-connected systems.

SI-8(1). SPAM PROTECTION | CENTRAL MANAGEMENT

Tailoring Justification: Central management of spam protection is not applicable to RDT&E systems due to SI-8 being tailored out.

SI-8(2). SPAM PROTECTION | AUTOMATIC UPDATES

Tailoring Justification: Automatic updates of spam protection is not applicable to RDT&E systems due to SI-8 being tailored out.

SI-16. MEMORY PROTECTION

Value Definition: The IS implements [hardware- and/or software-enforced security safeguards (e.g., Data Execution Prevention and Address Space Layout Randomization] to protect its memory from unauthorized code execution.

This page intentionally left blank.

APPENDIX A

Citations

Committee on National Security Systems. *Committee on National Security Systems (CNSS) Glossary*. CNSSI 4009. 6 April 2015. May be superseded by update. Retrieved 4 June 2024. Available at https://www.cnss.gov/cnss/.

———. *Security Categorization and Control Selection for National Security Systems*. CNSSI 1253. 27 March 2014. May be superseded by update. Retrieved 4 June 2024. Available at https://www.dcsa.mil/portals/91/documents/ctp/nao/CNSSI_No1253.pdf.

DoD Risk Management Framework Knowledge Service. https://rmfks.osd.mil/rmf/Pages/default.aspx.

National Institute of Standards and Technology. *Security and Privacy Controls for Federal Information Systems and Organizations*. SP 800-53. April 2013. Updated 22 January 2015. Superseded by SP 800-53 Rev. 5, 23 September 2020. Superseding document retrieved 16 August 2021. Available at https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

*** * * END OF FILE * * ***