Controls Applicability Assessment For Naval Aviation Weapon Systems

NAVAIR Cyber Warfare Detachment

POC: David Burke, PhD, Technical Director

Accepted and agreed:

6/21/17

VADM P. A.GROSKLAGS, USN
Commander, Naval Air Systems Command
Functional Authorizing Official

date

6/15/17

RDML S. G. GAHAGAN, USN
Chief Engineer, Naval Air Systems Command
Functional Security Control Assessor

date

PROBLEM STATEMENT

NAVAIR initially lacked a comprehensive engineering analysis to support a robust implementation of NIST published Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP800-53R4). This was required to support control tailoring decisions for Risk Management Framework (RMF) and CYBERSAFE in NAVAIR weapon systems.

Consequently, NAVAIR conducted this control applicability assessment (CAA) to carefully assess each control relative to weapon system mission and operational needs. The goal was to identify the high value controls for each weapon system context: Manned Aircraft, Unmanned Air Vehicle, Unmanned Aircraft System (UAS) Control Segment, Support Equipment, and Shipboard Installed System. NAVAIR also assessed the difficulty of implementing each control in legacy systems. This assessment required the combination of aviation domain and cyber warfare expertise.

BACKGROUND

NIST SP800-53R4 was developed to further statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. The updated publication provides a holistic strategy (security controls) for protecting critical infrastructure and improving information security.

CNSS Instruction 1253, *Security Categorization and Control Selection for National Security Systems (NSS),* provides guidance on the categorization and selection of controls, and the selection and application of overlays, for NSS. As an example, the "Classified Overlay" identifies additional controls and enhancements that do not appear in CNSSI 1253 baseline sets. DoD Instruction 8500.01 further directs all DoD Information Systems and Platform IT systems to be categorized in accordance with CNSSI 1253 and implements corresponding controls (published in NIST SP800-53A) regardless of whether they are NSS or non-NSS.[1]

NIST SP 800-53R4 and CNSSI 1253 both allow for the application of "overlays" – controls, enhancements, formal guidance, and other supporting information that complement (and further refine) control baselines. Agencies may apply overlays and tailor controls in support of specialized requirements, business processes, unique missions and operational environments.

INTENT

The intent of this assessment is to create a reference engineering artifact that determines highest value controls for Naval Aviation Weapon Systems. It serves two purposes: provides a foundation for the development of Common Control Packages (CCP) to streamline the NAVAIR Assessment and Authorization (A&A) process and aids in program-specific tailoring of controls during RMF Step Two and overlays. NAVAIR overlays are domain specific sets of controls used to adjust the baseline set of controls. A CCP is a technique within RMF that allows for central management and compliant implementation of a set of controls each program can leverage during the tailoring process.

[1] DoD Instruction 8500.01, "Cybersecurity," March 14, 2014

APPLICABILITY AND SCOPE

The security controls are derived.[2] This assessment provides informative security control recommendations that will be used across NAVAIR to inform and guide decisions relative to the weapon systems' cybersecurity posture. In this manner, program managers can avoid performing an ad hoc assessment of every control during RMF Step 2, thus eliminating duplication of effort. By doing this work once, this assessment will accelerate the A&A process by streamlining RMF Steps One and Two. Furthermore, this assessment will provide consistency of control application and achieve efficiencies by moving towards a weapon system model that:

- Prioritizes all controls and identifies common control package groupings;
- Provides engineering justification for the creation of NAVAIR overlays; and
- Provides engineering reference artifacts to support program-specific tailoring.

NAVAIR has every expectation this document will result in significant time savings, facilitate transition to RMF, and support the integration of CYBERSAFE certifications and improve the cyber resiliency and survivability of platforms. This assessment is geared toward embedded weapon systems and may not be as applicable to enterprise IT systems[3].

METHODOLOGY

This assessment was performed by a cross functional team comprised of engineers, cybersecurity professionals and program representatives.[4] The team carefully reviewed and analyzed every security control to determine the value added within each of the contexts below:

Applicable to Manned Aircraft	Applicable to Unmanned Aircraft Vehicle	Applicable to Unmanned Aircraft Control Station	Applicable to Support Equipment	Applicable to Shipboard Embedded Systems	Difficulty with Legacy Systems

Assigned values (understanding the added value of the security controls within each IT context):

- Not Applicable: Control does not make sense in this context (*always tailored out*);
- Low value: Control technically feasible, but adds little or no cyber resiliency due to its overly enterprise IT centric focus (*usually tailored out*);
- Medium value: Control is a solid technique that improves cyber resiliency of systems and should be part of program trade space *(usually included);*
- High value: Control is a crucial technique that provides major improvement in cyber resiliency of NAVAIR systems (*always included*).

In addition to the value assessments above, the difficulty of applying each control to legacy systems was assessed. OSD defines legacy systems as those already fielded or in post Milestone B development.

[2] NIST 800-53 Rev. 4, Ch.1 "Security requirements are derived from mission/business needs, laws, Executive Orders, directives, regulations, policies, instructions, standards, guidance, and/or procedures"
[3] Enterprise IT systems to follow normal RMF process
[4] Representatives from Cyber Warfare Detachment, AIR-4.0P CYBERSAFE, AIR-1.0, AIR/AD-4.0, AIR-7.2.6

- High difficulty – expected to require significant reengineering and architectural change in a legacy weapon system
- Moderate difficulty – expected to require some modification to existing system
- Low difficulty – expected to require minor or no modification to the system, or addressed through process change

The goal behind tracking the difficulty of implementing each control for legacy systems was to bring some realism into feasibility in a fiscally constrained environment. This provides supporting information to assist with program return on investment decisions. As programs execute engineering change proposals (ECP), they should consider the full set of controls for incorporation during that design change, regardless of noted legacy difficulty.

TAILORING CONTROLS

The baseline review is the starting point for a tailoring process that results in a selected set of security controls that closely fits mission requirements and operational environments. Tailoring may occur throughout a system's lifecycle and can include:

- Applying scoping and compensating control guidance;
- Supplementing the baseline with a control or set of controls unique to mission, business functions, or operations;
- Assigning specific values to control parameters or modifying a control's parameters;
- Specifying minimum assurance requirements;
- Augmenting with any additional information relative to weapon systems; and
- Identifying common controls that may be inherited from other entities.
- Residual risk may be mitigated by adding controls or enhancing existing controls[5].

> NIST 800-53R4 delineates these seven tailoring steps and provides expanded guidance for tailoring baseline security controls. The tailoring process, as part of control selection, is part of a comprehensive organizational risk management process. Tailoring decisions should be defensible based on mission and business needs. *(Sec. 3.2, pg. 30-31 of NIST SP 800-53)*

GROUPINGS / COMMONALITIES (COMMON CONTROL PACKAGES)

During the assessment, 12 natural control groupings emerged, above and beyond the control family associations:

- Squadron Standard Operating Procedures (SOP) (~50 controls/enhancements)
- ACAS Usage, Threat Intelligence, NALCOMIS (~10 controls/enhancements)
- Systems Engineering Technical Review, DoD 5000 Series (~20 controls/enhancements)
- Safety and Environmental Protections (~10 controls/enhancements)
- Risk Management Framework Processes (~25 controls/enhancements)
- OPSEC Personnel Screening Processes (~20 controls/enhancements)
- Handling Classified Information SOP (~25 controls/enhancements)
- Configuration Management Processes (~10 controls/enhancements)

[5] NIST SP 800-53 Section 3.2, page 30

- Cyber Incident Response Team (~20 controls/enhancements)
- PKI Capability (~20 controls/enhancements)

All controls were assessed and determined to be value added; however, these controls are integrated into or complement existing DOD, DON and NAVAIR instructions, policies and procedures.

CONTROLS

NAVAIR developed a reference matrix to identify the various CNSSI 1253 baselines, overlays, and all controls. The final sets of overlays and common control packages were incorporated and met the intent of CNSSI 1253. Other sources were incorporated into the reference matrix for comparative analysis.

Each control was evaluated in terms of value added to each of the contexts. A control could be deemed high value in one area and not applicable in another. The difficulty of applying each control to legacy systems was captured as well (e.g., cost, schedule, performance). Throughout the analysis, candidate controls deemed of value were designated as possible common control packages.

ANALYSIS

Following is an analysis of every control contained in NIST 800-53R4, the qualitative values assigned and the rationale for these decisions. The intent is to use this rationale to aid system owners in determining the relevance or applicability of controls to their systems or the environments in which they operate. All high value controls must be implemented unless technically unfeasible. Medium controls are to be implemented, but are in the trade space based on availability of funds, time and technical feasibility. Low controls are not to be ignored; on the contrary, an evaluation should be performed to determine if one or more applies to specific components, technologies, or operating environments. The control may be of value and worth the additional time and investment.

This is a 'living document' designed to be reevaluated and updated as threat landscape evolves, technologies advance, and our experiences change.

CONTROLS

ACCESS CONTROL

AC-1	ACCESS CONTROL POLICY AND PROCEDURES
	Control: The organization: a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy [*Assignment: organization-defined frequency*]; and

	2. Access control procedures [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	All -1 are Medium, covered by policy. This is an assurance control supported by policy. Access control policy is defined by DoD, DON, PMAs, and squadrons.				

AC-2	**ACCOUNT MANAGEMENT**				
	Control: The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by [*Assignment: organization-defined personnel or roles]* for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*]; g. Monitors the use of information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 4. A valid access authorization; 5. Intended system usage; and 6. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements [*Assignment: organization-defined frequency];* and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	M	M	M
Difficulty w/Legacy	High – legacy systems may not have configured account types compliant with this control. Compliance with this control would likely require reengineering.				
Comments/ Rationale	Potential gap due to shared or group accounts; however, likely a mission requirement.				

AC-2(1)	ACCOUNT MANAGEMENT | *AUTOMATED SYSTEM ACCOUNT MANAGEMENT*				
	The organization employs automated mechanisms to support the management of information system accounts.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	N/A	L	L	L
Difficulty w/Legacy	High – few legacy systems have mechanisms to support automated account management.				
Comments/ Rationale	Low – there are a limited number of accounts in weapon systems, manageable in non-automated fashions. Not applicable to unmanned air vehicle, unless they have unique login to the system. Not applicable to systems using shared accounts; control assumes individual login.				

AC-2(2)	ACCOUNT MANAGEMENT | *REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*				
	The information system automatically [Selection: removes; disables] temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Weapon systems do not create temporary accounts; shared/group accounts avoid need.				

AC-2(3)	ACCOUNT MANAGEMENT | *DISABLE INACTIVE ACCOUNTS*				
	The information system automatically disables inactive accounts after [*Assignment: organization-defined time period*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	N/A	L	L	L
Difficulty w/Legacy	High – Compliance with this control would likely require reengineering.				
Comments/ Rationale	Not applicable to shared accounts. Low because there is a limited, controlled user community, partially mitigated by physical access controls.				

AC-2(4)	ACCOUNT MANAGEMENT | *AUTOMATED AUDIT ACTIONS*
	The information system automatically audits account creation, modification, enabling, disabling, and

	removal actions, and notifies [*Assignment: organization-defined personnel or roles*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High – Compliance with this control would likely require reengineering.				
Comments/ Rationale	STIG requirement meets the intent. Logging important, unclear how notification might work (possible an alert). AU-2/AU-12 If the underlying operating system is configured in accordance with the applicable STIG(s), during development, this control should be met.				

AC-2(5)	**ACCOUNT MANAGEMENT | *INACTIVITY LOGOUT***				
	The organization requires that users log out when [A*ssignment: organization-defined time-period of expected inactivity or description of when to log out*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	L	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	In the context of NAVAIR systems, applying this control would have an adverse impact on operator's ability to execute the mission. Mitigated by physical security controls.				

AC-2(6)	**ACCOUNT MANAGEMENT | *DYNAMIC PRIVILEGE MANAGEMENT***				
	The information system implements the following dynamic privilege management capabilities: [*Assignment: organization-defined list of dynamic privilege management capabilities*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High – Compliance with this control would likely require reengineering.				
Comments/ Rationale	Note: This control is not in any CNSSI 1253 profiles. Host Based Security System (HBSS) might do this function on alerts. Dynamic privilege capability not typically needed in weapon systems.				

AC-2(7)	**ACCOUNT MANAGEMENT | *ROLE-BASED SCHEMES***
	The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;

	(b) Monitors privileged role assignments; and (c) Takes [*Assignment: organization-defined actions*] when privileged role assignments are no longer appropriate.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low - Addressed in current practice of creating admin accounts vice user accounts.				
Comments/ Rationale	Operator/user accounts should not include privileged access/functions. Separate account should be created to support privileged access/functions.				

AC-2(8)	**ACCOUNT MANAGEMENT | *DYNAMIC ACCOUNT CREATION***				
	The information system creates [Assignment: organization-defined information system accounts] dynamically.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Dynamic account creation should be avoided! Greatly increases attack surface.				

AC-2(9)	**ACCOUNT MANAGEMENT | *RESTRICTIONS ON USE OF SHARED / GROUP ACCOUNTS***				
	The organization only permits the use of shared/group accounts that meet [*Assignment: organization-defined conditions for establishing shared/group accounts*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low - This is should already be addressed by systems using shared /group accounts.				
Comments/ Rationale	Not applicable if the systems do not use shared /group accounts. Care must be taken in creating shared /group accounts to ensure they are necessary mission requirements.				

AC-2(10)	**ACCOUNT MANAGEMENT | *SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION***
	The information system terminates shared/group account credentials when members leave the group.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low – termination of account credentials, although feasible, likely has significant mission impact.				
Comments/ Rationale	Not applicable to systems not using shared/group accounts; may apply to some group account architectures. Persistent group accounts should not be terminated; mitigated by physical and personnel controls.				

AC-2(11)	**ACCOUNT MANAGEMENT | *USAGE CONDITIONS***				
	The information system enforces [*Assignment: organization-defined circumstances and/or usage conditions]* for [*Assignment: organization-defined information system accounts*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High – Compliance with this control would likely require reengineering.				
Comments/ Rationale	Supplemental Guidance not applicable in military systems; control is not useful in military weapon systems.				

AC-2(12)	**ACCOUNT MANAGEMENT | *ACCOUNT MONITORING / ATYPICAL USAGE***				
	The organization: (a) Monitors information system accounts for [*Assignment: organization-defined atypical usage*]; and (b) Reports atypical usage of information system accounts to [*Assignment: organization-defined personnel or roles*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High – Compliance with this control would likely require reengineering.				
Comments/ Rationale	Dynamic notification may be impractical; logging may have value in certain situations.				

AC-2(13)	**ACCOUNT MANAGEMENT | *DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS***
	The organization disables accounts of users posing a significant risk within [*Assignment: organization-defined time period*] of discovery of the risk.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Addressed via military security vetting and personnel management.				

AC-3	**ACCESS ENFORCEMENT**				
	Control: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Permissions configured for user vs. admin accounts meet this requirement. Not applicable to flight deck. Makes sense for mission systems. UAS mission side might be High.				

AC-3(1) – Withdrawn

AC-3(2)	**ACCESS ENFORCEMENT | *DUAL AUTHORIZATION***				
	The information system enforces dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Not in CNSSI 1253; no examples of use. Typically covered by other operational processes for two-person integrity. This control will typically bring unsatisfactory operational constraints.				

AC-3(3)	**ACCESS ENFORCEMENT | *MANDATORY ACCESS CONTROL***
	The information system enforces [*Assignment: organization-defined mandatory access control policy*] over all subjects and objects where the policy: (a) Is uniformly enforced across all subjects and objects within the boundary of the information system;

	(b) Specifies that a subject that has been granted access to information is constrained from doing any of the following; **(1)** Passing the information to unauthorized subjects or objects; **(2)** Granting its privileges to other subjects; **(3)** Changing one or more security attributes on subjects, objects, the information system, or information system components; **(4)** Choosing the security attributes and attribute values to be associated with newly created or modified objects; or **(5)** Changing the rules governing access control; and (c) Specifies that [*Assignment: organization-defined subjects*] may explicitly be granted [*Assignment: organization-defined privileges (i.e., they are trusted subjects)*] such that they are not limited by some or all of the above constraints.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	L	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Not in CNSSI 1253, shows up in cross-domain solution (CDS) overlays. Makes sense for role determinations in systems with different security domains.				

AC-3(4)	**ACCESS ENFORCEMENT | *DISCRETIONARY ACCESS CONTROL***				
	The information system enforces [*Assignment: organization-defined 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: (a) Pass the information to any other subjects or objects; (b) Grant its privileges to other subjects; (c) Change security attributes on subjects, objects, the information system, or the information system's components; (d) Choose the security attributes to be associated with newly created or revised objects; or (e) Change the rules governing access control.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	L	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Permissions configured for user vs admin accounts meet this requirement (opposite of AC-3(3)).				

AC-3(5)	**ACCESS ENFORCEMENT | *SECURITY-RELEVANT INFORMATION***				
	The information system prevents access to [*Assignment: organization-defined security-relevant information*] except during secure, non-operable system states.				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Only in cross-domain solution (CDS) overlay, perhaps changing security settings (e.g. CDS rules) during operation; covered by router STIGs.				

AC-3(6) – Withdrawn

AC-3(7)	**ACCESS ENFORCEMENT | *ROLE-BASED ACCESS CONTROL***				
	The information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*Assignment: organization-defined roles and users authorized to assume such roles*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High – Compliance with this control would likely require reengineering.				
Comments/ Rationale	Role-based Access Control is a valid strategy, but brings with it additional administrative overhead. Recommended for new start programs. Very difficult to add to legacy platforms.				

AC-3(8)	**ACCESS ENFORCEMENT | *REVOCATION OF ACCESS AUTHORIZATIONS***				
	The information system enforces the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [*Assignment: organization-defined rules governing the timing of revocations of access authorizations*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High – Compliance with this control would likely require reengineering.				
Comments/ Rationale	Due to mission requirements, weapon systems do not typically desire this capability; mitigated by operational Standard Operating Procedures (SOP) and physical security controls.				

AC-3(9)	**ACCESS ENFORCEMENT | *CONTROLLED RELEASE***
	The information system does not release information outside of the established system boundary unless: (a) The receiving [*Assignment: organization-defined information system or system component*]

	provides [*Assignment: organization-defined security safeguards*]; and (b) [*Assignment: organization-defined security safeguards*] are used to validate the appropriateness of the information designated for release.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High – Compliance with this control would likely require reengineering.				
Comments/ Rationale	Note: Only in NC3 overlay. Controlling the data flow leaving a system is important; typically addressed by SOPs, rather than technical safeguards.				

AC-3(10)	**ACCESS ENFORCEMENT | *AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS***				
	The organization employs an audited override of automated access control mechanisms under [*Assignment: organization-defined conditions*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Note: The intent of this control is unclear; no foreseeable application in any NAVAIR systems.				

NAVAIR will not accredit cross-domain solution (CDS). As such, many of the AC-4 enhancements are marked as N/A [AC-4(2)-(5), (7)-(15), and (17)-(19)]. AC-4(20) is the key enhancement for NAVAIR systems to use approved CDS solutions.

AC-4	**INFORMATION FLOW ENFORCEMENT**				
	Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [*Assignment: organization-defined information flow control policies*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Has value to prevent unauthorized configuration changes. Router/switch STIG compliant configurations should meet this requirement.				

AC-4(1)	**INFORMATION FLOW ENFORCEMENT | *OBJECT SECURITY ATTRIBUTES***				
	The information system uses [*Assignment: organization-defined security attributes*] associated with [*Assignment: organization-defined information, source, and destination objects*] to enforce [*Assignment: organization-defined information flow control policies*] as a basis for flow control decisions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High – Many legacy systems do not have metadata for tracking the classification of data within their systems.				
Comments/ Rationale	Good security metadata tagging has a lot of value; difficult to implement in legacy systems.				

AC-4(2)	**INFORMATION FLOW ENFORCEMENT | *PROCESSING DOMAINS***				
	The information system uses protected processing domains to enforce [*Assignment: organization-defined information flow control policies]* as a basis for flow control decisions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	NA	NA	NA	NA	NA
Difficulty w/Legacy	N/A				
Comments/ Rationale	Only makes sense in cross-domain solution (CDS) systems; high assurance guards.				

AC-4(3)	**INFORMATION FLOW ENFORCEMENT | *DYNAMIC INFORMATION FLOW CONTROL***				
	The information system enforces dynamic information flow control based on [*Assignment: organization-defined policies*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Unlikely to ever make sense in a weapon system.				

AC-4(4)	**INFORMATION FLOW ENFORCEMENT | *CONTENT CHECK ENCRYPTED INFORMATION***				
	The information system prevents encrypted information from bypassing content-checking mechanisms by [Selection (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; [*Assignment: organization-defined procedure or method*]].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	NAVAIR specifically does not want to enforce content checking; this increases the attack surface.				

AC-4(5)	**INFORMATION FLOW ENFORCEMENT | *EMBEDDED DATA TYPES***				
	The information system enforces [*Assignment: organization-defined limitations*] on embedding data types within other data types.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not applicable to weapon systems; tied to boundary inspection tool limitations. Good for cross-domain solutions (CDS).				

AC-4(6)	**INFORMATION FLOW ENFORCEMENT | *METADATA***				
	The information system enforces information flow control based on [*Assignment: organization-defined metadata*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	N/A	L
Difficulty w/Legacy	High – Compliance with this control would likely require reengineering.				
Comments/ Rationale	Could be valuable for new systems; difficult for legacy.				

AC-4(7)	**INFORMATION FLOW ENFORCEMENT | *ONE-WAY FLOW MECHANISMS***

	The information system enforces [*Assignment: organization-defined one-way information flows*] using hardware mechanisms.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	This is a hardware diode; NAVAIR uses cross-domain solution (CDS). Other DoD entities handle CDS accreditation.				

AC-4(8)	**INFORMATION FLOW ENFORCEMENT | *SECURITY POLICY FILTERS***				
	The information system enforces information flow control using [*Assignment: organization-defined security policy filters*] as a basis for flow control decisions for [*Assignment: organization-defined information flows*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Typically handled by data validation guards, not as information flow enforcement. Other DoD entities handle cross-domain solution (CDS) accreditation.				

AC-4(9)	**INFORMATION FLOW ENFORCEMENT | *HUMAN REVIEWS***				
	The information system enforces the use of human reviews for [*Assignment: organization-defined information flows*] under the following conditions: [*Assignment: organization-defined conditions*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not applicable to weapon systems.				

AC-4(10)	**INFORMATION FLOW ENFORCEMENT | *ENABLE/DISABLE SECURITY POLICY FILTERS***
	The information system provides the capability for privileged administrators to enable/disable [*Assignment: organization-defined security policy filters*] under the following conditions:

	[*Assignment: organization-defined conditions*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not applicable to weapon systems.				

AC-4(11)	**INFORMATION FLOW ENFORCEMENT | *CONFIGURATION OF SECURITY POLICY FILTERS***				
	The information system provides the capability for privileged administrators to configure [*Assignment: organization-defined security policy filters*] to support different security policies.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not applicable to weapon systems.				

AC-4(12)	**INFORMATION FLOW ENFORCEMENT | *DATA TYPE IDENTIFIERS***				
	The information system, when transferring information between different security domains, uses [*Assignment: organization-defined data type identifiers*] to validate data essential for information flow decisions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not applicable, covered by metadata control AC-4(6).				

AC-4(13)	**INFORMATION FLOW ENFORCEMENT | *DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS***
	The information system, when transferring information between different security domains, decomposes information into [*Assignment: organization-defined policy-relevant subcomponents*] for

	submission to policy enforcement mechanisms.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not applicable to weapon systems.				

AC-4(14)	**INFORMATION FLOW ENFORCEMENT | *SECURITY POLICY FILTER CONSTRAINTS***				
	The information system, when transferring information between different security domains, implements [*Assignment: organization-defined security policy filters*] requiring fully enumerated formats that restrict data structure and content.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	For NAVAIR weapon systems, this is handled by data validation.				

AC-4(15)	**INFORMATION FLOW ENFORCEMENT | *DETECTION OF UNSANCTIONED INFORMATION***				
	The information system, when transferring information between different security domains, examines the information for the presence of [*Assignment: organized-defined unsanctioned information]* and prohibits the transfer of such information in accordance with the [Assignment: organization-defined security policy].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	For NAVAIR weapon systems, this is handled by data validation.				

AC-4(16) – Withdrawn

AC-4(17)	INFORMATION FLOW ENFORCEMENT | *DOMAIN AUTHENTICATION*				
	The information system uniquely identifies and authenticates source and destination points by [Selection (one or more): organization, system, application, individual] for information transfer.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not applicable to weapon systems.				

AC-4(18)	INFORMATION FLOW ENFORCEMENT | *SECURITY ATTRIBUTE BINDING*				
	The information system binds security attributes to information using [*Assignment: organization-defined binding techniques*] to facilitate information flow policy enforcement				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not applicable to weapon systems.				

AC-4(19)	INFORMATION FLOW ENFORCEMENT | *VALIDATION OF METADATA*				
	The information system, when transferring information between different security domains, applies the same security policy filtering to metadata as it applies to data payloads.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not applicable to weapon systems.				

AC-4(20)	INFORMATION FLOW ENFORCEMENT | *APPROVED SOLUTIONS*
	The organization employs [*Assignment: organization-defined solutions in approved configurations]* to control the flow of [*Assignment: organization-defined information*] across security domains.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR uses the Unified Cross Domain Management Office (UCDMO). This is the justification to mark many of the enhancements above as not applicable.				

AC-4(21)	**INFORMATION FLOW ENFORCEMENT | *PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS***				
	The information system separates information flows logically or physically using [*Assignment: organization-defined mechanisms and/or techniques*] to accomplish [*Assignment: organization-defined required separations by types of information*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	H	H	M	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Although typically associated with cross-domain solutions (CDS), this control has significant value in weapon systems when applied more broadly. For example, separating UAS flight commands and UAS mission system commands.				

AC-4(22)	**INFORMATION FLOW ENFORCEMENT | *ACCESS ONLY***				
	The information system provides access from a single device to computing platforms, applications, or data residing on multiple different security domains, while preventing any information flow between the different security domains.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	N/A	L
Difficulty w/Legacy	High – Compliance with this control would likely require reengineering.				
Comments/ Rationale	This control involves multiple independent levels of security systems. As most weapons systems operate at their highest security classification, this is less useful. More virtualized systems (particularly UAS) may use this more in the future.				

AC-5	**SEPARATION OF DUTIES**
	Control: The organization:

	a. Separates [*Assignment: organization-defined duties of individuals*]; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	This control primarily refers to the separation of user and admin privileges.				

Non-severable capability for least privilege means the following controls function together as one capability [AC-6, enhancements AC-6(1), AC-6(2), AC-6(5), and AC-6(10)].

AC-6	**LEAST PRIVILEGE**				
	Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Effectively tied to AC-5. NAVAIR separates duties based on least privilege.				

AC-6(1)	**LEAST PRIVILEGE | *AUTHORIZE ACCESS TO SECURITY FUNCTIONS***				
	The organization explicitly authorizes access to [*Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Captured in NAVAIR's method of creating admin accounts.				

AC-6(2)	LEAST PRIVILEGE | *NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*				
	The organization requires users of information system accounts, or roles, with access to [*Assignment: organization-defined security functions or security-relevant information*], use non-privileged accounts or roles, when accessing non-security functions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Captured in NAVAIR's method of creating admin accounts.				

AC-6(3)	LEAST PRIVILEGE | *NETWORK ACCESS TO PRIVILEGED COMMANDS*				
	The organization authorizes network access to [*Assignment: organization-defined privileged commands*] only for [*Assignment: organization-defined compelling operational needs*] and documents the rationale for such access in the security plan for the information system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Note: NIST 800-53 wording is weak; Control Correlation Identifiers (CCI) are more clear. Need clear operational requirement to justify network access to privileged commands.				

AC-6(4)	LEAST PRIVILEGE | *SEPARATE PROCESSING DOMAINS*				
	The information system provides separate processing domains to enable finer-grained allocation of user privileges.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Used on cross-domain solutions (CDS); not useful for typical weapon systems.				

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

	The organization restricts privileged accounts on the information system to [*Assignment: organization-defined personnel or roles*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	User should never have admin rights/privileges.				

AC-6(6)	**LEAST PRIVILEGE | *PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS***				
	The organization prohibits privileged access to the information system by non-organizational users.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale					

AC-6(7)	**LEAST PRIVILEGE | *REVIEW OF USER PRIVILEGES***				
	The organization: (a) Reviews [*Assignment: organization-defined frequency*] the privileges assigned to [*Assignment: organization-defined roles or classes of users]* to validate the need for such privileges; and (b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Less relevant to shared /group account environment; weapon systems are fairly static.				

AC-6(8)	**LEAST PRIVILEGE | *PRIVILEGE LEVELS FOR CODE EXECUTION***
	The information system prevents [*Assignment: organization-defined software*] from executing at higher privilege levels than users executing the software

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	STIG requirement and good practice.				

AC-6(9)	**LEAST PRIVILEGE | *AUDITING USE OF PRIVILEGED FUNCTIONS***				
	The information system audits the execution of privileged functions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	STIG requirements meet this control. Unclear from Control Correlation Identifier (CCI) what operational workload this may drive to systems in which a STIG does not exist.				

AC-6(10)	**LEAST PRIVILEGE | *PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS***				
	The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards / countermeasures				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Part of standard practice for user vs. admin accounts.				

AC-7	**UNSUCCESSFUL LOGON ATTEMPTS**
	Control: The information system: a. Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid logon attempts by a user during a [*Assignment: organization-defined time period*]; and b. Automatically [Selection: locks the account/node for an [*Assignment: organization-defined time period*]; locks the account/node until released by an administrator; delays next logon prompt according to [*Assignment: organization-defined delay algorithm*]] when the maximum number

	of unsuccessful attempts is exceeded.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	H	M
Difficulty w/Legacy	Low				
Comments/ Rationale	CCI-000043/44 sets the attempts to three. Tactical systems will need a higher number. Valuable control if properly scaled.				

AC-7(1) – Withdrawn

Mobile device clarification: weapon systems are not mobile devices. Some weapon systems have components that would qualify as mobile devices (e.g., electronic kneeboard, tactical UAS control segment).

AC-7(2)	**UNSUCCESSFUL LOGON ATTEMPTS | *PURGE / WIPE MOBILE DEVICE***				
	The information system purges/wipes information from [*Assignment: organization-defined mobile devices*] based on [*Assignment: organization-defined purging/wiping requirements/techniques*] after [*Assignment: organization-defined number*] consecutive, unsuccessful device logon attempts.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	M	L	N/A
Difficulty w/Legacy	Low				
Comments/ Rationale	Valid for true mobile devices (e.g. electronic kneeboard (EKB)). Not applicable to most weapon systems. Valid for tactical UAS control segments that might inadvertently be left behind or overrun.				

AC-8	**SYSTEM USE NOTIFICATION**
	<u>Control</u>: The information system: a. Displays to users [*Assignment: organization-defined system use notification message or banner*] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states : 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays system use information [*Assignment: organization-defined conditions*], before

	granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Standard DoD Warning Banner should meet this requirement. Does not actually stop anyone. Legal requirement, unlikely to tailor out.				

AC-9	**PREVIOUS LOGON (ACCESS) NOTIFICATION**				
	Control: The information system notifies the user, upon successful logon (access) to the system, of the date and time of the last logon (access).				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	This is not applicable to any systems using shared /group accounts, since operators unlikely to have the knowledge in re last valid login. Low value elsewhere, logging more useful.				

AC-9(1)	**PREVIOUS LOGON (ACCESS) NOTIFICATION | *UNSUCCESSFUL LOGONS***				
	The information system notifies the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	More useful than base control.				

AC-9(2)	**PREVIOUS LOGON (ACCESS) NOTIFICATION | *SUCCESSFUL / UNSUCCESSFUL LOGONS***
	The information system notifies the user of the number of [*Selection: successful logons/accesses;*

	unsuccessful logon/access attempts; both] during [*Assignment: organization-defined time period*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Combines base control and AC-9(1).				

AC-9(3)	**PREVIOUS LOGON (ACCESS) NOTIFICATION | *NOTIFICATION OF ACCOUNT CHANGES***				
	The information system notifies the user of changes to [*Assignment: organization-defined security-related characteristics/parameters of the user's account*] during [*Assignment: organization-defined time period*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Unclear as to what account changes would occur or make sense for weapon systems.				

AC-9(4)	**PREVIOUS LOGON (ACCESS) NOTIFICATION | *ADDITIONAL LOGON INFORMATION***				
	The information system notifies the user, upon successful logon (access), of the following additional information: [*Assignment: organization-defined information to be included in addition to the date and time of the last logon (access)*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Unclear as to what additional information might be useful.				

AC-10	**CONCURRENT SESSION LOCK**
	Control: The information system limits the number of concurrent sessions for each [*Assignment: organization-defined account and/or account type*] to [*Assignment: organization-defined number*].

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Without centralized authentication (e.g. domain controllers), very difficult to implement. Little usage of concurrent sessions in tactical weapon systems. This would lock an asset to a single session for group accounts if set to one (1).				

AC-11	**SESSION LOCK**				
	Control: The information system: a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	N/A	L	M	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	The ability to command a session lock can have some value, but must be balanced with operational constraints. Often not applicable to tactical platforms where delay in log-in could be unacceptable. No weapon system should have an inactivity logout.				

AC-11(1)	**SESSION LOCK | *PATTERN-HIDING DISPLAYS***				
	The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	N/A	L	M	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Any implementation of session lock should meet the pattern (data) hiding control.				

AC-12	**SESSION TERMINATION**
	Control: The information system automatically terminates a user session after [*Assignment:*

	organization-defined conditions or trigger events requiring session disconnect].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	L	N/A
Difficulty w/Legacy	Low				
Comments/ Rationale	Not applicable to weapon systems; could be used against NAVAIR. Useful for support equipment, but adds little beyond protection of session lock due to inactivity.				

AC-12(1)	**SESSION TERMINATION | *USER-INITIATED LOGOUTS / MESSAGE DISPLAYS***				
	The information system: (a) Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [*Assignment: organization-defined information resources*]; and (b) Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Where feasible, positive confirmation of log-out is a good feature.				

AC-13 – Withdrawn

AC-14	**PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION**				
	Control: The organization: a. Identifies [*Assignment: organization-defined user actions*] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/	Not applicable. Emergency stop switch (e-stop) type functionality should be viewed as a discrete				

Rationale	non-IT component of the control system, not a privileged command.

AC-14(1) – Withdrawn

AC-15 – Withdrawn

Non-severable classification marking capability (AC-16 and enhancements (1) through (5))

AC-16	**SECURITY ATTRIBUTES**				
	Control: The organization: a. Provides the means to associate [*Assignment: organization-defined types of security attributes*] having [*Assignment: organization-defined security attribute values*] with information in storage, in process, and/or in transmission; b. Ensures the security attribute associations are made and retained with the information; c. Establishes the permitted [*Assignment: organization-defined security attributes*] for [*Assignment: organization-defined information systems*]; and d. Determines the permitted [*Assignment: organization-defined values or ranges*] for each of the established security attributes.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Deals with classification markings (or FOUO, PII); policy defined.				

AC-16(1)	**SECURITY ATTRIBUTES | *DYNAMIC ATTRIBUTE ASSOCIATION***				
	The information system dynamically associates security attributes with [*Assignment: organization-defined subjects and objects*] in accordance with [*Assignment: organization-defined security policies*] as information is created and combined.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Should always be done, in accordance with policy.				

AC-16(2)	**SECURITY ATTRIBUTES | *ATTRIBUTE VALUE CHANGES BY AUTHORIZED***

	INDIVIDUALS				
	The information system provides authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated security attributes.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Key to implement base control.				

AC-16(3)	**SECURITY ATTRIBUTES | *MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY INFORMATION SYSTEM***				
	The information system maintains the association and integrity of [*Assignment: organization-defined security attributes*] to [*Assignment: organization-defined subjects and objects*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Key to implement base control.				

AC-16(4)	**SECURITY ATTRIBUTES | *ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS***				
	The information system supports the association of [*Assignment: organization-defined security attributes*] with [*Assignment: organization-defined subjects and objects*] by authorized individuals (or processes acting on behalf of individuals).				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Key to implement base control.				

AC-16(5)	**SECURITY ATTRIBUTES | *ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES***

	The information system displays security attributes in human-readable form on each object the system transmits to output devices to identify [*Assignment: organization-identified special dissemination, handling, or distribution instructions*] using [*Assignment: organization-identified human-readable, standard naming conventions*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Key to implement base control. NAVAIR systems use banners.				

AC-16(6)	**SECURITY ATTRIBUTES | *MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION***				
	The organization allows personnel to associate, and maintain the association of [*Assignment: organization-defined security attributes*] with [*Assignment: organization-defined subjects and objects*] in accordance with [*Assignment: organization-defined security policies*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Manual security classification tagging process.				

AC-16(7)	**SECURITY ATTRIBUTES | *CONSISTENT ATTRIBUTE INTERPRETATION***				
	The organization provides a consistent interpretation of security attributes transmitted between distributed information system components				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Defined by classification policy.				

AC-16(8)	**SECURITY ATTRIBUTES | *ASSOCIATION TECHNIQUES / TECHNOLOGIES***

	The information system implements [*Assignment: organization-defined techniques or technologies*] with [*Assignment: organization-defined level of assurance*] in associating security attributes to information				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Due to existing SOPs and policies for handling classified material, NAVAIR systems typically do not need to provide this control; NAVAIR does not worry much about tampering of security markings.				

AC-16(9)	**SECURITY ATTRIBUTES | *ATTRIBUTE REASSIGNMENT***				
	The organization ensures security attributes associated with information are reassigned only via re-grading mechanisms validated using [*Assignment: organization-defined techniques or procedures*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Unclear how this differs from AC-16(2).				

AC-16(10)	**SECURITY ATTRIBUTES | *ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS***				
	The information system provides authorized individuals the capability to define or change the type and value of security attributes available for association with subjects and objects.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Unclear how this differs from AC-16(2).				

AC-17	**REMOTE ACCESS**
	Control: The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and

	implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	To align with Cyber Risk Assessment (CRA) approach, this should be viewed as all data streams entering the system, not just User Name/Password (UN/PW) type logins.				

AC-17(1)	**REMOTE ACCESS | *AUTOMATED MONITORING / CONTROL***				
	The information system monitors and controls remote access methods.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Difficult to monitor without centralized authentication servers.				

AC-17(2)	**REMOTE ACCESS | *PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION***				
	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	In general, great practice. Cyber Risk Assessment tries to identify unencrypted system inputs. Some data streams may only be available unencrypted. UN/PW type logins should always be over encrypted tunnels. Most weapon system Radio Frequency (RF)/remote connections will have to be encrypted due to classification regardless of this control.				

AC-17(3)	**REMOTE ACCESS | *MANAGED ACCESS CONTROL POINTS***
	The information system routes all remote accesses through [*Assignment: organization-defined number*] managed network access control points.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Overly enterprise IT centric. Not recommended for weapon systems; could drive single points of failure.				

AC-17(4)	**REMOTE ACCESS | *PRIVILEGED COMMANDS / ACCESS***				
	The organization: (a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [*Assignment: organization-defined needs*]; and (b) Documents the rationale for such access in the security plan for the information system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Valid for NAVAIR systems. Items such as Link16 would be exempt since they do not have priv. commands. UAS Command and Control (C2) commands could still be considered priv.				

AC-17(5) – Withdrawn

AC-17(6)	**REMOTE ACCESS | *PROTECTION OF INFORMATION***				
	The organization ensures users protect information about remote access mechanisms from unauthorized use and disclosure.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	User training. For weapon systems, this also falls under handling sensitive information.				

AC-17(7) – Withdrawn

AC-17(8) – Withdrawn

AC-17(9)	REMOTE ACCESS | *DISCONNECT / DISABLE ACCESS*				
	The organization provides the capability to expeditiously disconnect or disable remote access to the information system within [*Assignment: organization-defined time period*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	M	M
Difficulty w/Legacy	High – Compliance with this control would likely require reengineering				
Comments/ Rationale	Key feature needed to be able to sever external data streams. Legacy systems not often structured to provide capability.				

AC-18	WIRELESS ACCESS				
	Control: The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and b. Authorizes wireless access to the information system prior to allowing such connections.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Encompasses all Radio Frequency (RF) connections (not just 802.11).				

AC-18(1)	WIRELESS ACCESS | *AUTHENTICATION AND ENCRYPTION*				
	The information system protects wireless access to the system using authentication of [*Selection (one or more): users; devices*] and encryption.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Closely linked with AC-17(2), same comments apply. Some data may have to be handled unencrypted.				

AC-18(2) – Withdrawn

AC-18(3)	WIRELESS ACCESS | *DISABLE WIRELESS NETWORKING*				
	The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Key part of base control.				

AC-18(4)	WIRELESS ACCESS | *RESTRICT CONFIGURATIONS BY USERS*				
	The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Typically covered by operational procedures and roles/responsibilities.				

AC-18(5)	WIRELESS ACCESS | *ANTENNAS / TRANSMISSION POWER LEVELS*				
	The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Typically covered by TEMPEST and Emissions Control (EMCON) requirements.				

AC-19	ACCESS CONTROL FOR MOBILE DEVICES
	Control: The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and

	implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	M	M	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Valid for true mobile devices (e.g. Electronic Kneeboard (EKB)); not applicable to most weapon systems. Valid for tactical UAS control segments that might get left behind or overrun.				

AC-19(1) – Withdrawn

AC-19(2) – Withdrawn

AC-19(3) – Withdrawn

AC-19(4)	**ACCESS CONTROL FOR MOBILE DEVICES | *RESTRICTIONS FOR CLASSIFIED INFORMATION***				
	The organization: (a) Prohibits the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official; and (b) Enforces the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information: **(1)** Connection of unclassified mobile devices to classified information systems is prohibited; **(2)** Connection of unclassified mobile devices to unclassified information systems requires approval from the authorizing official; **(3)** Use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited; and **(4)** Unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by [*Assignment: organization-defined security officials*], and if classified information is found, the incident handling policy is followed. (c) Restricts the connection of classified mobile devices to classified information systems in accordance with [*Assignment: organization-defined security policies*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Addressed in policy and training. Note: Context of this enhancement is broader than base control.				

AC-19(5)	**ACCESS CONTROL FOR MOBILE DEVICES | *FULL DEVICE / CONTAINER-BASED ENCRYPTION***				
	The organization employs [*Selection: full-device encryption; container encryption*] to protect the confidentiality and integrity of information on [*Assignment: organization-defined mobile devices*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	For mobile devices. Not applicable to weapon systems. Military systems should perform full disk style encryption.				

AC-20	**USE OF EXTERNAL INFORMATION SYSTEMS**				
	Control: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from external information systems; and b. Process, store, or transmit organization-controlled information using external information systems.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Cyber Risk Assessment (CRA) works to identify such connections. Important to track all of them.				

AC-20(1)	**USE OF EXTERNAL INFORMATION SYSTEMS | *LIMITS ON AUTHORIZED USE***				
	The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: (a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or (b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H

Difficulty w/Legacy	Moderate
Comments/ Rationale	Policy portion of base control.

AC-20(2)	**USE OF EXTERNAL INFORMATION SYSTEMS | *PORTABLE STORAGE DEVICES***				
	The organization [*Selection: restricts; prohibits*] the use of organization-controlled portable storage devices by authorized individuals on external information systems.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Addressed in policy and training: Do not use government hard drive at home for personal use.				

AC-20(3)	**USE OF EXTERNAL INFORMATION SYSTEMS | *NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES***				
	The organization [*Selection: restricts; prohibits*] the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Addressed in policy and training: Do not allow non-government devices on government equipment.				

AC-20(4)	**USE OF EXTERNAL INFORMATION SYSTEMS | *NETWORK ACCESSIBLE STORAGE DEVICES***				
	The organization prohibits the use of [*Assignment: organization-defined network accessible storage devices*] in external information systems.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	M	L
Difficulty w/Legacy	High				

Comments/ Rationale	Should only allow external accessible network storage devices specific to operational requirements (e.g. maintenance). Control language is all or nothing ("prohibit"). Only those connections deemed operationally necessary should be allowed; all others should be prohibited.

AC-21	**INFORMATION SHARING**				
	Control: The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [*Assignment: organization-defined information sharing circumstances where user discretion is required*]; and b. Employs [*Assignment: organization-defined automated mechanisms or manual processes*] to assist users in making information sharing/collaboration decisions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Required for classified information, defined by policy.				

AC-21(1)	**INFORMATION SHARING | *AUTOMATED DECISION SUPPORT***				
	The information system enforces information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Automated processes can be difficult and expensive to implement.				

AC-21(2)	**INFORMATION SHARING | *INFORMATION SEARCH AND RETRIEVAL***				
	The information system implements information search and retrieval services that enforce [*Assignment: organization-defined information sharing restrictions*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A

Difficulty w/Legacy	Low
Comments/ Rationale	Not applicable. NAVAIR handles by isolation between classification levels.

AC-22	**PUBLICLY ACCESSIBLE CONTENT**				
	Control: The organization: a. Designates individuals authorized to post information onto a publicly accessible information system; b. Trains authorized individuals to ensure publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure nonpublic information is not included; and d. Reviews the content on the publicly accessible information system for nonpublic information [*Assignment: organization-defined frequency*] and removes such information, if discovered.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	N/A	N/A
Difficulty w/Legacy	High				
Comments/ Rationale	Most weapon systems have no reason to provide publicly accessible data. May make sense for providing data to non-DOD entities for humanitarian relief operations.				

AC-23	**DATA MINING PROTECTION**				
	Control: The organization employs [*Assignment: organization-defined data mining prevention and detection techniques*] for [*Assignment: organization-defined data storage objects*] to adequately detect and protect against data mining.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not applicable to tactical systems. Still applicable to publically exposed acquisition websites (out of scope for this assessment).				

AC-24	**ACCESS CONTROL DECISIONS**				
	Control: The organization establishes procedures to ensure [*Assignment: organization-defined access control decisions*] are applied to each access request prior to access enforcement.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C	Applicable Unmanned A/C	Applicable Support	Applicable Shipboard

		Vehicle	Control Station	Equipment	Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not applicable to tactical weapon systems. Operational requirements may implement separation of duties for other reasons.				

AC-24(1)	**ACCESS CONTROL DECISIONS | *TRANSMIT ACCESS AUTHORIZATION INFORMATION***				
	The information system transmits [*Assignment: organization-defined access authorization information*] using [*Assignment: organization-defined security safeguards*] to [*Assignment: organization-defined information systems*] that enforce access control decisions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

AC-24(2)	**ACCESS CONTROL DECISIONS | *NO USER OR PROCESS IDENTITY***				
	The information system enforces access control decisions based on [*Assignment: organization-defined security attributes*] that do not include the identity of the user or process acting on behalf of the user.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not applicable to tactical systems. Anonymous reporting mechanisms already operationally supported (e.g., IG hotline, whistleblower safeguards)				

AC-25	**REFERENCE MONITOR**				
	Control: The information system implements a reference monitor for [*Assignment: organization-defined access control policies*] that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Assurance control for AC-2/AC-3. Very costly for tactical systems.				

AWARENESS AND TRAINING

AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES				
	Control: The organization: a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy [*Assignment: organization-defined frequency*]; and 2. Security awareness and training procedures [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** All -1 are Medium; covered by policy.				

AT-2	SECURITY AWARENESS TRAINING				
	Control: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. [*Assignment: organization-defined frequency*] thereafter.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** Covered by standard IA/CS training.				

AT-2(1)	SECURITY AWARENESS TRAINING | *PRACTICAL EXERCISES*				
	The organization includes practical exercises in security awareness training that simulate actual cyber-attacks.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded

					Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** Covered by standard Navy IA/CS training (CBT go through the rooms); weapon system specific cyber-attack exercises could be higher value (likely captured by AT-3(3).				

AT-2(2)	**SECURITY AWARENESS TRAINING | *INSIDER THREAT***				
	The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** Covered by standard Navy IA/CS training, CBT Cybersecurity Refresher, more depth in CBT for Insider Threats.				

AT-3	**ROLE-BASED SECURITY TRAINING**				
	Control: The organization provides role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. [*Assignment: organization-defined frequency*] thereafter.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by standard Navy IA/CS training for broad application. Focusing on Sys admin type roles would push this higher (e.g. change mentality to security over make it work).				

AT-3(1)	**ROLE-BASED SECURITY TRAINING | *ENVIRONMENTAL CONTROLS***
	The organization provides [*Assignment: organization-defined personnel or roles*] with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of environmental controls.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Limited improvement in cyber resiliency; critical for operator safety. Covered by operational procedures and Naval Air Training and Operating Procedures Standardization (NATOPS) in the fleet.				

AT-3(2)	**ROLE-BASED SECURITY TRAINING | *PHYSICAL SECURITY CONTROLS***				
	The organization provides [*Assignment: organization-defined personnel or roles*] with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of physical security controls.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by operational procedures.				

AT-3(3)	**ROLE-BASED SECURITY TRAINING | *PRACTICAL EXERCISES***				
	The organization includes practical exercises in security training that reinforce training objectives.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR should do more of this in its weapon system programs (“play like you practice”).				

AT-3(4)	**ROLE-BASED SECURITY TRAINING | *SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR***
	The organization provides training to its personnel on [*Assignment: organization-defined indicators of malicious code]* to recognize suspicious communications and anomalous behavior in organizational information systems.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Need vigilant operators to detect anomalous behavior as a precursor to a full cyber-attack. Legacy systems lack sensor capability to provide much info to operators (hence high difficulty). Major issue with high false positive rate. Need effort to determine what normal is.				

AT-4	**SECURITY TRAINING RECORDS**				
	Control: The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for [*Assignment: organization-defined time period*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Not listed in the draft overlay, but would be covered by NATOPS or General Military Training (GMT) Jacket. Auditable component for AT-2 and AT-3. Could be higher if it included the feedback loop for AT-3(3) to improve processes.				

AT-5 – Withdrawn

AUDIT AND ACCOUNTABILITY

AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES				
	Control: The organization: a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Reviews and updates the current: 1. Audit and accountability policy [*Assignment: organization-defined frequency*]; and 2. Audit and accountability procedures [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	All -1 are Medium, covered by policy.				

AU-2	AUDIT EVENTS				
	Control: The organization: a. Determines the information system is capable of auditing the following events: [*Assignment: organization-defined auditable events*]; b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines the following events are to be audited within the information system: [*Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Note: having auditable records will be key for NAVAIR Cyber Incident Response Team (CIRT) activities. This control is passive and does not direct what should be auditable.				

AU-2(1) – Withdrawn

AU-2(2) – Withdrawn

AU-2(3)	**AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES | *REVIEWS AND UPDATES***				
	The organization reviews and updates the audited events [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Part of Continuous Monitoring process (typically annually) and good system engineering.				

AU-2(4) – Withdrawn

AU-3	**CONTENT OF AUDIT RECORDS**				
	Control: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Closely tied with AU-2 (content of records).				

AU-3(1)	**CONTENT OF AUDIT RECORDS | *ADDITIONAL AUDIT INFORMATION***				
	The information system generates audit records containing the following additional information: [*Assignment: organization-defined additional, more detailed information*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	This control requires more implementation guidance. If NAVAIR addresses this as mission related information (e.g. aircraft location), this may not be a variable of which a specific information system				

	would be aware. Likely low value without guidance; could be much higher if tailored implementation guidance provided.

AU-3(2)	**CONTENT OF AUDIT RECORDS | *CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT***				
	The information system provides centralized management and configuration of the content to be captured in audit records generated by [*Assignment: organization-defined information system components*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Expect squadron/detachment/operational level would fulfill "centrally managed" aspect of this control for NAVAIR systems. (PMA may also fulfill for NAVAIR systems.)				

AU-4	**AUDIT STORAGE CAPACITY**				
	Control: The organization allocates audit record storage capacity in accordance with [*Assignment: organization-defined audit record storage requirements*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Closely tied to AU-2 (content of records) and AU-11 (time of retention). Operational restrictions are important due to different deployments and operational settings. Business IT systems do not typically DET to foreign countries.				

AU-4(1)	**AUDIT STORAGE CAPACITY | *TRANSFER TO ALTERNATE STORAGE***				
	The information system off-loads audit records [*Assignment: organization-defined frequency*] onto a different system or media than the system being audited.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				

Comments/ Rationale	This control is the moving of logs from the operational asset to a local repository. This is how NAVAIR systems handle logs operationally (typically every flight), although it is best if programs move beyond event triggered retention.

AU-5	**RESPONSE TO AUDIT PROCESSING FAILURES**				
	Control: The information system: a. Alerts [*Assignment: organization-defined personnel or roles*] in the event of an audit processing failure; and b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Part of the overall audit structure. Needs to be balanced with operational settings and tempo.				

AU-5(1)	**RESPONSE TO AUDIT PROCESSING FAILURES | *AUDIT STORAGE CAPACITY***				
	The information system provides a warning to [*Assignment: organization-defined personnel, roles, and/or locations*] within [*Assignment: organization-defined time period*] when allocated audit record storage volume reaches [*Assignment: organization-defined percentage*] of repository maximum audit record storage capacity.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Useful to alert operator when storage is getting full. Overwrite versus stop logging should be default behavior.				

AU-5(2)	**RESPONSE TO AUDIT PROCESSING FAILURES | *REAL-TIME ALERTS***				
	The information system provides an alert in [*Assignment: organization-defined real-time period*] to [*Assignment: organization-defined personnel, roles, and/or locations*] when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded

					Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	In an operational setting, audit capability likely not an "urgent" message.				

AU-5(3)	**RESPONSE TO AUDIT PROCESSING FAILURES | *CONFIGURABLE TRAFFIC VOLUME THRESHOLDS***				
	The information system enforces configurable network communications traffic volume thresholds reflecting limits on auditing capacity and [Selection: rejects; delays] network traffic above those thresholds.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	L
Difficulty w/Legacy	High				
Comments/ Rationale	This is an overly enterprise IT control for data volume control on large numbers of clients. Perhaps applicable to shipboard embedded systems.				

AU-5(4)	**RESPONSE TO AUDIT PROCESSING FAILURES | *SHUTDOWN ON FAILURE***				
	The information system invokes a [Selection: full system shutdown; partial system shutdown; degraded operational mode with limited mission/business functionality available] in the event of [*Assignment: organization-defined audit failures*], unless an alternate audit capability exists.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Failure of audit process should not affect mission critical functions.				

AU-6	**AUDIT REVIEW, ANALYSIS, AND REPORTING**
	Control: The organization: a. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*]; and b. Reports findings to [*Assignment: organization-defined personnel or roles*].

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	This is this log review. Must be balanced with operational bandwidth and cost; seven-day timeline from DoD likely too frequent.				

AU-6(1)	**AUDIT REVIEW, ANALYSIS, AND REPORTING | *PROCESS INTEGRATION***				
	The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Lack of persistent connectivity makes most automated mechanisms infeasible**.**				

AU-6(2) – Withdrawn

AU-6(3)	**AUDIT REVIEW, ANALYSIS, AND REPORTING | *CORRELATE AUDIT REPOSITORIES***				
	The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

AU-6(4)	**AUDIT REVIEW, ANALYSIS, AND REPORTING | *CENTRAL REVIEW AND ANALYSIS***				
	The information system provides the capability to centrally review and analyze audit records from multiple components within the system.				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	L	L	L	L	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Refer to base control.				

AU-6(5)	**AUDIT REVIEW, ANALYSIS, AND REPORTING | *INTEGRATION / SCANNING AND MONITORING CAPABILITIES***				
	The organization integrates analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; information system monitoring information; [*Assignment: organization-defined data/information collected from other sources*]] to further enhance the ability to identify inappropriate or unusual activity.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	M	L	M
Difficulty w/Legacy	High				
Comments/ Rationale	Maintaining situational awareness inside NAVAIR weapon systems is useful, but most tactical systems do not have useful scanners available.				

AU-6(6)	**AUDIT REVIEW, ANALYSIS, AND REPORTING | *CORRELATION WITH PHYSICAL MONITORING***				
	The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Reference visitor logs at squadrons, varies by location and levels of rigor.				

AU-6(7)	**AUDIT REVIEW, ANALYSIS, AND REPORTING | *PERMITTED ACTIONS***
	The organization specifies the permitted actions for each [Selection (one or more): information system process; role; user] associated with the review, analysis, and reporting of audit information.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Admin privileges required to modify logs.				

AU-6(8)	**AUDIT REVIEW, ANALYSIS, AND REPORTING | *FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS***				
	The organization performs a full text analysis of audited privileged commands in a physically distinct component or subsystem of the information system, or other information system that is dedicated to that analysis.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Likely to create significant overhead.				

AU-6(9)	**AUDIT REVIEW, ANALYSIS, AND REPORTING | *CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES***				
	The organization correlates information from nontechnical sources with audit information to enhance organization-wide situational awareness.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Likely to create significant overhead.				

AU-6(10)	**AUDIT REVIEW, ANALYSIS, AND REPORTING | *AUDIT LEVEL ADJUSTMENT***
	The organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information**.**

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	This is the ability to modify audit scope. Valid given changing threat postures and new intelligence. Frequency modification does not require an automated mechanism.				

AU-7	**AUDIT REDUCTION AND REPORT GENERATION**				
	Control: The information system provides an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Assumes enterprise IT construct and central repositories. Due to limited number of weapon systems, this is not as much of a concern.				

AU-7(1)	**AUDIT REDUCTION AND REPORT GENERATION | *AUTOMATIC PROCESSING***				
	The information system provides the capability to process audit records for events of interest based on [*Assignment: organization-defined audit fields within audit records*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Automated processes difficult and expensive.				

AU-7(2)	**AUDIT REDUCTION AND REPORT GENERATION | *AUTOMATIC SORT AND SEARCH***				
	The information system provides the capability to sort and search audit records for events of interest based on the content of [*Assignment: organization-defined audit fields within audit records*].				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Likely supported by any log management tool.				

AU-8	**TIME STAMPS**				
	Control: The information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [*Assignment: organization-defined granularity of time measurement*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Typically, GPS is the authoritative source. Some consideration should be given to variations in time stamp source disparity in disconnected weapon systems.				

AU-8(1)	**TIME STAMPS | *SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE***				
	The information system: (a) Compares the internal information system clocks [*Assignment: organization-defined frequency]* with [*Assignment: organization-defined authoritative time source*]; and (b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [*Assignment: organization-defined time period*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Typically, GPS is the authoritative source.				

AU-8(2)	**TIME STAMPS | *SECONDARY AUTHORITATIVE TIME SOURCE***
	The information system identifies a secondary authoritative time source that is located in a different

	geographic region than the primary authoritative time source.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	From an audit perspective, not very useful to weapon systems. Some weapons systems may have separate time source.				

AU-9	**PROTECTION OF AUDIT INFORMATION**				
	Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Good to protect audit records.				

AU-9(1)	**PROTECTION OF AUDIT INFORMATION | *HARDWARE WRITE-ONCE MEDIA***				
	The information system writes audit trails to hardware-enforced, write-once media.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Not operationally valid due to logistics concerns for deployed systems.				

AU-9(2)	**PROTECTION OF AUDIT INFORMATION | *AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS***				
	The information system backs up audit records [*Assignment: organization-defined frequency*] onto a physically different system or system component than the system or component being audited.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C	Applicable Unmanned A/C	Applicable Support	Applicable Shipboard

		Vehicle	Control Station	Equipment	Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Not operationally valid due to Size, Weight and Power (SWaP) concerns.				

AU-9(3)	**PROTECTION OF AUDIT INFORMATION | *CRYPTOGRAPHIC PROTECTION***				
	The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Difficult to implement on tactical systems. Mitigated by physical security controls and requirements for handling National Security Systems data.				

AU-9(4)	**PROTECTION OF AUDIT INFORMATION | *ACCESS BY SUBSET OF PRIVILEGED USERS***				
	The organization authorizes access to management of audit functionality to only [*Assignment: organization-defined subset of privileged users*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Relates to Insider Threat. Valid to have admin-only access.				

AU-9(5)	**PROTECTION OF AUDIT INFORMATION | *DUAL AUTHORIZATION***				
	The organization enforces dual authorization for [Selection (one or more): movement; deletion] of [*Assignment: organization-defined audit information*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems

	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Not operationally relevant.				

AU-9(6)	**PROTECTION OF AUDIT INFORMATION | *READ ONLY ACCESS***				
	The organization authorizes read-only access to audit information to [*Assignment: organization-defined subset of privileged users*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Not operationally relevant.				

AU-10	**NON-REPUDIATION**				
	Control: The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [*Assignment: organization-defined actions to be covered by non-repudiation*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Very difficult to do for shared /group accounts (effectively not applicable). Valid for individual accounts with Personal Identity Verification (PIV).				

AU-10(1)	**NON-REPUDIATION | *ASSOCIATION OF IDENTITIES***				
	The information system: (a) Binds the identity of the information producer with the information to [*Assignment: organization-defined strength of binding*]; and (b) Provides the means for authorized individuals to determine the identity of the producer of the information.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems

	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

AU-10(2)	**NON-REPUDIATION | *VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY***				
	The information system: (a) Validates the binding of the information producer identity to the information at [*Assignment: organization-defined frequency*]; and (b) Performs [Assignment: organization-defined actions] in the event of a validation error.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

AU-10(3)	**NON-REPUDIATION | *CHAIN OF CUSTODY***				
	The information system maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

AU-10(4)	**NON-REPUDIATION | *VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY***				
	The information system: (a) Validates the binding of the information reviewer identity to the information at the transfer or release points prior to release/transfer between [*Assignment: organization-defined security domains*]; and (b) Performs [*Assignment: organization-defined actions*] in the event of a validation error.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded

					Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

AU-10(5) – Withdrawn

AU-11	**AUDIT RECORD RETENTION**				
	Control: The organization retains audit records for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Valid to retain audit records.				

AU-11(1)	**AUDIT RECORD RETENTION | *LONG-TERM RETRIEVAL CAPABILITY***				
	The organization employs [*Assignment: organization-defined measures*] to ensure long-term audit records generated by the information system can be retrieved.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Valid to ensure formats are supported.				

AU-12	**AUDIT GENERATION**
	Control: The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [*Assignment: organization-defined information system components*]; b. Allows [*Assignment: organization-defined personnel or roles*] to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Important to generate audit records.				

AU-12(1)	**AUDIT GENERATION | *SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL***				
	The information system compiles audit records from [*Assignment: organization-defined information system components*] into a system-wide (logical or physical) audit trail that is time-correlated to within [*Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Per timestamp control (AU-8).				

AU-12(2)	**AUDIT GENERATION | *STANDARDIZED FORMATS***				
	The information system produces a system-wide (logical or physical) audit trail composed of audit records in a standardized format.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Good to have standard format; not as critical for systems doing local audits as standard practice. Unique audit formats may be needed for tactical systems.				

AU-12(3)	**AUDIT GENERATION | *CHANGES BY AUTHORIZED INDIVIDUALS***
	The information system provides the capability for [*Assignment: organization-defined individuals or roles*] to change the auditing to be performed on [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined selectable event criteria*] within [*Assignment: organization-defined time thresholds*].

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Effectively part of AU-7, allows audit scoping.				

AU-13	**MONITORING FOR INFORMATION DISCLOSURE**				
	The organization monitors [*Assignment: organization-defined open source information and/or information sites*] [*Assignment: organization-defined frequency*] for evidence of unauthorized disclosure of organizational information				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Not applicable to weapon systems. Naval Criminal Investigative Service (NCIS) covers part of this scope.				

AU-13(1)	**MONITORING FOR INFORMATION DISCLOSURE | *USE OF AUTOMATED TOOLS***				
	The organization employs automated mechanisms to determine if organizational information has been disclosed in an unauthorized manner.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Refer to base control.				

AU-13(2)	**MONITORING FOR INFORMATION DISCLOSURE | *REVIEW OF MONITORED SITES***				
	The organization reviews the open source information sites being monitored [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C	Applicable Unmanned A/C	Applicable Support	Applicable Shipboard

		Vehicle	Control Station	Equipment	Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Refer to base control.				

AU-14	**SESSION AUDIT**				
	Control: The information system provides the capability for authorized users to select a user session to capture/record or view/hear.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	High				
Comments/ Rationale	Adds attack surface for tactical systems. Must be behind Computer Network Defense (CND) capability to make useful.				

AU-14(1)	**SESSION AUDIT | *SYSTEM START-UP***				
	The information system initiates session audits at system start-up.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

AU-14(2)	**SESSION AUDIT | *CAPTURE / RECORD AND LOG CONTENT***				
	The information system provides the capability for authorized users to capture/record and log content related to a user session.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A

Difficulty w/Legacy	High
Comments/ Rationale	Refer to base control.

AU-14(3)	**SESSION AUDIT | *REMOTE VIEWING / LISTENING***				
	The information system provides the capability for authorized users to remotely view/hear all content related to an established user session in real time.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

AU-15	**ALTERNATE AUDIT CAPABILITY**				
	Control: The organization provides an alternate audit capability in the event of a failure in primary audit capability that provides [*Assignment: organization-defined alternate audit functionality*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Redundancy in audit; not likely critical enough to require this.				

AU-16	**CROSS-ORGANIZATIONAL AUDITING**				
	Control: The organization employs [*Assignment: organization-defined methods*] for coordinating [*Assignment: organization-defined audit information*] among external organizations when audit information is transmitted across organizational boundaries.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				

Comments/ Rationale	Unlikely tactical systems would benefit from cross-organization auditing.

AU-16(1)	**CROSS-ORGANIZATIONAL AUDITING | *IDENTITY PRESERVATION***				
	The organization requires that the identity of individuals be preserved in cross-organizational audit trails.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Refer to base control.				

AU-16(2)	**CROSS-ORGANIZATIONAL AUDITING | *SHARING OF AUDIT INFORMATION***				
	The organization provides cross-organizational audit information to [*Assignment: organization-defined organizations*] based on [*Assignment: organization-defined cross-organizational sharing agreements*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Refer to base control.				

SECURITY ASSESSMENT AND AUTHORIZATION

CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES				
	Control: The organization: a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and updates the current: 1. Security assessment and authorization policy [*Assignment: organization-defined frequency*]; and 2. Security assessment and authorization procedures [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	All -1 are Medium, covered by policy.				

CA-2	SECURITY ASSESSMENTS				
	Control: The organization: a. Develops a security assessment plan that describes the scope of the assessment including: 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to [*Assignment: organization-defined individuals or roles*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR RMF process fulfills the intent of this control.				

CA-2(1)	**SECURITY ASSESSMENTS | *INDEPENDENT ASSESSORS***				
	The organization employs assessors or assessment teams with [*Assignment: organization-defined level of independence*] to conduct security control assessments.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control. Specifically, Navy Validator and Functional Security Control Assessor (FSCA) Role for AIR 4.0. Some open discussion on 'independent' is needed.				

CA-2(2)	**SECURITY ASSESSMENTS | *SPECIALIZED ASSESSMENTS***				
	The organization includes as part of security control assessments, [*Assignment: organization-defined frequency*], [*Selection: announced; unannounced*], [*Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing;* [*Assignment: organization-defined other forms of security assessment*]].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control. Typically, inclusion of system vulnerability scan data from ACAS or physical audit, manual review, pen testing results, Cyber Risk Assessment (CRA) results and mitigations.				

CA-2(3)	**SECURITY ASSESSMENTS | *EXTERNAL ORGANIZATIONS***				
	The organization accepts the results of an assessment of [*Assignment: organization-defined information system*] performed by [*Assignment: organization-defined external organization*] when the assessment meets [*Assignment: organization-defined requirements*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	This is the NAVAIR RMF process for reciprocity.				

CA-3	SYSTEM INTERCONNECTIONS				
	Control: The organization: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Most NAVAIR weapon systems do not use Interconnection Service Agreements (ISA). More often used for enterprise to enterprise connections. Supported by NAVAIR RMF Process; typically, NAVAIR covers external connections under Service Provider agreements (e.g. SLA, MOA). Needs to be comprehensive of all connections not just IP based (e.g. tactical datalinks).				

CA-3(1)	SYSTEM INTERCONNECTIONS | *UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS*				
	The organization prohibits the direct connection of an [*Assignment: organization-defined unclassified, national security system*] to an external network without the use of [*Assignment: organization-defined boundary protection device*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

CA-3(2)	SYSTEM INTERCONNECTIONS | *CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS*				
	The organization prohibits the direct connection of a classified, national security system to an external network without the use of [*Assignment: organization-defined boundary protection device*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M

Difficulty w/Legacy	Low
Comments/ Rationale	Refer to base control. This should include tactical data links (non-IP) which gets more difficult to determine who is connected as it changes operationally.

CA-3(3)	**SYSTEM INTERCONNECTIONS | *UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS***				
	The organization prohibits the direct connection of an [*Assignment: organization-defined unclassified, non-national security system*] to an external network without the use of [*Assignment; organization-defined boundary protection device*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control. Limited rationale as to why weapon systems should be connecting to non-National Security Systems (NSS). This control can be difficult depending on individual components' designation as NSS.				

CA-3(4)	**SYSTEM INTERCONNECTIONS | *CONNECTIONS TO PUBLIC NETWORKS***				
	The organization prohibits the direct connection of an [*Assignment: organization-defined information system*] to a public network.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control. Limited rationale as to why weapon systems should be connecting to public networks.				

CA-3(5)	**SYSTEM INTERCONNECTIONS | *RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS***				
	The organization employs [*Selection: allow-all, deny-by-exception; deny-all, permit-by-exception*] policy for allowing [*Assignment: organization-defined information systems*] to connect to external information systems.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems

	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control. Permit by exception should be the default (e.g., whitelisting as a design trade-space to enhance above controls).				

CA-4 – Withdrawn

CA-5	**PLAN OF ACTION AND MILESTONES**				
	Control: The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Part of NAVAIR's RMF Process.				

CA-5(1)	**PLAN OF ACTION AND MILESTONES | *AUTOMATED SUPPORT FOR ACCURACY / CURRENCY***				
	The organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is accurate, up to date, and readily available.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control. Primarily covered by NAVAIR-mandated use of eMASS (limited automation).				

CA-6	**SECURITY AUTHORIZATION**
	Control: The organization: a. Assigns a senior-level executive or manager as the authorizing official for the information

	system; b. Ensures the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Part of NAVAIR's RMF Process (AIR-00 for weapon systems).				

CA-7	**CONTINUOUS MONITORING**				
	Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [*Assignment: organization-defined metrics*] to be monitored; b. Establishment of [*Assignment: organization-defined freq*uencies] for monitoring and [*Assignment: organization-defined freq*uencies] for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to [*Assignment: organization-defined personnel or roles*] [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Continuous monitoring should be one of the key improvements NAVAIR RMF brings to the table over DIACAP. The data and process for weapon systems likely differs greatly compared to enterprise. Needs to be documented in a tailored plan for each program.				

CA-7(1)	**CONTINUOUS MONITORING | *INDEPENDENT ASSESSMENT***				
	The organization employs assessors or assessment teams with [*Assignment: organization-defined level of independence*] to monitor the security controls in the information system on an ongoing basis.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C	Applicable Unmanned A/C	Applicable Support	Applicable Shipboard

		Vehicle	Control Station	Equipment	Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Functional Security Control Assessor (FSCA) fulfills function at NAVAIR.				

CA-7(2) – Withdrawn

CA-7(3)	**CONTINUOUS MONITORING | *TREND ANALYSES***				
	The organization employs trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Trend analysis requires a good understanding of baseline behavior. NAVAIR personnel often lack knowledge on what they should be looking for. Good concept, likely very difficult to implement. Also likely highly variable program to program based on available data and operational conditions.				

Penetration testing is a critical control that needs to be more broadly applied across NAVAIR systems. NAVAIR will interpret penetration testing in the following contexts.
- NAVAIR test Team Penetration testing fulfills the intent of CA-8
- External assessments not utilizing STRATCOM/NSA/SERVICE Red Team Authorities fulfill intent of CA-8(1)
- External assessments utilizing STRATCOM/NSA/SERVICE Red Team Authorities fulfill intent of CA-8(2)

CA-8	**PENETRATION TESTING**				
	Control: The organization conducts penetration testing [*Assignment: organization-defined frequency*] on [*Assignment: organization-defined information systems or system components*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	High value if done right, needs to go beyond IP scope, Cyber Warfare Detachment /5.0 focus area.				

CA-8(1)	PENETRATION TESTING | *INDEPENDENT PENETRATION AGENT OR TEAM*				
	The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	This control must be assessed in re scope and level of independence needed. Clearly National Cyber Range (NCR) and other national ranges, as well as Operational Technology (OT) cyber assessment, should meet the intent of this control.				

CA-8(2)	PENETRATION TESTING | *RED TEAM EXERCISES*				
	The organization employs [*Assignment: organization-defined red team exercises*] to simulate attempts by adversaries to compromise organizational information systems in accordance with [*Assignment: organization-defined rules of engagement*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Current Cyber Operational Technology tries to do this (caveat – limited capability). Very good concept if done correctly to model adversary threats.				

CA-9	INTERNAL SYSTEM CONNECTIONS				
	Control: The organization: a. Authorizes internal connections of [*Assignment: organization-defined information system components or classes of components*] to the information system; and b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/	Covered in numerous locations. NAVAIR Covered by Configuration Management (CM) policy				

Rationale	(NAVAIR Instruction 4130.1E) /design baseline (SETR) / CRA process / NAVAIR RMF documentation (programs documentation for RMF process would be the artifact for this control).

CA-9(1)	**INTERNAL SYSTEM CONNECTIONS | *SECURITY COMPLIANCE CHECKS***				
	The information system performs security compliance checks on constituent system components prior to the establishment of the internal connection.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Device Control Management is a very good feature. For enterprise systems, typically this is fulfilled by HBSS; HBSS' one-size fits all design has known limitations weapon system architectures. is a spectrum of compliance with this control, ranging from event-driven to persistent self-check of compliance. This control must be applied selectively to avoid excessive cost.				

CONFIGURATION MANAGEMENT

CM-1	CONFIGURATION MANAGEMENT POLICIES AND PROCEDURES				
	Control: The organization: a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and b. Reviews and updates the current: 1. Configuration management policy [*Assignment: organization-defined frequency*]; and 2. Configuration management procedures [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	All -1 are Medium, covered by policy.				

CM-2	BASELINE CONFIGURATION				
	Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by NAVAIR Configuration Management (CM) policy (NAVAIR Instruction 4130.1E) / PMA CM Plan, provided program adheres to policy.				

CM-2(1)	BASELINE CONFIGURATION | ***REVIEWS AND UPDATES***				
	The organization reviews and updates the baseline configuration of the information system: (a) [*Assignment: organization-defined frequency*]; (b) When required due to [*Assignment organization-defined circumstances*]; and (c) As an integral part of information system component installations and upgrades.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems

	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

CM-2(2)	**BASELINE CONFIGURATION | *AUTOMATION SUPPORT FOR ACCURACY / CURRENCY***				
	The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Bit checks may partially meet this. Technical, not a process control. Future platforms performing configuration checks would meet the intent of this control.				

CM-2(3)	**BASELINE CONFIGURATION | *RETENTION OF PREVIOUS CONFIGURATIONS***				
	The organization retains [*Assignment: organization-defined previous versions of baseline configurations of the information system*] to support rollback.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

CM-2(4) – Withdrawn

CM-2(5) – Withdrawn

CM-2(6)	**BASELINE CONFIGURATION | *DEVELOPMENT AND TEST ENVIRONMENTS***				
	The organization maintains a baseline configuration for information system development and test environments that is managed separately from the operational baseline configuration.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded

					Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	For NAVAIR systems, this is usually accomplished by Software in the loop (SIL), hardware in the loop (HIL) and software integration labs (government and contractor). Control appears duplicative with CM-4(1).				

CM-2(7)	**BASELINE CONFIGURATION | *CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS***				
	The organization: (a) Issues [*Assignment: organization-defined information systems, system components, or devices*] with [*Assignment: organization-defined configurations*] to individuals traveling to locations that the organization deems to be of significant risk; and (b) Applies [*Assignment: organization-defined security safeguards*] to the devices when the individuals return.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	L	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Weapon systems are in a high risk exposed environment.				

CM-3	**CONFIGURATION CHANGE CONTROL**				
	Control: The organization: a. Determines the types of changes to the information system that are configuration-controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the information system; e. Retains records of configuration-controlled changes to the information system for [*Assignment: organization-defined time period*]; f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board)*] that convenes [*Selection (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M

Difficulty w/Legacy	Low
Comments/ Rationale	Covered by NAVAIR CM policy (NAVAIR Instruction 4130.1E) / PMA CM Plan and operational procedures, provided program adheres to policy.

CM-3(1)	**CONFIGURATION CHANGE CONTROL | *AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES***				
	The organization employs automated mechanisms to: (a) Document proposed changes to the information system; (b) Notify [*Assignment: organized-defined approval authorities*] of proposed changes to the information system and request change approval; (c) Highlight proposed changes to the information system that have not been approved or disapproved by [*Assignment: organization-defined time period*]; (d) Prohibit changes to the information system until designated approvals are received; (e) Document all changes to the information system; and (f) Notify [*Assignment: organization-defined personnel*] when approved changes to the information system are completed.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by operational procedures. Note: control states "automated", NAVAIR uses manual processes for most systems.				

CM-3(2)	**CONFIGURATION CHANGE CONTROL | *TEST / VALIDATE / DOCUMENT CHANGES***				
	The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by standard NAVAIR development, Airworthiness, and SETR processes.				

CM-3(3)	**CONFIGURATION CHANGE CONTROL | *AUTOMATED CHANGE IMPLEMENTATION***				
	The organization employs automated mechanisms to implement changes to the current information system baseline and deploys the updated baseline across the installed base**.**				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	For connected non-weapon systems, this has some value; not applicable to weapon systems due to static configuration requirements.				

CM-3(4)	**CONFIGURATION CHANGE CONTROL | *SECURITY REPRESENTATIVE***				
	The organization requires an information security representative to be a member of the [*Assignment: organization-defined configuration change control element*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Cybersecurity representative in CM process, as directed (NAVAIRINST 4130.1E).				

CM-3(5)	**CONFIGURATION CHANGE CONTROL | *AUTOMATED SECURITY RESPONSE***				
	The information system implements [*Assignment: organization-defined security responses*] automatically if baseline configurations are changed in an unauthorized manner.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not applicable to most weapon systems, handled by flight clearance; could have significant operational impact and prevent battle short needs.				

CM-3(6)	**CONFIGURATION CHANGE CONTROL | *CRYPTOGRAPHY MANAGEMENT***				
	The organization ensures that cryptographic mechanisms used to provide [*Assignment: organization-defined security safeguards*] are under configuration management.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems

	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Management of Certificates and Stores.				

CM-4	**SECURITY IMPACT ANALYSIS**				
	Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by NAVAIR SETR / RMF / CM processes.				

CM-4(1)	**SECURITY IMPACT ANALYSIS | *SEPARATE TEST ENVIRONMENTS***				
	The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice**.**				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	For NAVAIR systems, this is usually accomplished by Software in the loop (SIL), hardware in the loop (HIL) and software integration labs (government and contractor).				

CM-4(2)	**SECURITY IMPACT ANALYSIS | *VERIFICATION OF SECURITY FUNCTIONS***				
	The organization, after the information system is changed, checks the security functions to verify the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M

Difficulty w/Legacy	Low
Comments/ Rationale	Covered by Step 4 of NAVAIR RMF process.

CM-5	**ACCESS RESTRICTIONS FOR CHANGE**				
	Control: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by NAVAIR CM policy (NAVAIR Instruction 4130.1E) and OPNAVINST 4790.2J Naval Aviation Maintenance Program (NAMP).				

CM-5(1)	**ACCESS RESTRICTIONS FOR CHANGE | *AUTOMATED ACCESS ENFORCEMENT / AUDITING***				
	The information system enforces access restrictions and supports auditing of the enforcement actions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

CM-5(2)	**ACCESS RESTRICTIONS FOR CHANGE | *REVIEW SYSTEM CHANGES***				
	The organization reviews information system changes [*Assignment: organization-defined frequency*] and [*Assignment: organization-defined circumstances*] to determine whether unauthorized changes have occurred.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				

Comments/ Rationale	This is a blue hunt activity.

CM-5(3)	**ACCESS RESTRICTIONS FOR CHANGE | *SIGNED COMPONENTS***				
	The information system prevents the installation of [*Assignment: organization-defined software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High – Most legacy systems do not have code signing verification capabilities. Compliance with this control would likely require reengineering.				
Comments/ Rationale	Code signing of software components is a critical safeguard that should be deployed in our systems, where feasible. Options on where in the supply chain to implement (end to end).				

CM-5(4)	**ACCESS RESTRICTIONS FOR CHANGE | *DUAL AUTHORIZATION***				
	The organization enforces dual authorization for implementing changes to [*Assignment: organization-defined information system components and system-level information*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Dual authorization not operationally feasible in most cases.				

CM-5(5)	**ACCESS RESTRICTIONS FOR CHANGE | *LIMIT PRODUCTION / OPERATIONAL PRIVILEGES***				
	The organization: (a) Limits privileges to change information system components and system-related information within a production or operational environment; and (b) Reviews and reevaluates privileges [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				

Comments/ Rationale	This is covered by other Least Privilege controls (not needed as a configuration management control).

CM-5(6)	**ACCESS RESTRICTIONS FOR CHANGE | *LIMIT LIBRARY PRIVILEGES***				
	The organization limits privileges to change software resident within software libraries.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	NAVAIR libraries are part of the baseline configuration management process (control is not needed).				

CM-5(7) – Withdrawn

CM-6	**CONFIGURATION SETTINGS**				
	Control: The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined operational requirements*]; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by NAVAIR CM policy (NAVAIR Instruction 4130.1E) / PMA CM Plan and Operational Procedures, providing the program adheres to the policy.				

CM-6(1)	**CONFIGURATION SETTINGS | *AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION***				
	The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [*Assignment: organization-defined information system components*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C	Applicable Unmanned A/C	Applicable Support	Applicable Shipboard

		Vehicle	Control Station	Equipment	Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Weapon systems cannot be centrally managed and automated due to deployment restrictions.				

CM-6(2)	**CONFIGURATION SETTINGS | *RESPOND TO UNAUTHORIZED CHANGES***				
	The organization employs [*Assignment: organization-defined security safeguards*] to respond to unauthorized changes to [*Assignment: organization-defined configuration settings*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Bit checks meet this, partially. Weapon systems should avoid automatically halting.				

CM-6(3) – Withdrawn

CM-6(4) – Withdrawn

CM-7	**LEAST FUNCTIONALITY**				
	Control: The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment*				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Good design principle. Remove unneeded capabilities (e.g. uninstall web server if not needed).				

CM-7(1)	**LEAST FUNCTIONALITY | *PERIODIC REVIEW***
	The organization:

	(a) Reviews the information system [*Assignment: organization-defined frequency*] to identify unnecessary and/or non-secure functions, ports, protocols, and services; and (b) Disables [*Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Good practice. Moderate because not all components are scan-able.				

CM-7(2)	**LEAST FUNCTIONALITY | *PREVENT PROGRAM EXECUTION***				
	The information system prevents program execution in accordance with [*Selection (one or more):* [*Assignment: organization-defined policies regarding software program usage and restrictions*]*; rules authorizing the terms and conditions of software program usage*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	This is the creation of rules for whitelisting. Packaged control with CM-7(5)				

CM-7(3)	**LEAST FUNCTIONALITY | *REGISTRATION COMPLIANCE***				
	The organization ensures compliance with [*Assignment: organization-defined registration requirements for functions, ports, protocols, and services*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	This is white list management; more important for large enterprise registration than weapon systems.				

CM-7(4)	**LEAST FUNCTIONALITY | *UNAUTHORIZED SOFTWARE / BLACKLISTING***

	The organization: (a) Identifies [*Assignment: organization-defined software programs not authorized to execute on the information system*]; (b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and (c) Reviews and updates the list of unauthorized software programs [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	This is application blacklisting, not typically feasible.				

CM-7(5)	**LEAST FUNCTIONALITY | *AUTHORIZED SOFTWARE / WHITELISTING***				
	The organization: (a) Identifies [*Assignment: organization-defined software programs authorized to execute on the information system*]; (b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and (c) Reviews and updates the list of authorized software programs [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High – Compliance with this control would likely require reengineering;				
Comments/ Rationale	Application whitelisting is a critical control NAVAIR should be using broadly.				

CM-8	**INFORMATION SYSTEM COMPONENT INVENTORY**				
	<u>Control</u>: The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]; and b. Reviews and updates the information system component inventory [*Assignment: organization-defined frequency*].				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by NAVAIR CM policy (NAVAIR Instruction 4130.1E), PMA CM Plan, Airworthiness, and/ OPNAVINST 4790 activities.				

CM-8(1)	**INFORMATION SYSTEM COMPONENT INVENTORY | *UPDATES DURING INSTALLATIONS / REMOVALS***				
	The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by Naval Aviation Logistics Command Management Information System (NALCOMIS).				

CM-8(2)	**INFORMATION SYSTEM COMPONENT INVENTORY | *AUTOMATED MAINTENANCE***				
	The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components**.**				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by NALCOMIS and Navy Messages.				

CM-8(3)	**INFORMATION SYSTEM COMPONENT INVENTORY | *AUTOMATED UNAUTHORIZED COMPONENT DETECTION***
	The organization: (a) Employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and (b) Takes the following actions when unauthorized components are detected: [*Selection (one or*

	more): disables network access by such components; isolates the components; notifies [*Assignment: organization-defined personnel or roles*]].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Typically solved by HBSS to detect USB installed. Often not feasible in weapon systems. Mitigated by OPSEC controls.				

CM-8(4)	**INFORMATION SYSTEM COMPONENT INVENTORY | *ACCOUNTABILITY INFORMATION***				
	The organization includes in the information system component inventory information, a means for identifying by [*Selection (one or more): name; position; role*], individuals responsible/accountable for administering those components.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by NALCOMIS.				

CM-8(5)	**INFORMATION SYSTEM COMPONENT INVENTORY | *NO DUPLICATE ACCOUNTING OF COMPONENTS***				
	The organization verifies all components within the authorization boundary of the information system are not duplicated in other information system component inventories.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by NALCOMIS.				

CM-8(6)	**INFORMATION SYSTEM COMPONENT INVENTORY | *ASSESSED CONFIGURATIONS / APPROVED DEVIATIONS***

	The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by NAVAIR CM policy (NAVAIR Instruction 4130.1E)/ OPNAVINST 4790 (and Flight Clearance, where applicable).				

CM-8(7)	**INFORMATION SYSTEM COMPONENT INVENTORY | *CENTRALIZED REPOSITORY***				
	The organization provides a centralized repository for the inventory of information system components.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by NALCOMIS.				

CM-8(8)	**INFORMATION SYSTEM COMPONENT INVENTORY | *AUTOMATED LOCATION TRACKING***				
	The organization employs automated mechanisms to support tracking of information system components by geographic location.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	OPSEC – automatic position reporting is not applicable to weapon systems.				

CM-8(9)	**INFORMATION SYSTEM COMPONENT INVENTORY | *ASSIGNMENT OF COMPONENTS TO SYSTEMS***
	The organization:

	(a) Assigns [*Assignment: organization-defined acquired information system components*] to an information system; and (b) Receives an acknowledgement from the information system owner of this assignment**.**				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by NALCOMIS.				

CM-9	**CONFIGURATION MANAGEMENT PLAN**				
	Control: The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the information system and places the configuration items under configuration management; and d. Protects the configuration management plan from unauthorized disclosure and modification.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by NAVAIR CM policy (NAVAIR Instruction 4130.1E)/ OPNAVINST 4790.				

CM-9(1)	**CONFIGURATION MANAGEMENT PLAN | *ASSIGNMENT OF RESPONSIBILITY***				
	The organization assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in information system development.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control				

CM-10	SOFTWARE USAGE RESTRICTIONS				
	Control: The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by DoD 5000 Acquisition Requirements and DFARS.				

CM-10(1)	SOFTWARE USAGE RESTRICTIONS | *OPEN SOURCE SOFTWARE*				
	The organization establishes the following restrictions on the use of open source software: [*Assignment: organization-defined restrictions*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control				

CM-11	USER-INSTALLED SOFTWARE				
	Control: The organization: a. Establishes [*Assignment: organization-defined policies*] governing the installation of software by users; b. Enforces software installation policies through [*Assignment: organization-defined methods*]; and c. Monitors policy compliance at [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M

Difficulty w/Legacy	Low
Comments/ Rationale	Covered by NAVAIR CM policy (NAVAIR Instruction 4130.1E) / OPNAVINST 4790.

CM-11(1)	**USER-INSTALLED SOFTWARE | *ALERTS FOR UNAUTHORIZED INSTALLATIONS***				
	The information system alerts [*Assignment: organization-defined personnel or roles*] when the unauthorized installation of software is detected.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Good practice, but difficult for dynamic checks in weapon systems.				

CM-11(2)	**USER-INSTALLED SOFTWARE | *PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS***				
	The information system prohibits user installation of software without explicit privileged status				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Good practice; must be balanced with operational needs. Should be part of the least privilege structure.				

CONTINGENCY PLANNING

CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES				
	Control: The organization: a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and b. Reviews and updates the current: 1. Contingency planning policy [*Assignment: organization-defined frequency*]; and 2. Contingency planning procedures [*Assignment: organization-defined frequency*				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	All -1 are Medium, covered by policy.				

CP-2	CONTINGENCY PLAN				
	Control: The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*]; b. Distributes copies of the contingency plan to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*]; e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*]; and g. Protects the contingency plan from unauthorized disclosure and modification.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems

	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Operational requirements dictate contingency planning beyond information system components**.**				

CP-2(1)	**CONTINGENCY PLAN | *COORDINATE WITH RELATED PLANS***				
	The organization coordinates contingency plan development with organizational elements responsible for related plans.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Primarily refers to coordinating with the operational plans for the system.				

CP-2(2)	**CONTINGENCY PLAN | *CAPACITY PLANNING***				
	The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Primarily refers to coordinating with the operational plans for the system. Operational requirements will dictate capacity planning, not cybersecurity requirements for NAVAIR weapon systems.				

CP-2(3)	**CONTINGENCY PLAN | *RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS***				
	The organization plans for the resumption of essential missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				

Comments/ Rationale	Should be covered by other operational plans.

CP-2(4)	**CONTINGENCY PLAN | *RESUME ALL MISSIONS / BUSINESS FUNCTIONS***				
	The organization plans for the resumption of all missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Should be covered by other operational plans.				

CP-2(5)	**CONTINGENCY PLAN | *CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS***				
	The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Should be covered by other operational plans.				

CP-2(6)	**CONTINGENCY PLAN | *ALTERNATE PROCESSING / STORAGE SITE***				
	The organization plans for the transfer of essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through information system restoration to primary processing and/or storage sites.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	High				
Comments/	Not operationally relevant.				

Rationale	

CP-2(7)	**CONTINGENCY PLAN | *COORDINATE WITH EXTERNAL SERVICE PROVIDERS***				
	The organization coordinates its contingency plan with the contingency plans of external service providers to ensure contingency requirements can be satisfied**.**				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Should be covered by other operational plans. Commercial SATCOM is most likely interface for weapon systems.				

CP-2(8)	**CONTINGENCY PLAN | *IDENTIFY CRITICAL ASSETS***				
	The organization identifies critical information system assets supporting essential missions and business functions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Should be covered by other operational plans.				

CP-3	**CONTINGENCY TRAINING**				
	Control: The organization provides contingency training to information system users consistent with assigned roles and responsibilities: a. Within [*Assignment: organization-defined time period*] of assuming a contingency role or responsibility; b. When required by information system changes; and c. [*Assignment: organization-defined frequency*] thereafter.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				

Comments/ Rationale	Contingency training is conducted according to operational plans. More emphasis should be placed on the cyber resiliency aspects of those training exercises.

CP-3(1)	**CONTINGENCY TRAINING | *SIMULATED EVENTS***				
	The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Cyber resiliency contingency training is typically accomplished through simulated events.				

CP-3(2)	**CONTINGENCY TRAINING | *AUTOMATED TRAINING ENVIRONMENTS***				
	The organization employs automated mechanisms to provide a more thorough and realistic contingency training environment.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Legacy tactical weapon systems often do not have automated training environments, especially within the context of cyber resiliency operations.				

CP-4	**CONTINGENCY PLAN TESTING**				
	Control: The organization: a. Tests the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests*] to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the contingency plan test results; and c. Initiates corrective actions, if needed.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				

Comments/ Rationale	Contingency test plan should exist as part of broader operational contingency planning.

CP-4(1)	**CONTINGENCY PLAN TESTING | *COORDINATE WITH RELATED PLANS***				
	The organization coordinates contingency plan testing with organizational elements responsible for related plans				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Should be part of other operational plans.				

CP-4(2)	**CONTINGENCY PLAN TESTING | *ALTERNATE PROCESSING SITE***				
	The organization tests the contingency plan at the alternate processing site: (a) To familiarize contingency personnel with the facility and available resources; and (b) To evaluate the capabilities of the alternate processing site to support contingency operations.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Only valid for alternate UAS Control Segments.				

CP-4(3)	**CONTINGENCY PLAN TESTING | *AUTOMATED TESTING***				
	The organization employs automated mechanisms to provide a more thorough and realistic contingency training environment.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not valid for weapon systems.				

CP-4(4)	CONTINGENCY PLAN TESTING | *FULL RECOVERY / RECONSTITUTION*				
	The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Critical to be able to restore NAVAIR tactical systems to a known good state. See CP-10.				

CP-5 – Withdrawn

CP-6	ALTERNATE STORAGE SITE				
	Control: The organization: a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures the alternate storage site provides information security safeguards equivalent to that of the primary site.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not applicable to tactical systems.				

CP-6(1)	ALTERNATE STORAGE SITE | *SEPARATION FROM PRIMARY SITE*				
	The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/	Refer to base control.				

Rationale	

CP-6(2)	**ALTERNATE STORAGE SITE | *RECOVERY TIME / POINT OBJECTIVES***				
	The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

CP-6(3)	**ALTERNATE STORAGE SITE | *ACCESSIBILITY***				
	The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

CP-7	**ALTERNATE PROCESSING SITE**				
	Control: The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [*Assignment: organization-defined information system operations*] for essential missions/business functions within [*Assignment: organization-defined time period consistent with recovery time and recovery point objectives*] when the primary processing capabilities are unavailable; b. Ensures equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and c. Ensures the alternate processing site provides information security safeguards equivalent to those of the primary site.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems

	N/A	N/A	L	N/A	N/A
Difficulty w/Legacy	High				
Comments/ Rationale	Only valid for alternate UAS Control Segments.				

CP-7(1)	**ALTERNATE PROCESSING SITE | *SEPARATION FROM PRIMARY SITE***				
	The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	N/A	N/A
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

CP-7(2)	**ALTERNATE PROCESSING SITE | *ACCESSIBILITY***				
	The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	N/A	N/A
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

CP-7(3)	**ALTERNATE PROCESSING SITE | *PRIORITY OF SERVICE***				
	The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	N/A	N/A
Difficulty	High				

w/Legacy	
Comments/ Rationale	Refer to base control.

CP-7(4)	**ALTERNATE PROCESSING SITE | *PREPARATION FOR USE***				
	The organization prepares the alternate processing site so the site is ready to be used as the operational site supporting essential missions and business functions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	N/A	N/A
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

CP-7(5) – Withdrawn

CP-7(6)	**ALTERNATE PROCESSING SITE | *INABILITY TO RETURN TO PRIMARY SITE***				
	The organization plans and prepares for circumstances that preclude returning to the primary processing site.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	N/A	N/A
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

CP-8	**TELECOMMUNICATIONS SERVICES**				
	Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [*Assignment: organization-defined information system operations*] for essential missions and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	N/A	N/A

Difficulty w/Legacy	Low
Comments/ Rationale	Inherited from DISA/SPAWAR.

CP-8(1)	**TELECOMMUNICATIONS SERVICES | *PRIORITY OF SERVICE PROVISIONS***				
	The organization: **(a)** Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and **(b)** Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event the primary and/or alternate telecommunications services are provided by a common carrier.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	N/A	N/A
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

CP-8(2)	**TELECOMMUNICATIONS SERVICES | *SINGLE POINTS OF FAILURE***				
	The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	N/A	N/A
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

CP-8(3)	**TELECOMMUNICATIONS SERVICES | *SEPARATION OF PRIMARY / ALTERNATE PROVIDERS***				
	The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems

	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not valid for weapon systems.				

CP-8(4)	**TELECOMMUNICATIONS SERVICES | *PROVIDER CONTINGENCY PLAN***				
	The organization: (a) Requires primary and alternate telecommunications service providers to have contingency plans; (b) Reviews provider contingency plans to ensure the plans meet organizational contingency requirements; and (c) Obtains evidence of contingency testing/training by providers [*Assignment: organization-defined frequency]*.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	N/A	N/A
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

CP-8(5)	**TELECOMMUNICATIONS SERVICES | *ALTERNATE TELECOMMUNICATION SERVICE TESTING***				
	The organization tests alternate telecommunication services [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not valid for weapon systems.				

CP-9	**INFORMATION SYSTEM BACKUP**
	Control: The organization: a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; c. Conducts backups of information system documentation including security-related

	documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and d. Protects the confidentiality, integrity, and availability of backup information at storage locations.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	This control is typically not applicable to weapons systems due to standard practice of reconstituting or reimaging the system.				

CP-9(1)	**INFORMATION SYSTEM BACKUP | *TESTING FOR RELIABILITY / INTEGRITY***				
	The organization tests backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Refer to base control.				

CP-9(2)	**INFORMATION SYSTEM BACKUP | *TEST RESTORATION USING SAMPLING***				
	The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Refer to base control.				

CP-9(3)	**INFORMATION SYSTEM BACKUP | *SEPARATE STORAGE FOR CRITICAL INFORMATION***
	The organization stores backup copies of [*Assignment: organization-defined critical information*

	system software and other security-related information] in a separate facility or in a fire-rated container that is not collocated with the operational system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not valid for weapon systems.				

CP-9(4) – Withdrawn

CP-9(5)	**INFORMATION SYSTEM BACKUP | *TRANSFER TO ALTERNATE STORAGE SITE***				
	The organization transfers information system backup information to the alternate storage site [*Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not valid for weapon systems.				

CP-9(6)	**INFORMATION SYSTEM BACKUP | *REDUNDANT SECONDARY SYSTEM***				
	The organization accomplishes information system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	N/A	N/A
Difficulty w/Legacy	High				
Comments/ Rationale	Only valid for alternate UAS Control Segments.				

CP-9(7)	INFORMATION SYSTEM BACKUP | *DUAL AUTHORIZATION*				
	The organization enforces dual authorization for the deletion or destruction of [*Assignment: organization-defined backup information*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not valid for weapon systems.				

CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION				
	Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Critical to be able to restore NAVAIR tactical systems to a known good state. See CP-4(4)				

CP-10(1) – Withdrawn

CP-10(2)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | *TRANSACTION RECOVERY*				
	The information system implements transaction recovery for systems that are transaction-based.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Tactical systems are not transactional.				

CP-10(3) – Withdrawn

CP-10(4)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | *RESTORE WITHIN TIME PERIOD*				
	The organization provides the capability to restore information system components within [*Assignment: organization-defined restoration time-periods*] from configuration-controlled and integrity-protected information representing a known, operational state for the components.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

CP-10(5) – Withdrawn

CP-10(6)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | *COMPONENT PROTECTION*				
	The organization protects backup and restoration hardware, firmware, and software.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Protecting the known good state.				

CP-11	ALTERNATE COMMUNICATIONS PROTOCOLS				
	Control: The information system provides the capability to employ [*Assignment: organization-defined alternative communications protocols*] in support of maintaining continuity of operations.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	This should not be done on weapon systems.				

CP-12	SAFE MODE				
	Control: The information system, when [*Assignment: organization-defined conditions*] are detected, enters a safe mode of operation with [*Assignment: organization-defined restrictions of safe mode of operation*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	L	H
Difficulty w/Legacy	High				
Comments/ Rationale	For tactical weapon systems, the concept of 'safe mode' must be broader than standard IT systems. Large trade space with this control in re how to maneuver the system during a cyber-attack (e.g., Battle Short Switch capability).				

CP-13	ALTERNATIVE SECURITY MECHANISMS				
	Control: The organization employs [*Assignment: organization-defined alternative or supplemental security mechanisms*] for satisfying [*Assignment: organization-defined security functions*] when the primary means of implementing the security function is unavailable or compromised.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	This control, as written, is of limited value ("catch all"). Can only see this as being a compensating control mechanism.				

IDENTIFICATION AND AUTHENTICATION

IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES				
	Control: The organization: a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and b. Reviews and updates the current: 1. Identification and authentication policy [*Assignment: organization-defined frequency*]; and 2. Identification and authentication procedures [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** All -1 are Medium, covered by policy.				

IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)				
	Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Many tactical systems identify and authenticate to the role, not the individual. Many safety critical systems (e.g., flight deck) have no identity or authentication mechanism beyond physical presence at the controls.				

Care must be taken in defining network versus local access scope in context for proximity/attack surface for a particular system. Some weapons systems have internal architectures that appear to be local access, when a network access is being established internal to the weapon system. In such cases where network access is not accessible outside the weapon system, it may be appropriate to treat as local access.

IA-2(1)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ***NETWORK ACCESS TO PRIVILEGED ACCOUNTS***

	The information system implements multifactor authentication for network access to privileged accounts.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control. Multifactor authentication can be achieved through mechanisms other than PKI.				

IA-2(2)	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | *NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS***				
	The information system implements multifactor authentication for network access to non-privileged accounts.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to IA-2(1).				

IA-2(3)	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | *LOCAL ACCESS TO PRIVILEGED ACCOUNTS***				
	The information system implements multifactor authentication for local access to privileged accounts.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to IA-2(1).				

IA-2(4)	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | *LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS***
	The information system implements multifactor authentication for local access to non-privileged

	accounts.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to IA-2(1).				

IA-2(5)	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | *GROUP AUTHENTICATION***				
	The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Having an additional individual login after a group account login does not make sense for weapon systems.				

IA-2(6)	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | *NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE***				
	The information system implements multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*Assignment: organization-defined strength of mechanism requirements*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	May be cases in which RSA tokens are useful, but generally not useful to enforce this multifactor on weapon systems.				

IA-2(7)	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | *NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - SEPARATE DEVICE***
	The information system implements multifactor authentication for network access to non-privileged

	accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*Assignment: organization-defined strength of mechanism requirements*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	May be cases in which RSA tokens are useful, but generally not useful to enforce this multifactor on weapon systems.				

IA-2(8)	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | *NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT***				
	The information system implements replay-resistant authentication mechanisms for network access to privileged accounts**.**				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Only a concern when network access is part of the exposed attack surface of the weapon system.				

IA-2(9)	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | *NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT***				
	The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to IA-2(8).				

IA-2(10)	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | *SINGLE SIGN-ON***
	The information system provides a single sign-on capability for [*Assignment: organization-defined*

	information system accounts and services].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	NAVAIR weapon system design implicitly creates single sign-on.				

IA-2(11)	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | *REMOTE ACCESS - SEPARATE DEVICE***				
	The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*Assignment: organization-defined strength of mechanism requirements*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Remote access to NAVAIR weapon systems is not a common feature. (Overarching remote access controls are of higher importance).				

IA-2(12)	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | *ACCEPTANCE OF PIV CREDENTIALS***				
	The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control. Multifactor authentication can be achieved through mechanisms other than PKI.				

IA-2(13)	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | *OUT-OF-BAND AUTHENTICATION***

	The information system implements [*Assignment: organization-defined out-of-band authentication*] under [*Assignment: organization-defined conditions*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Out of band login requirement not operationally valid in most situations.				

IA-3	**DEVICE IDENTIFICATION AND AUTHENTICATION**				
	Control: The information system uniquely identifies and authenticates [*Assignment: organization-defined specific and/or types of devices*] before establishing a [*Selection (one or more): local; remote; network*] connection.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	H	H	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Device to device authentication – not found in most weapon systems. Trust is by physical connection. This control may be more important in context of UAS.				

IA-3(1)	**DEVICE IDENTIFICATION AND AUTHENTICATION | *CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION***				
	The information system authenticates [*Assignment: organization-defined specific devices and/or types of devices*] before establishing [*Selection (one or more): local; remote; network*] connection using bidirectional authentication that is cryptographically based.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	H	H	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

IA-3(2) – Withdrawn

IA-3(3)	DEVICE IDENTIFICATION AND AUTHENTICATION | *DYNAMIC ADDRESS ALLOCATION*				
	The organization: (a) Standardizes dynamic address allocation lease information and the lease duration assigned to devices in accordance with [*Assignment: organization-defined lease information and lease duration*]; and (b) Audits lease information when assigned to a device.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	NAVAIR does not want to use Dynamic Host Configuration Protocol (DHCP) inside weapon systems.				

IA-3(4)	DEVICE IDENTIFICATION AND AUTHENTICATION | *DEVICE ATTESTATION*				
	The organization ensures that device identification and authentication based on attestation is handled by [*Assignment: organization-defined configuration management process*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Device attestation can be a very powerful cyber resiliency capability, but also expensive.				

IA-4	IDENTIFIER MANAGEMENT				
	Control: The organization manages information system identifiers by: a. Receiving authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. Preventing reuse of identifiers for [*Assignment: organization-defined time period*]; and e. Disabling the identifier after [*Assignment: organization-defined time period of inactivity*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M

Difficulty w/Legacy	Moderate
Comments/ Rationale	Typically usernames and static IP addresses for weapon systems.

IA-4(1)	**IDENTIFIER MANAGEMENT | *PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS***				
	The organization prohibits the use of information system account identifiers that are the same as public identifiers for individual electronic mail accounts.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Good practice.				

IA-4(2)	**IDENTIFIER MANAGEMENT | *SUPERVISOR AUTHORIZATION***				
	The organization requires that the registration process to receive an individual identifier includes supervisor authorization.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Typically covered by operational procedures and roles/responsibilities where individual accounts are created in the field. Not applicable for legacy platforms with static accounts.				

IA-4(3)	**IDENTIFIER MANAGEMENT | *MULTIPLE FORMS OF CERTIFICATION***				
	The organization requires multiple forms of certification of individual identification be presented to the registration authority.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				

Comments/ Rationale	OPSEC addresses.

IA-4(4)	**IDENTIFIER MANAGEMENT | *IDENTIFY USER STATUS***				
	The organization manages individual identifiers by uniquely identifying each individual as [*Assignment: organization-defined characteristic identifying individual status*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Makes sense for email systems; not useful in tactical systems.				

IA-4(5)	**IDENTIFIER MANAGEMENT | *DYNAMIC MANAGEMENT***				
	The information system dynamically manages identifiers.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not valid for weapon systems.				

IA-4(6)	**IDENTIFIER MANAGEMENT | *CROSS-ORGANIZATION MANAGEMENT***				
	The organization coordinates with [*Assignment: organization-defined external organizations*] for cross-organization management of identifiers.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not valid for weapon systems.				

IA-4(7)	IDENTIFIER MANAGEMENT | *IN-PERSON REGISTRATION*				
	The organization requires that the registration process to receive an individual identifier be conducted in person before a designated registration authority.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by operational procedures.				

IA-5	AUTHENTICATOR MANAGEMENT				
	Control: The organization manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*]; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Password management in most NAVAIR systems. Subsystem accounts likely PMA managed. Crew accounts typically managed operationally (split requirement).				

IA-5(1)	AUTHENTICATOR MANAGEMENT | *PASSWORD-BASED AUTHENTICATION*
	The information system, for password-based authentication: (a) Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*]; (b) Enforces at least the following number of changed characters when new passwords are created:

	[*Assignment: organization-defined number*]; (c) Stores and transmits only cryptographically-protected passwords; (d) Enforces password minimum and maximum lifetime restrictions of [*Assignment: organization-defined numbers for lifetime minimum, lifetime maximum*]; (e) Prohibits password reuse for [*Assignment: organization-defined number*] generations; and (f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Important given the high use of passwords in weapon systems. Care must be taken to balance complexity requirements with operational needs.				

IA-5(2)	**AUTHENTICATOR MANAGEMENT | *PKI-BASED AUTHENTICATION***				
	The information system, for PKI-based authentication: (a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; (b) Enforces authorized access to the corresponding private key; (c) Maps the authenticated identity to the account of the individual or group; and (d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control. Multifactor authentication can be achieved through mechanisms other than PKI.				

IA-5(3)	**AUTHENTICATOR MANAGEMENT | *IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION***				
	The organization requires that the registration process to receive [*Assignment: organization-defined types of and/or specific authenticators*] be conducted [*Selection: in person; by a trusted third party*] before [*Assignment: organization-defined registration authority*] with authorization by *[Assignment: organization-defined personnel or roles*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems

	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** Weapon systems do not use third parties for account registration.				

IA-5(4)	**AUTHENTICATOR MANAGEMENT | *AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION***				
	The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [*Assignment: organization-defined requirements*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	PMA typically addresses for static accounts or base operating system (OS) group policy settings**.**				

IA-5(5)	**AUTHENTICATOR MANAGEMENT | *CHANGE AUTHENTICATORS PRIOR TO DELIVERY***				
	The organization requires developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	In weapon systems this is a critical control. Changing all default passwords and development/test passwords prior to sending to Fleet.				

IA-5(6)	**AUTHENTICATOR MANAGEMENT | *PROTECTION OF AUTHENTICATORS***				
	The organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H

Difficulty w/Legacy	Low
Comments/ Rationale	Required by policy; classified at level of systems access.

IA-5(7)	**AUTHENTICATOR MANAGEMENT | *NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS***				
	The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Critical there are no unprotected hardcoded User Name/Passwords (UN/PW).				

IA-5(8)	**AUTHENTICATOR MANAGEMENT | *MULTIPLE INFORMATION SYSTEM ACCOUNTS***				
	The organization implements [*Assignment: organization-defined security safeguards*] to manage the risk of compromise due to individuals having accounts on multiple information systems.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Uncommon implementation for NAVAIR weapon systems (requires individual logins, multiple assets).				

IA-5(9)	**AUTHENTICATOR MANAGEMENT | *CROSS-ORGANIZATION CREDENTIAL MANAGEMENT***				
	The organization coordinates with [*Assignment: organization-defined external organizations*] for cross-organization management of credentials.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty	N/A				

w/Legacy	
Comments/ Rationale	Weapon systems do not have these types of cross organizational relationships.

IA-5(10)	**AUTHENTICATOR MANAGEMENT | *DYNAMIC CREDENTIAL ASSOCIATION***				
	The information system dynamically provisions identities				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not done in weapon systems.				

IA-5(11)	**AUTHENTICATOR MANAGEMENT | *HARDWARE TOKEN-BASED AUTHENTICATION***				
	The information system, for hardware token-based authentication, employs mechanisms that satisfy [*Assignment: organization-defined token quality requirements*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Refer to base control. Multifactor authentication can be achieved through mechanisms other than PKI.				

IA-5(12)	**AUTHENTICATOR MANAGEMENT | *BIOMETRIC-BASED AUTHENTICATION***				
	The information system, for biometric-based authentication, employs mechanisms that satisfy [*Assignment: organization-defined biometric quality requirements*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control. Multifactor authentication can be achieved through mechanisms other than PKI.				

IA-5(13)	AUTHENTICATOR MANAGEMENT | *EXPIRATION OF CACHED AUTHENTICATORS*				
	The information system prohibits the use of cached authenticators after [*Assignment: organization-defined time period*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Good practice.				

IA-5(14)	AUTHENTICATOR MANAGEMENT | *MANAGING CONTENT OF PKI TRUST STORES*				
	The organization, for PKI-based authentication, employs a deliberate organization-wide methodology for managing the content of PKI trust stores installed across all platforms including networks, operating systems, browsers, and applications.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** Refer to base control. Multifactor authentication can be achieved through mechanisms other than PKI.				

IA-5(15)	AUTHENTICATOR MANAGEMENT | *FICAM-APPROVED PRODUCTS AND SERVICES*				
	The organization uses only FICAM-approved path discovery and validation products and services.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	DoD does not use Federated Identity, Credential, and Access Management (FICAM). Superseded by NSS policy.				

IA-6	AUTHENTICATOR FEEDBACK
	Control: The information system obscures feedback of authentication information during the

	authentication process to protect the information from possible exploitation/use by unauthorized individuals.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Good practice. (e.g., asterisk over password).				

IA-7	**CRYPTOGRAPHIC MODULE AUTHENTICATION**				
	Control: The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Required for all NSA-approved crypto solutions.				

Non-organizational users: many controls exist that involve non-organizational users (e.g., service technicians, cooperating companies, support contractors, et al). These controls are logical in a business context, but inappropriate for embedded weapon systems. Weapon system crew should all be considered organizational users, including maintenance activities.

IA-8	**IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)**				
	Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Weapon systems do not have non-organizational users.				

IA-8(1)	**IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)| *ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES***				
	The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

IA-8(2)	**IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)| *ACCEPTANCE OF THIRD-PARTY CREDENTIALS***				
	The information system accepts only FICAM-approved third-party credentials.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

IA-8(3)	**IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)| *USE OF FICAM-APPROVED PRODUCTS***				
	The organization employs only FICAM-approved information system components in [*Assignment: organization-defined information systems*] to accept third-party credentials.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

IA-8(4)	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)| *USE OF FICAM-ISSUED PROFILES*				
	The information system conforms to FICAM-issued profiles.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

IA-8(5)	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)| *ACCEPTANCE OF PIV-I CREDENTIALS*				
	The information system accepts and electronically verifies Personal Identity Verification-I (PIV-I) credentials.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

IA-9	SERVICE IDENTIFICATION AND AUTHENTICATION				
	Control: The organization identifies and authenticates [*Assignment: organization-defined information system services*] using [*Assignment: organization-defined security safeguards*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	N/A	N/A
Difficulty w/Legacy	High				
Comments/ Rationale	Not applicable to most legacy systems. May be applicable for newer systems with high levels of interoperability.				

IA-9(1)	SERVICE IDENTIFICATION AND AUTHENTICATION | *INFORMATION EXCHANGE*
	The organization ensures service providers receive, validate, and transmit identification and

	authentication information.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	N/A	N/A
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

IA-9(2)	**SERVICE IDENTIFICATION AND AUTHENTICATION | *TRANSMISSION OF DECISIONS***				
	The organization ensures identification and authentication decisions are transmitted between [*Assignment: organization-defined services*] consistent with organizational policies.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	N/A	N/A
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

IA-10	**ADAPTIVE IDENTIFICATION AND AUTHENTICATION**				
	Control: The organization requires that individuals accessing the information system employ [*Assignment: organization-defined supplemental authentication techniques or mechanisms*] under specific [*Assignment: organization-defined circumstances or situations*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR does not permit adaptive authentication in its embedded weapon systems.				

IA-11	**RE-AUTHENTICATION**				
	Control: The organization requires users and devices to re-authenticate when [*Assignment: organization-defined circumstances or situations requiring re-authentication*].				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	M	M	M	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Useful in Multi-Level Security (MLS) situations; care must be taken to not create operational issue with fixed time/periodic reauthorization requests				

INCIDENT RESPONSE

IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES				
	Control: The organization: a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy [*Assignment: organization-defined frequency*]; and 2. Incident response procedures [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** All -1 are Medium, covered by policy.				

IR-2	INCIDENT RESPONSE TRAINING				
	Control: The organization provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within [*Assignment: organization-defined time period*] of assuming an incident response role or responsibility; b. When required by information system changes; and c. [*Assignment: organization-defined frequency*] thereafter.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR Cyber Incident Response Team (CIRT) training and certification curriculum covers the intent of this control.				

IR-2(1)	INCIDENT RESPONSE TRAINING | *SIMULATED EVENTS*				
	The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded

					Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Threat simulation sessions are key techniques for NAVAIR CIRT.				

IR-2(2)	**INCIDENT RESPONSE TRAINING | *AUTOMATED TRAINING ENVIRONMENTS***				
	The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Simulated event training may include automated training environments that could support this control.				

IR-3	**INCIDENT RESPONSE TESTING**				
	Control: The organization tests the incident response capability for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests*] to determine the incident response effectiveness and documents the results.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR Cyber Incident Response Team (CIRT) covers this control.				

IR-3(1)	**INCIDENT RESPONSE TESTING | *AUTOMATED TESTING***				
	The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L

Difficulty w/Legacy	Moderate
Comments/ Rationale	Automation unlikely in NAVAIR CIRT testing.

IR-3(2)	**INCIDENT RESPONSE TESTING | *COORDINATION WITH RELATED PLANS***				
	The organization coordinates incident response testing with organizational elements responsible for related plans.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR CIRT will coordinate with other plans as Standard Operating Procedure.				

IR-4	**INCIDENT HANDLING**				
	Control: The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR Cyber Incident Response Team (CIRT) capability. Difficulty rated high due to deploying to ships and other operational locations.				

IR-4(1)	**INCIDENT HANDLING | *AUTOMATED INCIDENT HANDLING PROCESSES***				
	The organization employs automated mechanisms to support the incident handling process.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L

Difficulty w/Legacy	High
Comments/ Rationale	Due to the uniqueness of systems and lack of constant connectivity, automated processes are not as effective for weapon system activities, as they are for enterprise systems. NAVAIR CIRT team engagement with NCDOC may support this.

IR-4(2)	**INCIDENT HANDLING | *DYNAMIC RECONFIGURATION***				
	The organization includes dynamic reconfiguration of [Assignment: organization-defined information system components] as part of the incident response capability.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Dynamic reconfiguration not advised in weapon systems.				

IR-4(3)	**INCIDENT HANDLING | *CONTINUITY OF OPERATIONS***				
	The organization identifies [*Assignment: organization-defined classes of incidents*] and [*Assignment: organization-defined actions to take in response to classes of incidents*] to ensure continuation of organizational missions and business functions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** Defined in Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B – automatically compliant.				

IR-4(4)	**INCIDENT HANDLING | *INFORMATION CORRELATION***				
	The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M

Difficulty w/Legacy	Low
Comments/ Rationale	NAVAIR CIRT capability.

IR-4(5)	**INCIDENT HANDLING | *AUTOMATIC DISABLING OF INFORMATION SYSTEM***				
	The organization implements a configurable capability to automatically disable the information system if [*Assignment: organization-defined security violations*] are detected.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Automated disabling is prohibited in weapon systems.				

IR-4(6)	**INCIDENT HANDLING | *INSIDER THREATS - SPECIFIC CAPABILITIES***				
	The organization implements incident handling capability for insider threats.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR CIRT capability.				

IR-4(7)	**INCIDENT HANDLING | *INSIDER THREATS - INTRA-ORGANIZATION COORDINATION***				
	The organization coordinates incident handling capability for insider threats across [*Assignment: organization-defined components or elements of the organization*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR CIRT capability.				

IR-4(8)	INCIDENT HANDLING | *CORRELATION WITH EXTERNAL ORGANIZATIONS*				
	The organization coordinates with [*Assignment: organization-defined external organizations*] to correlate and share [*Assignment: organization-defined incident information*] to achieve a cross-organization perspective on incident awareness and more effective incident responses.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR CIRT capability.				

IR-4(9)	INCIDENT HANDLING | *DYNAMIC RESPONSE CAPABILITY*				
	The organization employs [*Assignment: organization-defined dynamic response capabilities*] to effectively respond to security incidents.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR CIRT capability.				

IR-4(10)	INCIDENT HANDLING | *SUPPLY CHAIN COORDINATION*				
	The organization coordinates incident handling activities involving supply chain events with other organizations involved in the supply chain.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR CIRT will consider supply chain.				

IR-5	INCIDENT MONITORING

	Control: The organization tracks and documents information system security incidents				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR CIRT capability.				

IR-5(1)	**INCIDENT MONITORING | *AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS***				
	The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	NAVAIR CIRT coordinates with U.S. Fleet Cyber Command, NCDOC, and other cyber incident response entities.				

IR-6	**INCIDENT REPORTING**				
	Control: The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [*Assignment: organization-defined time period*]; and b. Reports security incident information to [*Assignment: organization-defined authorities*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	DoD has defined CJCSM 6410.01B timelines. NAVAIR CIRT addresses; may need to indicate additional reporting requirements and associated timelines.				

IR-6(1)	**INCIDENT REPORTING | *AUTOMATED REPORTING***				
	The organization employs automated mechanisms to assist in the reporting of security incidents.				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	NAVAIR expects most incident-reporting to be manual.				

IR-6(2)	**INCIDENT REPORTING | *VULNERABILITIES RELATED TO INCIDENTS***				
	The organization reports information system vulnerabilities associated with reported security incidents to [*Assignment: organization-defined personnel or roles*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Important, will be covered by NAVAIR CIRT CONOPS / Standard Operating Procedures. Dissemination likely limited due to classification and need-to-know.				

IR-6(3)	**INCIDENT REPORTING | *COORDINATION WITH SUPPLY CHAIN***				
	The organization provides security incident information to other organizations involved in the supply chain for information systems or information system components related to the incident.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR CIRT coordinates with Naval Criminal Investigative Service (NCIS) and DoD Cyber Crime Center (DC3) for Supply Chain compromise reporting.				

IR-7	**INCIDENT RESPONSE ASSISTANCE**				
	Control: The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded

					Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR CIRT provides this capability/service.				

IR-7(1)	**INCIDENT RESPONSE ASSISTANCE | *AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT***				
	The organization employs automated mechanisms to increase the availability of incident response-related information and support.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	NAVAIR CIRT coordinates with U.S. Fleet Cyber Command, NCDOC, and other cyber incident response entities.				

IR-7(2)	**INCIDENT RESPONSE ASSISTANCE | *COORDINATION WITH EXTERNAL PROVIDERS***				
	The organization: (a) Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and (b) Identifies organizational incident response team members to the external providers.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to IR-7(1)				

IR-8	**INCIDENT RESPONSE PLAN**
	Control: The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization;

	4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*]; b. Distributes copies of the incident response plan to [*Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements*]; c. Reviews the incident response plan [*Assignment: organization-defined frequency*]; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to [*Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements*]; and f. Protects the incident response plan from unauthorized disclosure and modification.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Key to have a plan. NAVAIR programs are supported by NAVAIR CIRT capability, but CIRT capability does not directly meet this control.				

IR-9	**INFORMATION SPILLAGE RESPONSE**
	Control: The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination; b. Alerting [*Assignment: organization-defined personnel or roles*] of the information spill using a method of communication not associated with the spill; c. Isolating the contaminated information system or system component; d. Eradicating the information from the contaminated information system or component; e. Identifying other information systems or system components that may have been subsequently contaminated; and f. Performing other [*Assignment: organization-defined actions*].

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	AIR-7.4 (Security and Continuity of Operations Planning) responsibility; existing policies and operational procedures in place.				

IR-9(1)	**INFORMATION SPILLAGE RESPONSE | *RESPONSIBLE PERSONNEL***
	The organization assigns [*Assignment: organization-defined personnel or roles*] with responsibility

	for responding to information spills.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

IR-9(2)	**INFORMATION SPILLAGE RESPONSE | *TRAINING***				
	The organization provides information spillage response training [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

IR-9(3)	**INFORMATION SPILLAGE RESPONSE | *POST-SPILL OPERATIONS***				
	The organization implements [*Assignment: organization-defined procedures*] to ensure organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

IR-9(4)	**INFORMATION SPILLAGE RESPONSE | *EXPOSURE TO UNAUTHORIZED PERSONNEL***				
	The organization employs [*Assignment: organization-defined security safeguards*] for personnel exposed to information not within assigned access authorizations.				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

IR-10	**INTEGRATED INFORMATION SECURITY ANALYSIS TEAM**				
	Control: The organization establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR CIRT integrates network and computer forensics activities. Augmented by other agency support, as required.				

MAINTENANCE

MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES				
	Control: The organization: a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and b. Reviews and updates the current: 1. System maintenance policy [*Assignment: organization-defined frequency*]; and 2. System maintenance procedures [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	All -1 are Medium, covered by policy.				

MA-2	CONTROLLED MAINTENANCE				
	Control: The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that [*Assignment: organization-defined personnel or roles*] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes [*Assignment: organization-defined maintenance-related information*] in organizational maintenance records.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by OPNAVINST 4790 activities.				

MA-2(1) – Withdrawn

MA-2(2)	**CONTROLLED MAINTENANCE | *AUTOMATED MAINTENANCE ACTIVITIES***				
	The organization: (a) Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and (b) Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Weapon systems rarely have the fully automated maintenance activities seen in enterprise environments, but many semi-automated mechanisms exist. Program offices utilize many of the semi-automated mechanisms (e.g., Navy messages) as part of existing OPNAVINST 4790 processes that should meet the intent of this control.				

MA-3	**MAINTENANCE TOOLS**				
	Control: The organization approves, controls, and monitors information system maintenance tools.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by OPNAVINST 4790 processes and activities.				

MA-3(1)	**MAINTENANCE TOOLS | *INSPECT TOOLS***				
	The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M

Difficulty w/Legacy	Low
Comments/ Rationale	Refer to base control.

MA-3(2)	**MAINTENANCE TOOLS | *INSPECT MEDIA***				
	The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

MA-3(3)	**M MAINTENANCE TOOLS | *PREVENT UNAUTHORIZED REMOVAL***				
	The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: (a) Verifying there is no organizational information contained on the equipment; (b) Sanitizing or destroying the equipment; (c) Retaining the equipment within the facility; or (d) Obtaining an exemption from [*Assignment: organization-defined personnel or roles*] explicitly authorizing removal of the equipment from the facility.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

MA-3(4)	**MAINTENANCE TOOLS | *RESTRICTED TOOL USE***				
	The information system restricts the use of maintenance tools to authorized personnel only.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M

Difficulty w/Legacy	Low
Comments/ Rationale	Refer to base control.

MA-4	**NONLOCAL MAINTENANCE**				
	Control: The organization: a. Approves and monitors nonlocal maintenance and diagnostic activities; b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; d. Maintains records for nonlocal maintenance and diagnostic activities; and e. Terminates session and network connections when nonlocal maintenance is completed.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not a maintenance approach for weapon systems (e.g., Original Equipment Manufacturer (OEM) remotes into a piece of equipment to repair). If remote administration is being used, these values become 'M'; not recommended in weapon systems.				

MA-4(1)	**NONLOCAL MAINTENANCE | *AUDITING AND REVIEW***				
	The organization: (a) Audits nonlocal maintenance and diagnostic sessions [*Assignment: organization-defined audit events*]; and (b) Reviews the records of the maintenance and diagnostic sessions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

MA-4(2)	**NONLOCAL MAINTENANCE | *DOCUMENT NONLOCAL MAINTENANCE***				
	The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

MA-4(3)	**NONLOCAL MAINTENANCE | *COMPARABLE SECURITY / SANITIZATION***				
	The organization: (a) Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or (b) Removes the component to be serviced from the information system prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

MA-4(4)	**NONLOCAL MAINTENANCE | *AUTHENTICATION / SEPARATION OF MAINTENANCE SESSIONS***				
	The organization protects nonlocal maintenance sessions by: (a) Employing [*Assignment: organization-defined authenticators that are replay resistant*]; and (b) Separating the maintenance sessions from other network sessions with the information system by either: **(1)** Physically separated communications paths; or **(2)** Logically separated communications paths based upon encryption.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/	Refer to base control.				

Rationale	

MA-4(5)	**NONLOCAL MAINTENANCE | *APPROVALS AND NOTIFICATIONS***				
	The organization: (a) Requires the approval of each nonlocal maintenance session by [*Assignment: organization-defined personnel or roles*]; and (b) Notifies [*Assignment: organization-defined personnel or roles*] of the date and time of planned nonlocal maintenance.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

MA-4(6)	**NONLOCAL MAINTENANCE | *CRYPTOGRAPHIC PROTECTION***				
	The information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

MA-4(7)	**NONLOCAL MAINTENANCE | *REMOTE DISCONNECT VERIFICATION***				
	The information system implements remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/	Refer to base control.				

Rationale	

MA-5	**MAINTENANCE PERSONNEL**				
	Control: The organization: a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; b. Ensures non-escorted personnel performing maintenance on the information system have required access authorizations; and c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by OPNAV 4790 and operational OPSEC activities.				

MA-5(1)	**MAINTENANCE PERSONNEL | *INDIVIDUALS WITHOUT APPROPRIATE ACCESS***				
	The organization: **(a)** Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: **(1)** Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; **(2)** Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and **(b)** Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

MA-5(2)	**MAINTENANCE PERSONNEL | *SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS***

	The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for all compartments of information on the system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

MA-5(3)	**MAINTENANCE PERSONNEL | *CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS***				
	The organization ensures that personnel performing maintenance and diagnostic activities on information system processing, storing, or transmitting classified information are U.S. citizens.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

MA-5(4)	**MAINTENANCE PERSONNEL | *FOREIGN NATIONALS***				
	The organization ensures that: (a) Cleared foreign nationals (i.e., foreign nationals with appropriate security clearances), are used to conduct maintenance and diagnostic activities on classified information systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and (b) Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified information systems are fully documented within Memoranda of Agreements.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				

Comments/ Rationale	Refer to base control.

MA-5(5)	**MAINTENANCE PERSONNEL | *NONSYSTEM-RELATED MAINTENANCE***				
	The organization ensures that non-escorted personnel performing maintenance activities not directly associated with the information system but in the physical proximity of the system, have required access authorizations.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

MA-6	**TIMELY MAINTENANCE**				
	Control: The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined information system components*] within [*Assignment: organization-defined time period*] of failure.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Timely maintenance is good practice; needs to be coordinated with Configuration Management (CM) policy (NAVAIR Instruction 4130.1E) and flight clearance.				

MA-6(1)	**TIMELY MAINTENANCE | *PREVENTIVE MAINTENANCE***				
	The organization performs preventive maintenance on [*Assignment: organization-defined information system components*] at [*Assignment: organization-defined time intervals*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/	Refer to base control.				

Rationale	

MA-6(2)	**TIMELY MAINTENANCE | *PREDICTIVE MAINTENANCE***				
	The organization performs predictive maintenance on [*Assignment: organization-defined information system components] at [Assignment: organization-defined time intervals*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Refer to base control. .				

MA-6(3)	**TIMELY MAINTENANCE | *AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE***				
	The organization employs automated mechanisms to transfer predictive maintenance data to a computerized maintenance management system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Refer to base control.				

MEDIA PROTECTION

MP-1	MEDIA PROTECTION POLICY AND PROCEDURES				
	Control: The organization: a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and b. Reviews and updates the current: 1. Media protection policy [*Assignment: organization-defined frequency*]; and 2. Media protection procedures [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** All -1 are Medium, covered by policy.				

MP-2	MEDIA ACCESS				
	Control: The organization restricts access to [*Assignment: organization-defined types of digital and/or non-digital media*] to [*Assignment: organization-defined personnel or roles*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by DoD policy regarding the handling of CLASS & controlled UNCLASS information.				

MP-2(1) – Withdrawn

MP-2(2) – Withdrawn

MP-3	MEDIA MARKING
	Control: The organization: a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts [*Assignment: organization-defined types of information system media*] from marking as

	long as the media remain within [*Assignment: organization-defined controlled areas*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by DoD policy regarding the handling of CLASS & controlled UNCLASS information.				

MP-4	**MEDIA STORAGE**				
	Control: The organization: a. Physically controls and securely stores [*Assignment: organization-defined types of digital and/or non-digital media*] within [*Assignment: organization-defined controlled areas*]; and b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by DoD policy regarding the handling of CLASS & controlled UNCLASS information.				

MP-4(1) – Withdrawn

MP-4(2)	**MEDIA STORAGE | *AUTOMATED RESTRICTED ACCESS***				
	The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

MP-5	MEDIA TRANSPORT				
	Control: The organization: a. Protects and controls [*Assignment: organization-defined types of information system media*] during transport outside of controlled areas using [*Assignment: organization-defined security safeguards*]; b. Maintains accountability for information system media during transport outside of controlled areas; c. Documents activities associated with the transport of information system media; and d. Restricts the activities associated with the transport of information system media to authorized personnel.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by DoD policy regarding the handling of CLASS & controlled UNCLASS information.				

MP-5(1) – Withdrawn

MP-5(2) – Withdrawn

MP-5(3)	MEDIA TRANSPORT | *CUSTODIANS*				
	The organization employs an identified custodian during transport of information system media outside of controlled areas.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

MP-5(4)	MEDIA TRANSPORT | *CRYPTOGRAPHIC PROTECTION*				
	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems

	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Data at Rest (DAR) encryption on media during transport (good practice).				

MP-6	**MEDIA SANITIZATION**				
	Control: The organization: a. Sanitizes [*Assignment: organization-defined information system media*] prior to disposal, release out of organizational control, or release for reuse using [*Assignment: organization-defined sanitization techniques and procedures*] in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by DoD policy regarding the handling of CLASS & controlled UNCLASS information. Supported by operational procedures.				

MP-6(1)	**MEDIA SANITIZATION | *REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY***				
	The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

MP-6(2)	**MEDIA SANITIZATION | *EQUIPMENT TESTING***				
	The organization tests sanitization equipment and procedures [*Assignment: organization-defined frequency]* to verify that the intended sanitization is being achieved.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded

					Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

MP-6(3)	**MEDIA SANITIZATION | *NONDESTRUCTIVE TECHNIQUES***				
	The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [*Assignment: organization-defined circumstances requiring sanitization of portable storage devices*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Good practice to sanitize media coming from COTS source prior to first use.				

MP-6(4) – Withdrawn

MP-6(5) – Withdrawn

MP-6(6) – Withdrawn

MP-6(7)	**MEDIA SANITIZATION | *DUAL AUTHORIZATION***				
	The organization enforces dual authorization for the sanitization of [*Assignment: organization-defined information system media*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

MP-6(8)	**MEDIA SANITIZATION | *REMOTE PURGING / WIPING OF INFORMATION***

	The organization provides the capability to purge/wipe information from [*Assignment: organization-defined information systems, system components, or devices*] either remotely or under the following conditions: [*Assignment: organization-defined conditions*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not applicable to weapon systems, with the exception of mobile device components.				

MP-7	**MEDIA USE**				
	Control: The organization [*Selection: restricts; prohibits*] the use of [*Assignment: organization-defined types of information system media*] on [*Assignment: organization-defined information systems or system components*] using [*Assignment: organization-defined security safeguards*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by DoD policy regarding the handling of CLASS & controlled UNCLASS information. Supported by operational procedures.				

MP-7(1)	**MEDIA USE | *PROHIBIT USE WITHOUT OWNER***				
	The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

MP-7(2)	**MEDIA USE | *PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA***
	The organization prohibits the use of sanitization-resistant media in organizational information

	systems.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

MP-8	**MEDIA DOWNGRADING**				
	Control: The organization: a. Establishes [*Assignment: organization-defined information system media downgrading process*] that includes employing downgrading mechanisms with [*Assignment: organization-defined strength and integrity*]; b. Ensures the information system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information; c. Identifies [*Assignment: organization-defined information system media requiring downgrading*]; and d. Downgrades the identified information system media using the established process.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by DoD policy regarding the handling of CLASS & controlled UNCLASS information. Supported by operational procedures.				

MP-8(1)	**MEDIA DOWNGRADING | *DOCUMENTATION OF PROCESS***				
	The organization documents information system media downgrading actions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

MP-8(2)	**MEDIA DOWNGRADING | *EQUIPMENT TESTING***				
	The organization employs [*Assignment: organization-defined tests*] of downgrading equipment and procedures to verify correct performance [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

MP-8(3)	**MEDIA DOWNGRADING | *CONTROLLED UNCLASSIFIED INFORMATION***				
	The organization downgrades information system media containing [*Assignment: organization-defined Controlled Unclassified Information (CUI)*] prior to public release in accordance with applicable federal and organizational standards and policies.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

MP-8(4)	**MEDIA DOWNGRADING | *CLASSIFIED INFORMATION***				
	The organization downgrades information system media containing classified information prior to release to individuals without required access authorizations in accordance with NSA standards and policies.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

PHYSICAL AND ENVIRONMENTAL PROTECTION

PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES				
	Control: The organization: a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and b. Reviews and updates the current: 1. Physical and environmental protection policy [*Assignment: organization-defined frequency*]; and 2. Physical and environmental protection procedures [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** All -1 are Medium, covered by policy.				

PE-2	PHYSICAL ACCESS AUTHORIZATION				
	Control: The organization: a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; b. Issues authorization credentials for facility access; c. Reviews the access list detailing authorized facility access by individuals [*Assignment: organization-defined frequency*]; and d. Removes individuals from the facility access list when access is no longer required.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	General Access Control Procedures. Typically fulfilled by squadron Standard Operating Procedure (SOP) or ship personnel SOP. Commander, Naval Air Forces (COMNAVFOR) Antiterrorism Inst. (SECNAVINST 3300.3 series | OPNAVINST 5530.14 series). Future NAVAIR Instruction should cover Developmental Testing and depot aircraft. Operational Testing and Trainer (training wings) aircraft may be orphaned from policy.				

PE-2(1)	PHYSICAL ACCESS AUTHORIZATION | *ACCESS BY POSITION / ROLE*				
	The organization authorizes physical access to the facility where the information system resides based on position or role.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Enforcement of the general access control procedures. Squadron or ship forces SOPs meet the intent of this control.				

PE-2(2)	PHYSICAL ACCESS AUTHORIZATION | *TWO FORMS OF IDENTIFICATION*				
	The organization requires two forms of identification from [*Assignment: organization-defined list of acceptable forms of identification*] for visitor access to the facility where the information system resides.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to PE-2(1). Typically only applied on strategic/high sensitivity platforms, and often via secondary badges.				

PE-2(3)	PHYSICAL ACCESS AUTHORIZATION | *RESTRICT UNESCORTED ACCESS*				
	The organization restricts unescorted access to the facility where the information system resides to personnel with [*Selection (one or more): security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system;* [*Assignment: organization-defined credentials*]].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to PE-2(1). SOPs meet the intent of this control. NTTP for restricted area access (OPNAV 5530.14).				

PE-3	PHYSICAL ACCESS CONTROL				
	Control: The organization: a. Enforces physical access authorizations at [*Assignment: organization-defined entry/exit points to the facility where the information system resides*] by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using [*Selection (one or more):* [*Assignment: organization-defined physical access control systems/devices*]; *guards*]; b. Maintains physical access audit logs for [*Assignment: organization-defined entry/exit points*]; c. Provides [*Assignment: organization-defined security safeguards*] to control access to areas within the facility officially designated as publicly accessible; d. Escorts visitors and monitors visitor activity [*Assignment: organization-defined circumstances requiring visitor escorts and monitoring*]; e. Secures keys, combinations, and other physical access devices; f. Inventories [*Assignment: organization-defined physical access devices*] every [*Assignment: organization-defined frequency*]; and g. Changes combinations and keys [*Assignment: organization-defined frequency*] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Enforcement of the general access control procedures. Squadron or ship forces SOPs meet the intent of this control. See CNAF Instruction. Paired with PE-2.				

PE-3(1)	PHYSICAL ACCESS CONTROL | *INFORMATION SYSTEM ACCESS*				
	The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at [*Assignment: organization-defined physical spaces containing one or more components of the information system*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	N/A	L
Difficulty w/Legacy	High				
Comments/ Rationale	For most weapon systems, there is no separation of the information systems components and the weapon system. NAVAIR controls access to the weapon system; not appropriate to separately control access to the information system components onboard aircraft. Flight line or UAS control segments should be considered a separate Restricted Area. In physical security terms, refers to enclaving.				

PE-3(2)	PHYSICAL ACCESS CONTROL | *FACILITY / INFORMATION SYSTEM BOUNDARIES*
	The organization performs security checks [*Assignment: organization-defined frequency*] at the

	physical boundary of the facility or information system for unauthorized exfiltration of information or removal of information system components.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Restricted area policy meets the intent of this control. Enforcement may vary, but intent should be met.				

PE-3(3)	**PHYSICAL ACCESS CONTROL | *CONTINUOUS GUARDS / ALARMS / MONITORING***				
	The organization employs guards and/or alarms to monitor every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Restricted area policy meets the intent of this control. Enforcement may vary, but intent should be met.				

PE-3(4)	**PHYSICAL ACCESS CONTROL | *LOCKABLE CASINGS***				
	The organization uses lockable physical casings to protect [*Assignment: organization-defined information system components*] from unauthorized physical access.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	N/A	L
Difficulty w/Legacy	High				
Comments/ Rationale	Typically not applicable to weapon systems, operational/maintenance constraints. Mitigated by boundary controls per restricted area requirements.				

PE-3(5)	**PHYSICAL ACCESS CONTROL | *TAMPER PROTECTION***
	The organization employs [*Assignment: organization-defined security safeguards*] to [*Selection (one or more): detect; prevent*] physical tampering or alteration of [*Assignment: organization-defined hardware components*] within the information system.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	U.S. Navy has an Anti-Tamper Program. May be acceptable mitigations (e.g. USB Locker, tamper-evident tape). Can be a useful tool; should not be required.				

PE-3(6)	**PHYSICAL ACCESS CONTROL | *FACILITY PENETRATION TESTING***				
	The organization employs a penetration testing process that includes [*Assignment: organization-defined frequency*], unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Refers to testing the access controls at a flight line or on-board ship, not the traditional IT pen testing contexts. Unlikely to be required by assessment and authorization (A&A) process. Operational sensitivities would likely drive. Platform could take credit if applicable.				

PE-4	**ACCESS CONTROL FOR TRANSMISSION MEDIUM**				
	Control: The organization controls physical access to [*Assignment: organization-defined information system distribution and transmission lines*] within organizational facilities using [*Assignment: organization-defined security safeguards*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	N/A	L
Difficulty w/Legacy	High				
Comments/ Rationale	Typically this is conduit Protected Distribution System (PDS) requirements. Not applicable inside weapon systems. Possibly required in shipboard installs.				

PE-5	**ACCESS CONTROL FOR OUTPUT DEVICES**
	Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Overly IT centric. Output devices for weapon systems are inherently part of the weapon system. Aviation Data Management and Control System (ADMACS) might need to consider this as dictated by CNSSI 1253.				

PE-5(1)	**ACCESS CONTROL FOR OUTPUT DEVICES | *ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS***				
	The organization: (a) Controls physical access to output from [*Assignment: organization-defined output devices*]; and (b) Ensures only authorized individuals receive output from the device				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

PE-5(2)	**ACCESS CONTROL FOR OUTPUT DEVICES | *ACCESS TO OUTPUT BY INDIVIDUAL IDENTITY***				
	The information system: (a) Controls physical access to output from [*Assignment: organization-defined output devices*]; and (b) Links individual identity to receipt of the output from the device.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

PE-5(3)	**ACCESS CONTROL FOR OUTPUT DEVICES | *MARKING OUTPUT DEVICES***
	The organization marks [*Assignment: organization-defined information system output devices*]

	indicating the appropriate security marking of the information permitted to be output from the device.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

PE-6	**MONITORING PHYSICAL ACCESS**				
	Control: The organization: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs [*Assignment: organization-defined frequency*] and upon occurrence of [*Assignment: organization-defined events or potential indications of events*]; and c. Coordinates results of reviews and investigations with the organizational incident response capability.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Enforcement of the General Access Control Procedures. Fulfilled by squadron or ship forces SOPs. See CNAF Instruction. Paired with PE-2.				

PE-6(1)	**MONITORING PHYSICAL ACCESS | *INTRUSION ALARMS / SURVEILLANCE EQUIPMENT***				
	The organization monitors physical intrusion alarms and surveillance equipment**.**				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Fulfilled by the host facility (e.g. flight line, hangar). Restricted area requirements.				

PE-6(2)	**MONITORING PHYSICAL ACCESS | *AUTOMATED INTRUSION RECOGNITION /***

	RESPONSES				
	The organization employs automated mechanisms to recognize [*Assignment: organization-defined classes/types of intrusions*] and initiate [*Assignment: organization-defined response actions*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to PE-6(1).				

PE-6(3)	**MONITORING PHYSICAL ACCESS | *VIDEO SURVEILLANCE***				
	The organization employs video surveillance of [*Assignment: organization-defined operational areas*] and retains video recordings for [*Assignment: organization-defined time period*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to PE-6(1).				

PE-6(4)	**MONITORING PHYSICAL ACCESS | *MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS***				
	The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as [*Assignment: organization-defined physical spaces containing one or more components of the information system*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	N/A	L
Difficulty w/Legacy	High				
Comments/ Rationale	Not applicable to most systems. Refer to PE-3(1) NAVAIR does not have separation of Information System from weapon systems.				

PE-7 – Withdrawn

PE-7(1) – Withdrawn

PE-7(2) – Withdrawn

PE-8	**VISITOR ACCESS RECORDS**				
	Control: The organization: a. Maintains visitor access records to the facility where the information system resides for [*Assignment: organization-defined time period*]; and b. Reviews visitor access records [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Fulfilled by the host facility (e.g. flight line, hangar). Restricted area requirements.				

PE-8(1)	**VISITOR ACCESS RECORDS | *AUTOMATED RECORDS MAINTENANCE / REVIEW***				
	The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control. Should not be mandated by assessment and authorization (A&A) process beyond existing procedures.				

PE-8(2) – Withdrawn

PE-9	**POWER EQUIPMENT AND CABLING**				
	Control: The organization protects power equipment and power cabling for the information system from damage and destruction.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems

	N/A	N/A	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Not applicable to aircraft; there are some corner cases in which this could be inherited from host facility for shipboard or ashore equipment.				

PE-9(1)	**POWER EQUIPMENT AND CABLING | *REDUNDANT CABLING***				
	The organization employs redundant power cabling paths that are physically separated by [*Assignment: organization-defined distance*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Refer to base control.				

PE-9(2)	**POWER EQUIPMENT AND CABLING | *AUTOMATIC VOLTAGE CONTROLS***				
	The organization employs automatic voltage controls for [*Assignment: organization-defined critical information system components*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Refer to base control.				

PE-10	**EMERGENCY SHUTOFF**				
	Control: The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems

	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	This control does not provide additional cyber resiliency. Weapon systems will often meet control by design typically driven by safety requirements. Should not be driven to add e-stop type functionality for cybersecurity.				

PE-10(1) – Withdrawn

PE-11	**EMERGENCY POWER**				
	Control: The organization provides a short-term uninterruptible power supply to facilitate [*Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power*] in the event of a primary power source loss.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	As written, only applicable to ship- or shore-based equipment; possibly some support equipment.				

PE-11(1)	**EMERGENCY POWER | *LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY***				
	The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Refer to base control.				

PE-11(2)	**EMERGENCY POWER | *LONG-TERM ALTERNATE POWER SUPPLY - SELF-CONTAINED***
	The organization provides a long-term alternate power supply for the information system that is: (a) Self-contained; (b) Not reliant on external power generation; and

	(c) Capable of maintaining [*Selection: minimally required operational capability; full operational capability*] in the event of an extended loss of the primary power source				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Refer to base control.				

PE-12	**EMERGENCY LIGHTING**				
	Control: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and covers emergency exits and evacuation routes within the facility.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Fulfilled by the host facility per NFPA 101 (Life Safety Code®) requirements.				

PE-12(1)	**EMERGENCY LIGHTING | *ESSENTIAL MISSIONS / BUSINESS FUNCTIONS***				
	The organization provides emergency lighting for all areas within the facility supporting essential missions and business functions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

PE-13	**FIRE PROTECTION**
	Control: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Fire bad. Met by safety requirements in host facilities and airworthiness requirements in aircraft.				

PE-13(1)	**FIRE PROTECTION | *DETECTION DEVICES / SYSTEMS***				
	The organization employs fire detection devices/systems for the information system that activate automatically and notify [*Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined emergency responders*] in the event of a fire.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

PE-13(2)	**FIRE PROTECTION | *SUPPRESSION DEVICES / SYSTEMS***				
	The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to *Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined* emergency responders].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

PE-13(3)	**FIRE PROTECTION | *AUTOMATIC FIRE SUPPRESSION***				
	The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

PE-13(4)	**FIRE PROTECTION | *INSPECTIONS***				
	The organization ensures the facility undergoes [*Assignment: organization-defined frequency*] inspections by authorized and qualified inspectors and resolves identified deficiencies within [*Assignment: organization-defined time period*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

PE-14	**TEMPERATURE AND HUMIDITY CONTROLS**				
	Control: The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [*Assignment: organization-defined acceptable levels*]; and b. Monitors temperature and humidity levels [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Met by safety requirements in host facilities and airworthiness requirements in aircraft.				

PE-14(1)	**TEMPERATURE AND HUMIDITY CONTROLS | *AUTOMATIC CONTROLS***				
	The organization employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the information system.				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

PE-14(2)	**TEMPERATURE AND HUMIDITY CONTROLS | *MONITORING WITH ALARMS / NOTIFICATIONS***				
	The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

PE-15	**WATER DAMAGE PROTECTION**				
	Control: The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves are accessible, working properly, and known to key personnel.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Host facility fulfills this control.				

PE-15(1)	**WATER DAMAGE PROTECTION | *AUTOMATION SUPPORT***				
	The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts [*Assignment: organization-defined personnel or roles*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C	Applicable Unmanned A/C	Applicable Support	Applicable Shipboard

		Vehicle	Control Station	Equipment	Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

PE-16	**DELIVERY AND REMOVAL**				
	Control: The organization authorizes, monitors, and controls [*Assignment: organization-defined types of information system components*] entering and exiting the facility and maintains records of those items.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by policy and operational procedures.				

PE-17	**ALTERNATE WORK SITE**				
	Control: The organization: a. Employs [*Assignment: organization-defined security controls*] at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	N/A	N/A
Difficulty w/Legacy	High				
Comments/ Rationale	Not applicable to most weapon systems. May have applicability in terms of continuity of operations for UAS Control Station.				

PE-18	**LOCATION OF INFORMATION SYSTEM COMPONENTS**				
	Control: The organization positions information system components within the facility to minimize potential damage from [*Assignment: organization-defined physical and environmental hazards*] and to minimize the opportunity for unauthorized access.				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	L	L	L	N/A	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Not driven by cybersecurity requirements. Electromagnetic Pulse (EMP) requirements could meet intent as could aircraft survivability based separation of critical components.				

PE-18(1)	**LOCATION OF INFORMATION SYSTEM COMPONENTS | *FACILITY SITE***				
	The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	N/A	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Host facility fulfills this control.				

PE-19	**INFORMATION LEAKAGE**				
	Control: The organization protects the information system from information leakage due to electromagnetic signals emanations.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	N/A	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	TEMPEST meets the intent of this control; cybersecurity should not drive.				

PE-19(1)	**INFORMATION LEAKAGE | *NATIONAL EMISSIONS / TEMPEST POLICIES AND PROCEDURES***				
	The organization ensures information system components, associated data communications, and networks are protected in accordance with national emissions and TEMPEST policies and procedures based on the security category or classification of the information.				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	L	L	L	N/A	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Refer to base control.				

PE-20	**ASSET MONITORING AND TRACKING**				
	Control: The organization: a. Employs [*Assignment: organization-defined asset location technologies*] to track and monitor the location and movement of [*Assignment: organization-defined assets*] within [*Assignment: organization-defined controlled areas*]; and b. Ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Operational procedures (see configuration management controls) meet the intent of this control. This may be directed to DIPR-DON registration; not appropriate for weapon systems.				

PLANNING

PL-1	SECURITY PLANNING POLICY AND PROCEDURES				
	Control: The organization: a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: 1. Security planning policy [*Assignment: organization-defined frequency*]; and 2. Security planning procedures [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** All -1 are Medium, covered by policy.				

PL-2	SYSTEM SECURITY PLAN				
	Control: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distributes copies of the security plan and communicates subsequent changes to the plan to [*Assignment: organization-defined personnel or roles*]; c. Reviews the security plan for the information system [*Assignment: organization-defined frequency*]; d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protects the security plan from unauthorized disclosure and modification.				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR RMF requirement fulfills the intent of this control.				

PL-2(1) – Withdrawn

PL-2(2) – Withdrawn

PL-2(3)	**SYSTEM SECURITY PLAN | *PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES***				
	The organization plans and coordinates security-related activities affecting the information system with [*Assignment: organization-defined individuals or groups*] before conducting such activities in order to reduce the impact on other organizational entities.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

PL-3 – Withdrawn

PL-4	**RULES OF BEHAVIOR**				
	Control: The organization: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; b. Receives a signed acknowledgment from such individuals, indicating they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; c. Reviews and updates the rules of behavior [*Assignment: organization-defined frequency*]; and d. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems

	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Acceptable Use policy (SECNAV INSTRUCTION 5239.3C). Should be tied with operator training. Good spot to catch poor cyber hygiene issues.				

PL-4(1)	**RULES OF BEHAVIOR | *SOCIAL MEDIA AND NETWORKING RESTRICTIONS***				
	The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	The vast majority of weapon systems do not have outbound internet connections to reach social media so would be not applicable in those cases. Systems with that capability need to address social media in Acceptable Use Policy. Can also be blacklisted if forbidden (different control).				

PL-5 – Withdrawn

PL-6 – Withdrawn

PL-7	**SECURITY CONCEPT OF OPERATIONS**				
	Control: The organization: a. Develops a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security; and b. Reviews and updates the CONOPS [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Not in CNSSI 1253 profiles, typically required by NAO. Valid good practice; may be beneficial to have a template.				

PL-8	**INFORMATION SECURITY ARCHITECTURE**

	Control: The organization: a. Develops an information security architecture for the information system that: 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and 3. Describes any information security assumptions about, and dependencies on, external services; b. Reviews and updates the information security architecture [*Assignment: organization-defined frequency*] to reflect updates in the enterprise architecture; and c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR RMF best practice.				

PL-8(1)	**INFORMATION SECURITY ARCHITECTURE | *DEFENSE-IN-DEPTH***				
	The organization designs its security architecture using a defense-in-depth approach that: (a) Allocates [Assignment: organization-defined security safeguards] to [Assignment: organization-defined locations and architectural layers]; and (b) Ensures the allocated security safeguards operate in a coordinated and mutually reinforcing manner.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low (document existing) High (modify configuration to add depth)				
Comments/ Rationale	Defense-in-Depth Functional Implementation Architecture (DFIA) standard should be basis for new start programs. Legacy systems should document current defense in depth design.				

PL-8(2)	**INFORMATION SECURITY ARCHITECTURE | *SUPPLIER DIVERSITY***				
	The organization requires that [*Assignment: organization-defined security safeguards*] allocated to [*Assignment: organization-defined locations and architectural layers*] are obtained from different suppliers.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded

					Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	The concept of heterogeneity has some validity, but very difficult and expensive to implement (e.g., supportability and logistics challenges). Forces additional Sys Admin skills (different company) for consistent operation. Can lead to poorly configured systems. Should be mapped to SC-29.				

PL-9	**CENTRAL MANAGEMENT**				
	Control: The organization centrally manages [*Assignment: organization-defined security controls and related processes*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** Part of DoD RMF (Tier 1 Control).				

PROGRAM MANAGEMENT

PM-1	INFORMATION SECURITY PROGRAM PLAN				
	Control: The organization: a. Develops and disseminates an organization-wide information security program plan that: 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization-wide information security program plan [*Assignment: organization-defined frequency*]; c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and d. Protects the information security program plan from unauthorized disclosure and modification.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** All -1 are Medium, covered by policy.				

PM-2	SENIOR INFORMATION SECURITY OFFICER				
	Control: The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Command IO fulfills.				

PM-3	INFORMATION SECURITY RESOURCEES

	Control: The organization: a. Ensures all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and c. Ensures information security resources are available for expenditure as planned.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Likely fulfilled by Clinger-Cohen Act, DoD 5000 series acquisition, and FISMA.				

PM-4	**PLAN OF ACTION AND MILESTONES PROCESS**				
	Control: The organization: a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems: 1. Are developed and maintained; 2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and 3. Are reported in accordance with OMB FISMA reporting requirements. b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR RMF process fulfills the intent of this control.				

PM-5	**INFORMATION SYSTEM INVENTORY**				
	Control: The organization develops and maintains an inventory of its information systems.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				

Comments/ Rationale	Multiple databases already in place (e.g. eMASS, OOMA, WSPD, PMA CM Database). Programs will need to provide details of where they are registered to meet this control.

PM-6	**INFORMATION SECURITY MEASURES OF PERFORMANCE**				
	Control: The information organization develops, monitors, and reports on the results of information security measures of performance.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Focused on percentage of workforce meeting cybersecurity training requirements and other workforce-related efforts. Not applicable to weapon systems.				

PM-7	**ENTERPRISE ARCHITECTURE**				
	Control: The organization develops enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** Part of DoD RMF (Tier 1 Control).				

PM-8	**CRITICAL INFRASTRUCTURE PLAN**				
	Control: The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/	Unclear exact scope of term ‘infrastructure'. Likely covered by Program Protection Plan (PPP).				

Rationale	Marked as auto-compliant based on DODD 3020.40.

PM-9	**RISK MANAGEMENT STRATEGY**				
	Control: The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; b. Implements the risk management strategy consistently across the organization; and c. Reviews and updates the risk management strategy [*Assignment: organization-defined frequency*] or as required, to address organizational changes.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** Part of DoD RMF (Tier 1 Control).				

PM-10	**SECURITY AUTHORIZATION PROCESS**				
	Control: The organization: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization-wide risk management program.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** Part of DoD RMF (Tier 1 Control).				

PM-11	**MISSION/BUSINESS PROCESS DEFINITION**
	Control: The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes

	and revises the processes as necessary, until achievable protection needs are obtained.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR RMF process fulfills the intent of this control.				

PM-12	**INSIDER THREAT PROGRAM**				
	Control: The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Uniform Code of Military Justice (UCMJ). Existing OPSEC requirements for weapon systems meets the intent of this control.				

PM-13	**INFORMATION SECURITY WORKFORCE**				
	Control: The organization establishes an information security workforce development and improvement program.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Existing Cyberspace Workforce Management Policy meets the intent of this control. Auto compliant (DODD 8140.01).				

PM-14	**TESTING, TRAINING, AND MONITORING**
	Control: The organization: a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems:

	1. Are developed and maintained; and 2. Continue to be executed in a timely manner; b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR RMF process fulfills the intent of this control.				

PM-15	**CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS**				
	Control: The organization establishes and institutionalizes contact with selected groups and associations within the security community: a. To facilitate ongoing security education and training for organizational personnel; b. To maintain currency with recommended security practices, techniques, and technologies; and c. To share current security-related information including threats, vulnerabilities, and incidents.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Performed at Command (NAVAIR) level.				

PM-16	**THREAT AWARENESS PROGRAM**				
	Control: The organization implements a threat awareness program that includes a cross-organization information-sharing capability.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by DON/Command Training and Intel Coordination Efforts (STILO).				

PERSONNEL SECURITY

PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES				
	Control: The organization: a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and b. Reviews and updates the current: 1. Personnel security policy [*Assignment: organization-defined frequency*]; and 2. Personnel security procedures [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** All -1 are Medium, covered by policy.				

PS-2	POSITION RISK DESIGNATION				
	Control: The organization: a. Assigns a risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions; and Reviews and updates position risk designations [*Assignment: organization-defined*				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by policy and operational procedures.				

PS-3	PERSONNEL SCREENING				
	Control: The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to [*Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C	Applicable Unmanned A/C	Applicable Support	Applicable Shipboard

		Vehicle	Control Station	Equipment	Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by policy and operational procedures.				

PS-3(1)	**PERSONNEL SCREENING | *CLASSIFIED INFORMATION***				
	The organization ensures individuals accessing an information system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

PS-3(2)	**PERSONNEL SCREENING | *FORMAL INDOCTRINATION***				
	The organization ensures individuals accessing an information system processing, storing, or transmitting types of classified information which require formal indoctrination, are formally indoctrinated for all of the relevant types of information to which they have access on the system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

PS-3(3)	**PERSONNEL SCREENING | *INFORMATION WITH SPECIAL PROTECTION MEASURES***
	The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection: (a) Have valid access authorizations that are demonstrated by assigned official government duties; and (b) Satisfy [*Assignment: organization-defined additional personnel screening criteria*].

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

PS-4	**PERSONNEL TERMINATION**				
	Control: The organization, upon termination of individual employment: a. Disables information system access within [*Assignment: organization-defined time period*]; b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts exit interviews that include a discussion of [*Assignment: organization-defined information security topics*]; d. Retrieves all security-related organizational information system-related property; e. Retains access to organizational information and information systems formerly controlled by terminated individual; and f. Notifies [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*]				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by policy and operational procedures.				

PS-4(1)	**PERSONNEL TERMINATION | *POST-EMPLOYMENT REQUIREMENTS***				
	The organization: (a) Notifies terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information; and (b) Requires terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/	Refer to base control.				

Rationale	

PS-4(2)	**PERSONNEL TERMINATION | *AUTOMATED NOTIFICATION***				
	The organization employs automated mechanisms to notify [*Assignment: organization-defined personnel or roles*] upon termination of an individual.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Notification of termination may not be fully automated.				

PS-5	**PERSONNEL TRANSFER**				
	Control: The organization: a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*]; c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notifies [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by policy and operational procedures.				

PS-6	**ACCESS AGREEMENTS**
	Control: The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements [*Assignment: organization-defined frequency*]; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by policy and operational procedures.				

PS-6(1) - Withdrawn

PS-6(2)	**ACCESS AGREEMENTS | *CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION***				
	The organization ensures that access to classified information requiring special protection is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; (b) Satisfy associated personnel security criteria; and **(c)** Have read, understood, and signed a nondisclosure agreement.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by policy and operational procedures for those systems operating at this security levels. Not automatically applicable for all programs.				

PS-6(3)	**ACCESS AGREEMENTS | *POST-EMPLOYMENT REQUIREMENTS***				
	The organization: (a) Notifies individuals of applicable, legally binding post-employment requirements for protection of organizational information; and (b) Requires individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

PS-7	THIRD-PARTY PERSONNEL SECURITY				
	Control: The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify [*Assignment: organization-defined personnel or roles*] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [*Assignment: organization-defined time period*]; and e. Monitors provider compliance.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Industrial security (including prime contractor facilities) covered by policy and procedures. Likely inherited from host facility.				

PS-8	PERSONNEL SANCTIONS				
	Control: The organization: a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notifies [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by the Uniform Code of Military Justice (UCMJ) for military personnel and federal statues for all US citizens.				

RISK ASSESSMENT

RA-1	RISK ASSESSMENT POLICY AND PROCEDURES				
	Control: The organization: a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and b. Reviews and updates the current: 1. Risk assessment policy [*Assignment: organization-defined frequency*]; and 2. Risk assessment procedures [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** All -1 are Medium, covered by policy.				

RA-2	SECURITY CATEGORIZATION				
	Control: The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR RMF process fulfills the intent of this control.				

RA-3	RISK ASSESSMENT
	Control: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

	b. Documents risk assessment results in [*Selection: security plan; risk assessment report; [Assignment: organization-defined document]*]; c. Reviews risk assessment results [*Assignment: organization-defined frequency*]; d. Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*]; and e. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Preferred to meet this through Cyber Risk Assessment (CRA)/Cyber Tabletop (CTT) SWPs. This can also be met by being part of a larger CRA/CTT.				

RA-4 – Withdrawn

RA-5	**VULNERABILITY SCANNING**				
	Control: The organization: a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	ACAS meets this control (for scan-able systems). Current gap in scanning weapon systems. Not applicable if no scanning mechanism exists. Often at least part of a system will be scan-able.				

RA-5(1)	**VULNERABILITY SCANNING | *UPDATE TOOL CAPABILITY***				
	The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Scanning requires updating of signatures and profiles. Covered if using ACAS.				

RA-5(2)	**VULNERABILITY SCANNING | *UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED***				
	The organization updates the information system vulnerabilities scanned [*Selection (one or more):* [*Assignment: organization-defined frequency*]*; prior to a new scan; when new vulnerabilities are identified and reported*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to RA-5(1).				

RA-5(3)	**VULNERABILITY SCANNING | *BREADTH / DEPTH OF COVERAGE***				
	The organization employs vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Breadth/depth of weapon systems typically limited.				

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

	The organization determines what information about the information system is discoverable by adversaries and subsequently takes [*Assignment: organization-defined corrective actions*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Good practice. Brings up some classification by compilation concerns regarding scan data. Likely result is treating scan data as FOUO/CUI. Encrypt during storage and transport. Could also obfuscate scan to platform mapping.				

RA-5(5)	**VULNERABILITY SCANNING | *PRIVILEGED ACCESS***				
	The information system implements privileged access authorization to [*Assignment: organization-identified information system components*] for selected [*Assignment: organization-defined vulnerability scanning activities*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Use of credentialed scans meets the intent of this control.				

RA-5(6)	**VULNERABILITY SCANNING | *AUTOMATED TREND ANALYSES***				
	The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Use of directed scanning tools (e.g., ACAS, VRAM) meets the intent of this control.				

RA-5(7) – Withdrawn

RA-5(8)	VULNERABILITY SCANNING | *REVIEW HISTORIC AUDIT LOGS*				
	The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Good practice.				

RA-5(9) – Withdrawn

RA-5(10)	VULNERABILITY SCANNING | *CORRELATE SCANNING INFORMATION*				
	The organization correlates the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Good practice. Should be part of the input to a patch management strategy.				

RA-6	TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY				
	Control: The organization employs a technical surveillance countermeasures survey at [*Assignment: organization-defined locations*] [*Selection (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined events or indicators occur*]].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Expensive, focused primarily on preventing exfiltration. Not applicable for most weapon systems, but may be required based on physical security requirements.				

SYSTEM AND SERVICES ACQUISITION

SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES				
	Control: The organization: a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and updates the current: 1. System and services acquisition policy [*Assignment: organization-defined frequency*]; and 2. System and services acquisition procedures [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** All -1 are Medium, covered by policy.				

SA-2	ALLOCATION OF RESOURCES				
	Control: The organization: a. Determines information security requirements for the information system or information system service in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	SETR process and DoDI 8510.01, DoDI 5000.02 meet the intent of this control**.**				

SA-3	SYSTEM DEVELOPMENT LIFE CYCLE
	Control: The organization: a. Manages the information system using [*Assignment: organization-defined system development life cycle*] that incorporates information security considerations;

	b. Defines and documents information security roles and responsibilities throughout the system development life cycle; c. Identifies individuals having information security roles and responsibilities; and d. Integrates the organizational information security risk management process into system development life cycle activities.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	SETR process and DoDI 8510.01, DoDI 5000.02 meet the intent of this control**.**				

SA-4	**ACQUISITION PROCESS**				
	Control: The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs: a. Security functional requirements; b. Security strength requirements; c. Security assurance requirements; d. Security-related documentation requirements; e. Requirements for protecting security-related documentation; f. Description of the information system development environment and environment in which the system is intended to operate; and g. Acceptance criteria.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	SETR process and DoDI 8510.01, DoDI 5000.02 meet the intent of this control**.**				

SA-4(1)	**ACQUISITION PROCESS | *FUNCTIONAL PROPERTIES OF SECURITY CONTROLS***				
	The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems

	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

SA-4(2)	**ACQUISITION PROCESS | *DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS***				
	The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [*Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics;* [*Assignment: organization-defined design/implementation information*]] at [*Assignment: organization-defined level of detail*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

SA-4(3)	**ACQUISITION PROCESS | *DEVELOPMENT METHODS / TECHNIQUES / PRACTICES***				
	The organization requires the developer of the information system, system component, or information system service to demonstrate the use of a system development life cycle that includes [*Assignment: organization-defined state-of-the-practice system/security engineering methods, software development methods, testing/evaluation/validation techniques, and quality control processes*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

SA-4(4) – Withdrawn

SA-4(5)	**ACQUISITION PROCESS | *SYSTEM / COMPONENT / SERVICE CONFIGURATIONS***

	The organization requires the developer of the information system, system component, or information system service to: (a) Deliver the system, component, or service with [*Assignment: organization-defined security configurations*] implemented; and (b) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

SA-4(6)	**ACQUISITION PROCESS | *USE OF INFORMATION ASSURANCE PRODUCTS***				
	The organization employs: (a) Employs only government off-the-shelf (GOTS) or commercial off-the-shelf (COTS) information assurance (IA) and IA-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and (b) Ensures these products have been evaluated and/or validated by NSA or in accordance with NSA-approved procedures.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Checking for approved GOTS/COTS encryption solutions for bulk encryption of classified info over unclassified pipes. Note: SP 800-53 description is unclear in re this control being encryption-based.				

SA-4(7)	**ACQUISITION PROCESS | *NIAP-APPROVED PROTECTION PROFILES***				
	The organization: (a) Limits the use of commercially provided information assurance (IA) and IA-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; and (b) Requires, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded

					Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Valuable to track the National Information Assurance Partnership (NIAP) profile levels. Care must be taken not to unduly drive cost. This control states a spec would call out the appropriate NIAP level where appropriate.				

SA-4(8)	**ACQUISITION PROCESS | *CONTINUOUS MONITORING PLAN***				
	The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains [*Assignment: organization-defined level of detail*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR RMF process meets the intent.				

SA-4(9)	**ACQUISITION PROCESS | *FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE***				
	The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	NAVAIR RMF process meets the intent.				

SA-4(10)	**ACQUISITION PROCESS | *USE OF APPROVED PIV PRODUCTS***				
	The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems**.**				
Rating	Applicable Manned A/C	Applicable Unmanned A/C	Applicable Unmanned A/C	Applicable Support	Applicable Shipboard

		Vehicle	Control Station	Equipment	Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Defined by DoD policy (e.g., CAC).				

SA-5	**INFORMATION SYSTEM DOCUMENTATION**				
	Control: The organization: a. Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; b. Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and takes [*Assignment: organization-defined actions*] in response; d. Protects documentation as required, in accordance with the risk management strategy; and e. Distributes documentation to [*Assignment: organization-defined personnel or roles*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by several areas: SETR, Naval Air Training and Operating Procedures Standardization (NATOPS), NAVAIR RMF Process, Contractual/DFARS, DoD 5000 series (Personal Protection Plan (PPP)/Cybersecurity Strategy (CSS)).				

SA-5(1) – Withdrawn

SA-5(2) – Withdrawn

SA-5(3) – Withdrawn

SA-5(4) – Withdrawn

SA-5(5) – Withdrawn

SA-6 – Withdrawn

SA-7 – Withdrawn

SA-8	**SECURITY ENGINEERING PRINCIPLES**				
	Control: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by SETR.				

SA-9	**EXTERNAL INFORMATION SYSTEM SERVICES**				
	Control: The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ [*Assignment: organization-defined security controls*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs [*Assignment: organization-defined processes, methods, and techniques*] to monitor security control compliance by external service providers on an ongoing basis				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Care must be taken to define "external" for each system. Supplemental guidance indicates this would be anything outside of the Programs accreditation boundary. Should not be applied internally to a platform's subsystems. Typically addressed by Interagency Agreements or MOAs (rather than commercial agreements).				

SA-9(1)	**EXTERNAL INFORMATION SYSTEM SERVICES | *RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS***
	The organization:

	(a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and (b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by [*Assignment: organization-defined personnel or roles*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Typically core weapon functions such as these cannot be outsourced. Some cases may exist in which function is "outsourced" to original equipment manufacturer (OEM) or other SYSCOM. Could have cases where external security services are inherited.				

SA-9(2)	**EXTERNAL INFORMATION SYSTEM SERVICES | *IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES***				
	The organization requires providers of [*Assignment: organization-defined external information system services*] to identify the functions, ports, protocols, and other services required for the use of such services.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	L	N/A	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	For aircraft, avoid weakening firewall to try to support real time monitoring during operations.				

SA-9(3)	**EXTERNAL INFORMATION SYSTEM SERVICES | *ESTABLISH / MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS***				
	The organization establishes, documents, and maintains trust relationships with external service providers based on [*Assignment: organization-defined security requirements, properties, factors, or conditions defining acceptable trust relationships*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Critical to maintain relationships with any external service providers. This control should be paired with SA-9(1). This control should not be tailored out if external services exist.				

SA-9(4)	**EXTERNAL INFORMATION SYSTEM SERVICES | *CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS***				
	The organization employs [*Assignment: organization-defined security safeguards*] to ensure that the interests of [*Assignment: organization-defined external service providers*] are consistent with and reflect organizational interests.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Weapon systems will be limited to only using trusted service providers typically USG/DOD/DON providers rather than commercial.				

SA-9(5)	**EXTERNAL INFORMATION SYSTEM SERVICES | *PROCESSING, STORAGE, AND SERVICE LOCATION***				
	The organization restricts the location of [*Selection (one or more): information processing; information/data; information system services*] to [*Assignment: organization-defined locations*] based on [*Assignment: organization-defined requirements or conditions*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Weapon systems will be limited to only using trusted service providers typically USG/DOD/DON providers rather than commercial.				

SA-10	**DEVELOPER CONFIGURATION MANAGEMENT**				
	Control: The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service [*Selection (one or more): design; development; implementation; operation*]; b. Document, manage, and control the integrity of changes to [*Assignment: organization-defined configuration items under configuration management*]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [*Assignment: organization-defined personnel*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C	Applicable Unmanned A/C	Applicable Support	Applicable Shipboard

		Vehicle	Control Station	Equipment	Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Good practice; typically requires contract language and DFARS clauses.				

SA-10(1)	**DEVELOPER CONFIGURATION MANAGEMENT | *SOFTWARE / FIRMWARE INTEGRITY VERIFICATION***				
	The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	This control has some ambiguity based on its relationship with SI-7 (SI-7 is a critical (high) control). This control should be paired with SI-7 to drive integrity back to SSA regardless of prime contractor or government run.				

SA-10(2)	**DEVELOPER CONFIGURATION MANAGEMENT | *ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES***				
	The organization provides an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Alternate Configuration Management (CM) processes should not be allowed. (CM processes should be driven by contract requirements (typical) or by MOU with government run SSA.)				

SA-10(3)	**DEVELOPER CONFIGURATION MANAGEMENT | *HARDWARE INTEGRITY VERIFICATION***				
	The organization requires the developer of the information system, system component, or information system service to enable integrity verification of hardware components.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C	Applicable Unmanned A/C	Applicable Support	Applicable Shipboard

		Vehicle	Control Station	Equipment	Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Care must be taken not to unduly drive cost with this control. There are applications in which it is very valid. Needs to be highly targeted on key components and not broadly applied.				

SA-10(4)	**DEVELOPER CONFIGURATION MANAGEMENT | *TRUSTED GENERATION***				
	The organization requires the developer of the information system, system component, or information system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions and software/firmware source and object code with previous versions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Source code versioning system in an SSA typically meets the intent.				

SA-10(5)	**DEVELOPER CONFIGURATION MANAGEMENT | *MAPPING INTEGRITY FOR VERSION CONTROL***				
	The organization requires the developer of the information system, system component, or information system service to maintain the integrity of the mapping between the master build data (hardware drawings and software/firmware code) describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Note: Assumes all weapon system software is security-relevant. Configuration management processes and contractual requirements typically meet the intent.				

SA-10(6)	**DEVELOPER CONFIGURATION MANAGEMENT | *TRUSTED DISTRIBUTION***
	The organization requires the developer of the information system, system component, or information system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Critical to ensure weapon system software loads are trusted.				

SA-11	**DEVELOPER SECURITY TESTING AND EVALUATION**				
	Control: The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform [*Selection (one or more): unit; integration; system; regression*] testing/evaluation at [*Assignment: organization-defined depth and coverage*]; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Key to enforce secure-coding practices and flaw remediation – this will drive costs. There needs to be a spectrum of acceptable levels of T&E based on system criticality.				

SA-11(1)	**DEVELOPER SECURITY TESTING AND EVALUATION | *STATIC CODE ANALYSIS***				
	The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Probably the easiest T&E mechanism to implement. Need to ensure remediation, not just analysis.				

SA-11(2)	**DEVELOPER SECURITY TESTING AND EVALUATION | *THREAT AND VULNERABILITY ANALYSES***				
	The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	At a minimum, this would be a requirement for the developers to scan the DT system periodically with up to date signatures to find Common Vulnerabilities and Exposures (CVE) early.				

SA-11(3)	**DEVELOPER SECURITY TESTING AND EVALUATION | *INDEPENDENT VERIFICATION OF ASSESSMENT PLANS / EVIDENCE***				
	The organization: (a) Requires an independent agent satisfying [*Assignment: organization-defined independence criteria*] to verify the correct implementation of the developer security assessment plan and the evidence produced during security testing/evaluation; and (b) Ensures that the independent agent is either provided with sufficient information to complete the verification process or granted the authority to obtain such information.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	For classified systems, this might be fulfilled by DSS. Good practice to have independent assessment. Must be supported by CDRL and DFARS clauses.				

SA-11(4)	**DEVELOPER SECURITY TESTING AND EVALUATION | *MANUAL CODE REVIEWS***				
	The organization requires the developer of the information system, system component, or information system service to perform a manual code review of [*Assignment: organization-defined specific code*] using [*Assignment: organization-defined processes, procedures, and/or techniques*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				

Comments/ Rationale	Manual code reviews are notoriously expensive for large code bases and have known reducing returns as code base increases.

SA-11(5)	**DEVELOPER SECURITY TESTING AND EVALUATION | *PENETRATION TESTING***				
	The organization requires the developer of the information system, system component, or information system service to perform penetration testing at [*Assignment: organization-defined breadth/depth*] and with [*Assignment: organization-defined constraints*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Good practice to require industry partners to pen test prior to delivery. For government developers should be a requirement.				

SA-11(6)	**DEVELOPER SECURITY TESTING AND EVALUATION | *ATTACK SURFACE REVIEWS***				
	The organization requires the developer of the information system, system component, or information system service to perform attack surface reviews.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Good practice. Fulfilled by Cyber Risk Assessment (CRA), can also be done independent of CRA SWP methodology.				

SA-11(7)	**DEVELOPER SECURITY TESTING AND EVALUATION | *VERIFY SCOPE OF TESTING / EVALUATION***				
	The organization requires the developer of the information system, system component, or information system service to verify that the scope of security testing/evaluation provides complete coverage of required security controls at [*Assignment: organization-defined depth of testing/evaluation*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				

Comments/ Rationale	Can be a significant cost driver if too broadly applied (e.g. formal methods).

SA-11(8)	**DEVELOPER SECURITY TESTING AND EVALUATION | *DYNAMIC CODE ANALYSIS***				
	The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Dynamic code analysis typically requires deep hooks into system functions to provide the censoring of that execution. This can be very difficult to achieve in Real Time Operating Systems (RTOS). Can be expensive, but very powerful. Fuzzing is excellent technique to stim, but needs proper structuring. DAL A (DO-178C) meets the intent.				

SA-12	**SUPPLY CHAIN PROTECTION**				
	Control: The organization protects against supply chain threats to the information system, system component, or information system service by employing [*Assignment: organization-defined security safeguards*] as part of a comprehensive, defense-in-breadth information security strategy				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	If addressed in Program Protection Plan (PPP), can be leveraged to meet this control. Very expensive to apply broadly. At a minimum, existing protections must be documented for legacy systems (to extent visible to program office).				

SA-12(1)	**SUPPLY CHAIN PROTECTION | *ACQUISITION STRATEGIES / TOOLS / METHODS***				
	The organization employs [*Assignment: organization-defined tailored acquisition strategies, contract tools, and procurement methods*] for the purchase of the information system, system component, or information system service from suppliers.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M

Difficulty w/Legacy	High
Comments/ Rationale	Refer to base control. Limited ability of government acquisition to directly affect sub-tier suppliers.

SA-12(2)	**SUPPLY CHAIN PROTECTION | *SUPPLY REVIEWERS***				
	The organization conducts a supplier review prior to entering into a contractual agreement to acquire the information system, system component, or information system service.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control. Limited ability of government acquisition to directly affect sub-tier suppliers.				

SA-12(3) – Withdrawn

SA-12(4) – Withdrawn

SA-12(5)	**SUPPLY CHAIN PROTECTION | *LIMITATION OF HARM***				
	The organization employs [*Assignment: organization-defined security safeguards*] to limit harm from potential adversaries identifying and targeting the organizational supply chain.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Difficult for government acquisition to affect supplier selection.				

SA-12(6) – Withdrawn

SA-12(7)	**SUPPLY CHAIN PROTECTION | *ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE***				
	The organization conducts an assessment of the information system, system component, or information system service prior to selection, acceptance, or update.				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Difficult for government acquisition to affect supplier selection.				

SA-12(8)	**SUPPLY CHAIN PROTECTION | *USE OF ALL-SOURCE INTELLIGENCE***				
	The organization uses all-source intelligence analysis of suppliers and potential suppliers of the information system, system component, or information system service.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Difficult for government acquisition to affect supplier selection.				

SA-12(9)	**SUPPLY CHAIN PROTECTION | *OPERATIONS SECURITY***				
	The organization employs [*Assignment: organization-defined Operations Security (OPSEC) safeguards*] in accordance with classification guides to protect supply chain-related information for the information system, system component, or information system service.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Typically only applied on strategic/high sensitivity platforms – cost driver.				

SA-12(10)	**SUPPLY CHAIN PROTECTION | *VALIDATE AS GENUINE AND NOT ALTERED***				
	The organization employs [*Assignment: organization-defined security safeguards*] to validate that the information system or system component received is genuine and has not been altered.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded

					Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Care must be taken not to unduly drive cost with this control. There are applications in which this is very valid. Needs to be highly targeted on key components and not broadly applied. Tied to SA-10(3).				

SA-12(11)	**SUPPLY CHAIN PROTECTION | *PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS***				
	The organization employs [*Selection (one or more): organizational analysis, independent third-party analysis, organizational penetration testing, independent third-party penetration testing*] of [*Assignment: organization-defined supply chain elements, processes, and actors*] associated with the *information system, system component, or information system service*.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Typically only applied on strategic/high sensitivity platforms – cost driver.				

SA-12(12)	**SUPPLY CHAIN PROTECTION | *INTER-ORGANIZATIONAL AGREEMENTS***				
	The organization establishes inter-organizational agreements and procedures with entities involved in the supply chain for the information system, system component, or information system service.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Good practice.				

SA-12(13)	**SUPPLY CHAIN PROTECTION | *CRITICAL INFORMATION SYSTEM COMPONENTS***				
	The organization employs [*Assignment: organization-defined security safeguards*] to ensure an adequate supply of [*Assignment: organization-defined critical information system components*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C	Applicable Unmanned A/C	Applicable Support	Applicable Shipboard

		Vehicle	Control Station	Equipment	Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	Operationally met by sparing plans.				

SA-12(14)	**SUPPLY CHAIN PROTECTION | *IDENTITY AND TRACEABILITY***				
	The organization establishes and retains unique identification of [*Assignment: organization-defined supply chain elements, processes, and actors*] for the information system, system component, or information system service.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Typically only applied on strategic/high sensitivity platforms – cost driver.				

SA-12(15)	**SUPPLY CHAIN PROTECTION | *PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES***				
	The organization establishes a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Low				
Comments/ Rationale	DoD acquisition may struggle to force any changes.				

SA-13	**TRUSTWORTHINESS**
	Control: The organization: a. Describes the trustworthiness required in the [*Assignment: organization-defined information system, information system component, or information system service*] supporting its critical missions/business functions; and b. Implements [*Assignment: organization-defined assurance overlay*] to achieve such trustworthiness.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Abstract. Unclear how this would be met other than by doing NAVAIR RMF.				

SA-14	**CRITICALITY ANALYSIS**				
	Control: The organization identifies critical information system components and functions by performing a criticality analysis for [*Assignment: organization-defined information systems, information system components, or information system services*] at [*Assignment: organization-defined decision points in the system development life cycle*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Part of Program Protection Plan (PPP); also identified during CRA Process.				

SA-14(1) – Withdrawn

SA-15	**DEVELOPMENT PROCESS, STANDARDS, AND TOOLS**				
	Control: The organization: a. Requires the developer of the information system, system component, or information system service to follow a documented development process that: 1. Explicitly addresses security requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Reviews the development process, standards, tools, and tool options/configurations [*Assignment: organization-defined frequency*] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [*Assignment: organization-defined security requirements*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems

	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by SETR. Absolutely critical and needs to be matured.				

SA-15(1)	**DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | *QUALITY METRICS***				
	The organization requires the developer of the information system, system component, or information system service to: (a) Define quality metrics at the beginning of the development process; and (b) Provide evidence of meeting the quality metrics [*Selection (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined program review milestones*]; *upon delivery*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Metrics not as important as good cross-competency design and development in the SSE trade-space.				

SA-15(2)	**DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | *SECURITY TRACKING TOOLS***				
	The organization requires the developer of the information system, system component, or information system service to select and employ a security tracking tool for use during the development process.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	For NAVAIR acquisition systems, this is often tracked through a more comprehensive deficiency tracking database. Does not need to be a specific cybersecurity tool, but should be tracked. Often better to have it as a comprehensive tracking database rather than an independent cybersecurity tracking tool.				

SA-15(3)	**DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | *CRITICALITY ANALYSIS***
	The organization requires the developer of the information system, system component, or information system service to perform a criticality analysis at [*Assignment: organization-defined breadth/depth*] and at [*Assignment: organization-defined decision points in the system development life cycle*].

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Directly tied to SA-14. Part of Program Protection Plan (PPP) /Cyber Risk Assessment (CRA). Much of the system expertise during DT is resident at developer. Critical to have their input.				

SA-15(4)	**DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | *THREAT MODELING / VULNERABILITY ANALYSIS***				
	The organization requires that developers perform threat modeling and a vulnerability analysis for the information system at [*Assignment: organization-defined breadth/depth*] that: (a) Uses [*Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels*]; (b) Employs [*Assignment: organization-defined tools and methods*]; and (c) Produces evidence that meets [*Assignment: organization-defined acceptance criteria*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Developer side of Cyber Risk Assessment (CRA)/Cyber Tabletop (CTT). Met if developer included in CRA / CTT efforts.				

SA-15(5)	**DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | *ATTACK SURFACE REDUCTION***				
	The organization requires the developer of the information system, system component, or information system service to reduce attack surfaces to [*Assignment: organization-defined thresholds*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Mitigation/remediation phase following Cyber Risk Assessment (CRA)/Cyber Tabletop (CTT) /testing efforts.				

SA-15(6)	**DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | *CONTINUOUS IMPROVEMENT***

	The organization requires the developer of the information system, system component, or information system service to implement an explicit process to continuously improve the development process.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Cybersecurity should not be driving (e.g. cost) process improvement. NAVAIR has other 5000/Better Buying Power (BBP), et cetera. that cover this generally, but not specific to cybersecurity improvements.				

SA-15(7)	**DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | *AUTOMATED VULNERABILITY ANALYSIS***				
	The organization requires the developer of the information system, system component, or information system service to: (a) Perform an automated vulnerability analysis using [*Assignment: organization-defined tools*]; (b) Determine the exploitation potential for discovered vulnerabilities; (c) Determine potential risk mitigations for delivered vulnerabilities; and (d) Deliver the outputs of the tools and results of the analysis to [*Assignment: organization-defined personnel or roles*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Typically covered through scans (e.g. ACAS). Other tools also acceptable that go beyond simple scanning. Can be good practice. Not all weapon system components easily accessed by automated tools.				

SA-15(8)	**DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | *REUSE OF THREAT / VULNERABILITY INFORMATION***				
	The organization requires the developer of the information system, system component, or information system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty	Moderate				

w/Legacy	
Comments/ Rationale	This is aimed at updating scan databases to include current threats. From a DoD acquisition perspective, there is often a separation of duties in which sharing of information would occur at the government side, not enforced at the contractor level.

SA-15(9)	**DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | *USE OF LIVE DATA***				
	The organization approves, documents, and controls the use of live data in development and test environments for the information system, system component, or information system service.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Typically weapon system developers are already using test data rather than live data due to classification issues of the live data. Good practice to avoid Live Data in test environments when not absolutely needed (attack surface).				

SA-15(10)	**DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | *INCIDENT RESPONSE PLAN***				
	The organization requires the developer of the information system, system component, or information system service to provide an incident response plan.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by PPIP / DFARS when contractor is developer. It appears that when DoD is Lead System Integrator (LSI), this would be covered by existing command security response policies and processes.				

SA-15(11)	**DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | *ARCHIVE INFORMATION SYSTEM / COMPONENT***				
	The organization requires the developer of the information system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security review.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M

Difficulty w/Legacy	Low
Comments/ Rationale	Addressed by policy primarily dealing with not deploying new builds until they have ATO with conditions / ATO / IATT in place.

SA-16	**DEVELOPER-PROVIDED TRAINING**				
	Control: The organization requires the developer of the information system, system component, or information system service to provide [*Assignment: organization-defined training*] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	This should be incorporated into the broader weapon system training. Developer provided training is an option, but typically the overall responsibility for training on the weapon system is a PMA responsibility.				

SA-17	**DEVELOPER SECURITY ARCHITECTURE AND DESIGN**				
	Control: The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that: a. Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Key part of the System Security Engineering (SSE) process. This is the actual program artifacts, not just its inclusion in SETR.				

SA-17(1)	**DEVELOPER SECURITY ARCHITECTURE AND DESIGN | *FORMAL POLICY MODEL***
	The organization requires the developer of the information system, system component, or information system service to: (a) Produce, as an integral part of the development process, a formal policy model describing the [*Assignment: organization-defined elements of organizational security policy*] to be enforced;

	and (b) Prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security policy when implemented.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Care must be taken on this control. Great if done correctly (e.g., use of HACMS OS), but should not be mandated. Formal methods can become huge cost drivers.				

SA-17(2)	**DEVELOPER SECURITY ARCHITECTURE AND DESIGN | *SECURITY-RELEVANT COMPONENTS***				
	The organization requires the developer of the information system, system component, or information system service to: (a) Define security-relevant hardware, software, and firmware; and (b) Provide a rationale that the definition for security-relevant hardware, software, and firmware is complete.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Part of the NAVAIR RMF package for software and hardware lists. Effectively a required good practice.				

SA-17(3)	**DEVELOPER SECURITY ARCHITECTURE AND DESIGN | *FORMAL CORRESPONDENCE***
	The organization requires the developer of the information system, system component, or information system service to: (a) Produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects; (b) Show via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model; (c) Show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; (d) Show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and firmware; and (e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware, software, and firmware.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Care must be taken on this control. Great if done correctly (e.g., use of High Assurance Cyber Military Systems-Operating System (HACMS OS), but should not be mandated. Formal methods can become huge cost drivers.				

SA-17(4)	**DEVELOPER SECURITY ARCHITECTURE AND DESIGN | *INFORMAL CORRESPONDENCE***				
	The organization requires the developer of the information system, system component, or information system service to: (a) Produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects; (b) Show via [Selection: informal demonstration, convincing argument with formal methods as feasible] that the descriptive top-level specification is consistent with the formal policy model; (c) Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; (d) Show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware; and (e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware, software, and firmware.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Note the term "informal" is in relation to formal methods. This would still be formalized through contract requirements. Most weapon systems will meet this through ICD and required milestone demonstrations.				

SA-17(5)	**DEVELOPER SECURITY ARCHITECTURE AND DESIGN | *CONCEPTUALLY SIMPLE DESIGN***				
	The organization requires the developer of the information system, system component, or information system service to: (a) Design and structure the security-relevant hardware, software, and firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics; and (b) Internally structure the security-relevant hardware, software, and firmware with specific regard for this mechanism.				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Abstract concept has merit as a design principle. Unclear how testable this would be or what "simple" would be for complicated weapon systems.				

SA-17(6)	**DEVELOPER SECURITY ARCHITECTURE AND DESIGN | *STRUCTURE FOR TESTING***				
	The organization requires the developer of the information system, system component, or information system service to structure security-relevant hardware, software, and firmware to facilitate testing.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Abstract concept has merit as a design principle. Unclear how testable this would be.				

SA-17(7)	**DEVELOPER SECURITY ARCHITECTURE AND DESIGN | *STRUCTURE FOR LEAST PRIVILEGE***				
	The organization requires the developer of the information system, system component, or information system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Abstract concept has merit as a design principle. Unclear how testable this would be.				

SA-18	**TAMPER RESISTANCE AND DETECTION**				
	Control: The organization implements a tamper protection program for the information system, system component, or information system service.				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	U.S. Navy has an Anti-Tamper Program. May be acceptable mitigations (e.g. USB Locker, tamper-evident tape). Can be a useful tool; should not be required.				

SA-18(1)	**TAMPER RESISTANCE AND DETECTION | *MULTIPLE PHASES OF SDLC***				
	The organization employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including design, development, integration, operations, and maintenance.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

SA-18(2)	**TAMPER RESISTANCE AND DETECTION | *INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES***				
	The organization inspects [*Assignment: organization-defined information systems, system components, or devices*] [*Selection (one or more): at random;* at [*Assignment: organization-defined frequency*], *upon* [*Assignment: organization-defined indications of need for inspection*]] to detect tampering.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

SA-19	**COMPONENT AUTHENTICITY**
	Control: The organization: a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; and

	b. Reports counterfeit information system components to [*Selection (one or more): source of counterfeit component;* [*Assignment: organization-defined external reporting organizations*]; [*Assignment: organization-defined personnel or roles*]].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Would be documented in Program Protection Plan (PPP) and partially covered by SETR. Very expensive to apply broadly. Certainly needed for certain systems and components. Limited ability of government acquisition to directly affect sub-tier suppliers. This control would be broader than what is covered in the PPP and include items such as ensuring a router is genuine.				

SA-19(1)	**COMPONENT AUTHENTICITY | *ANTI-COUNTERFEIT TRAINING***				
	The organization trains [*Assignment: organization-defined personnel or roles*] to detect counterfeit information system components (including hardware, software, and firmware).				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SA-19(2)	**COMPONENT AUTHENTICITY | *CONFIGURATION CONTROL FOR COMPONENT SERVICE / REPAIR***				
	The organization maintains configuration control over [*Assignment: organization-defined information system components*] awaiting service/repair and serviced/repaired components awaiting return to service.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	High concern for Operational to Original Equipment Manufacturer (O to OEM) items; less concern for Depot Maintenance items where Navy personnel maintain control.				

SA-19(3)	COMPONENT AUTHENTICITY | *COMPONENT DISPOSAL*				
	The organization disposes of information system components using [*Assignment: organization-defined techniques and methods*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by policy (Demolition/Disposal/Destruction (DDD))				

SA-19(4)	COMPONENT AUTHENTICITY | *ANTI-COUNTERFEIT SCANNING*				
	The organization scans for counterfeit information system components [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SA-20	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS				
	Control: The organization re-implements or custom develops [*Assignment: organization-defined critical information system components*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	This would be custom Application-Specific Integrated Circuits (ASIC) or trusted foundry components. Must be applied very judiciously - significant cost driver. Would often be driven by policies external to NAVAIR RMF.				

SA-21	DEVELOPER SCREENING

	Control: The organization requires that the developer of [*Assignment: organization-defined information system, system component, or information system service*]: a. Have appropriate access authorizations as determined by assigned [*Assignment: organization-defined official government duties*]; and b. Satisfy [*Assignment: organization-defined additional personnel screening criteria*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Met by policy for cleared personnel in sensitive environments.				

SA-21(1)	**DEVELOPER SCREENING | *VALIDATION OF SCREENING***				
	The organization requires the developer of the information system, system component, or information system service take [*Assignment: organization-defined actions*] to ensure the required access authorizations and screening criteria are satisfied.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

SA-22	**UNSUPPORTED SYSTEM COMPONENTS**				
	Control: The organization: a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Partially covered by policy in 5000 acquisition. Solid best practice, but timelines need to be appropriate to weapon system upgrade and life cycle timelines (e.g. Unsupported Extended				

	Maintenance (USEM) / Win XP eradication).

SA-22(1)	**UNSUPPORTED SYSTEM COMPONENTS | *ALTERNATIVE SOURCES FOR CONTINUED SUPPORT***				
	The organization provides [*Selection (one or more): in-house support;* [*Assignment: organization-defined support from external providers*]] for unsupported information system components.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control. This would be DoD buying additional years of support for XP.				

SYSTEM AND COMMUNICATIONS PROTECTION

SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES				
	Control: The organization: a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates the current: 1. System and communications protection policy [*Assignment: organization-defined frequency*]; and 2. System and communications protection procedures [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	All -1 are Medium, covered by policy.				

SC-2	APPLICATION PARTITIONING				
	Control: The information system separates user functionality (including user interface services) from information system management functionality.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Some value in separation of interfaces; not feasible to allocate separate hardware in most NAVAIR weapon systems.				

SC-2(1)	APPLICATION PARTITIONING | *INTERFACES FOR NON-PRIVILEGED USERS*				
	The information system prevents the presentation of information system management-related functionality at an interface for non-privileged users.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C	Applicable Unmanned A/C	Applicable Support	Applicable Shipboard

		Vehicle	Control Station	Equipment	Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-3	**SECURITY FUNCTION ISOLATION**				
	Control: The information system isolates security functions from non-security functions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Weapon systems generally lack publically exposed functionality where this would be critical.				

SC-3(1)	**SECURITY FUNCTION ISOLATION | *HARDWARE SEPARATION***				
	The information system utilizes underlying hardware separation mechanisms to implement security function isolation.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Very expensive, low ROI; CNSSI 1253 does not require.				

SC-3(2)	**SECURITY FUNCTION ISOLATION | *ACCESS / FLOW CONTROL FUNCTIONS***				
	The information system isolates security functions enforcing access and information flow control from non-security functions and from other security functions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L

Difficulty w/Legacy	High
Comments/ Rationale	Refer to SC-3(1).

SC-3(3)	**SECURITY FUNCTION ISOLATION | *MINIMIZE NONSECURITY FUNCTIONALITY***				
	The organization minimizes the number of non-security functions included within the isolation boundary containing security functions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to SC-3(1).				

SC-3(4)	**SECURITY FUNCTION ISOLATION | *MODULE COUPLING AND COHESIVENESS***				
	The organization implements security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to SC-3(1).				

SC-3(5)	**SECURITY FUNCTION ISOLATION | *LAYERED STRUCTURES***				
	The organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty	High				

w/Legacy	
Comments/ Rationale	Refer to SC-3(1).

SC-4	**INFORMATION IN SHARED RESOURCES**				
	Control: The information system prevents unauthorized and unintended information transfer via shared system resources.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Typically accomplished by zeroing heap allocation before hand-back. Not valuable in weapon systems; typically do not share computing resources outside of the weapon system.				

SC-4(1) – Withdrawn

SC-4(2)	**INFORMATION IN SHARED RESOURCES | *PERIODS PROCESSING***				
	The information system prevents unauthorized information transfer via shared resources in accordance with [*Assignment: organization-defined procedures*] when system processing explicitly switches between different information classification levels or security categories.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Typically handled by operating the weapon system at the highest classification level. Otherwise enforced by Multi-Level Security (MLS) requirements and controls. Found in only one cross-domain solution (CDS) overlay, not CNSSI 1253.				

SC-5	**DENIAL OF SERVICE PROTECTION**				
	Control: The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined types of denial of service attacks or references to sources for such information*] by employing [*Assignment: organization-defined security safeguards*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded

					Systems
	M	M	M	L	M
Difficulty w/Legacy	High				
Comments/ Rationale	Control needs to be discussed as general DOS mitigations to include non-IP data flows. Most weapon systems are not directly IP addressable so enterprise concept of DOS/DDOS is not the concern.				

SC-5(1)	**DENIAL OF SERVICE PROTECTION | *RESTRICT INTERNAL USERS***				
	The information system restricts the ability of individuals to launch [*Assignment: organization-defined denial of service attacks*] against other information systems.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Difficult to implement on tactical systems without causing operational issues.				

SC-5(2)	**SYSTEM DENIAL OF SERVICE PROTECTION | *EXCESS CAPACITY / BANDWIDTH / REDUNDANCY***				
	The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Difficult to implement on tactical systems without causing operational issues. In enterprise example, this might be preventing a user from making more than 4K DNS requests in a time period.				

SC-5(3)	**DENIAL OF SERVICE PROTECTION | *DETECTION / MONITORING***				
	The organization: **(a)** Employs [*Assignment: organization-defined monitoring tools*] to detect indicators of denial of service attacks against the information system; and **(b)** Monitors [*Assignment: organization-defined information system resources*] to determine if sufficient resources exist to prevent effective denial of service attacks.				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Scope needs to be broader than IP-based data flows. NAVAIR should be monitoring all data flows for abnormal activity. Note: this does not mandate an automated response, just detect/monitor.				

SC-6	**RESOURCE AVAILABILITY**				
	Control: The information system protects the availability of resources by allocating [*Assignment: organization-defined resources*] by [*Selection (one or more); priority; quota;* [*Assignment: organization-defined security safeguards*]].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Computing resource segmentation is typically addressed for safety reasons (e.g. RTOS ARINC 653 Partitions) rather than cybersecurity, but meets the intent of this control (in many cases). Due to cost, care must be taken if cybersecurity is going to drive this control.				

SC-7	**BOUNDARY PROTECTION**				
	Control: The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [*Selection: physically; logically*] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	M	H
Difficulty w/Legacy	High				
Comments/ Rationale	Boundary Protection is a critical control that needs to be addressed appropriately. Some aspects of boundary protection are likely inherited from host platforms/networks. This control must be applied carefully in weapon systems to avoid driving unnecessary cost by requiring a boundary device at every antenna. Operational (e.g. latency) constraints must be considered as well.				

SC-7(1) – Withdrawn

SC-7(2) – Withdrawn

SC-7(3)	**BOUNDARY PROTECTION | *ACCESS POINTS***				
	The organization limits the number of external network connections to the information system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Access points should be dictated by operational threshold requirements for weapon systems rather than cybersecurity requirements. Any connections that do not have an operational driver (e.g. implemented for testing or convenience) should be removed. There may be access points that have a partial operational component that should be left as trade space for the program.				

SC-7(4)	**BOUNDARY PROTECTION | *EXTERNAL TELECOMMUNICATIONS SERVICES***				
	The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [*Assignment: organization-defined frequency*] and removes exceptions that are no longer supported by an explicit mission/business need.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not applicable to weapon systems. This would require offloading boundary protection responsibilities outside of DoD. Even in situations in which NAVAIR utilizes commercial satellite communications (SATCOM), NAVAIR bulk encrypts and manages the boundary protection natively on the weapon platform.				

SC-7(5)	**BOUNDARY PROTECTION | *DENY BY DEFAULT / ALLOW BY EXCEPTION***				
	The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Critical control; could also be implemented as a software firewall, even if no separate boundary device exists.				

SC-7(6) – Withdrawn

SC-7(7)	**BOUNDARY PROTECTION | *PREVENT SPLIT TUNNELING FOR REMOTE DEVICES***				
	The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	As a best practice, split tunneling should be avoided. Not a common design practice given weapon system architectures.				

SC-7(8)	**BOUNDARY PROTECTION | *ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS***				
	The information system routes [*Assignment: organization-defined internal communications traffic*] to [*Assignment: organization-defined external networks*] through authenticated proxy servers at managed interfaces.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	As a best practice, proxy servers should not be used in weapon systems.				

SC-7(9)	**BOUNDARY PROTECTION | *RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC***
	The information system:

	(a) Detects and denies outgoing communications traffic posing a threat to external information systems; and (b) Audits the identity of internal users associated with denied communications.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Good design principle. Should be part of NAVAIR's weapon system network situational awareness broader than this specific control. Unlikely weapon systems would have the connectivity to support typical DDOS style attacks from within.				

SC-7(10)	**BOUNDARY PROTECTION | *PREVENT UNAUTHORIZED EXFILTRATION***				
	The organization prevents the unauthorized exfiltration of information across managed interfaces.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Due to the critical nature of the data on weapon systems, must protect against exfiltration. Tactically useful data is the concern for exfiltration from the weapon system, not design data which could be ex-filtrated from other sources**.**				

SC-7(11)	**BOUNDARY PROTECTION | *RESTRICT INCOMING COMMUNICATIONS TRAFFIC***				
	The information system only allows incoming communications from [*Assignment: organization-defined authorized sources*] to be routed to [*Assignment: organization-defined authorized destinations*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Critical control; part of network situational awareness.				

SC-7(12)	**BOUNDARY PROTECTION | *HOST-BASED PROTECTION***

	The organization implements [*Assignment: organization-defined host-based boundary protection mechanisms*] at [*Assignment: organization-defined information system components*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	For enterprise systems, typically met by HBSS. HBSS' one-size fits all design has known limitations in weapon system architectures. Host level protection methods have value even when the HBSS solution is not valid.				

SC-7(13)	**BOUNDARY PROTECTION | *ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS***				
	The organization isolates [*Assignment: organization-defined information security tools, mechanisms, and support components*] from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	In most weapon systems, size, weight and power (SWaP) constraints make this impractical. Given protected access, low ROI.				

SC-7(14)	**BOUNDARY PROTECTION | *PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS***				
	The organization protects against unauthorized physical connections at [*Assignment: organization-defined managed interfaces*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	USB lockers, physical port lockers, and software based disabling all fit this control. Color coding of cables and jacks also falls into this. Critical control; NAVAIR has found it is not broadly followed. Spectrum of solutions and deployments need to be considered against operational requirements.				

SC-7(15)	SYSTE BOUNDARY PROTECTION | *ROUTE PRIVILEGED NETWORK ACCESSES*				
	The information system routes all networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	M	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Not typical weapon system architecture. More likely to appear on UAS Control Segments than any other context.				

SC-7(16)	BOUNDARY PROTECTION | *PREVENT DISCOVERY OF COMPONENTS / DEVICES*				
	The information system prevents discovery of specific system components composing a managed interface.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Unlikely NAVAIR could use this type of obfuscation. Difficult to implement. Likely low return on investment, given other protections on access.				

SC-7(17)	BOUNDARY PROTECTION | *AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS*				
	The information system enforces adherence to protocol formats.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Difficult to implement given typical weapon system designs. Low return on investment due to lack of available signatures for tailored attacks.				

SC-7(18)	BOUNDARY PROTECTION | *FAIL SECURE*
	The information system fails securely in the event of an operational failure of a boundary protection device.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Extreme care and due diligence must be taken with this control to avoid-operational issues. Should be left to program trade-space. Good practice to "fail secure", but should be driven by operational requirements. Battle short capabilities should not be the default, and should not be excluded by this control.				

SC-7(19)	**BOUNDARY PROTECTION | *BLOCKS COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS***				
	The information system blocks both inbound and outbound communications traffic between [*Assignment: organization-defined communication clients*] that are independently configured by end users and external service providers.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	For weapon systems, this is covered by whitelisting, configuration management, and firewall controls.				

SC-7(20)	**BOUNDARY PROTECTION | *DYNAMIC ISOLATION / SEGREGATION***				
	The information system provides the capability to dynamically isolate/segregate [*Assignment: organization-defined information system components*] from other components of the system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Weapon systems should avoid automated segmentation due to possibility of severe operational impacts.				

SC-7(21)	**BOUNDARY PROTECTION | *ISOLATION OF INFORMATION SYSTEM COMPONENTS***
	The organization employs boundary protection mechanisms to separate [*Assignment: organization-defined information system components*] supporting [*Assignment: organization-defined missions*

	and/or business functions].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	L	M
Difficulty w/Legacy	High				
Comments/ Rationale	Segmentation of functions, where possible, is a good design principle.				

SC-7(22)	**BOUNDARY PROTECTION | *SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS***				
	The information system implements separate network addresses (i.e., different subnets) to connect to systems in different security domains.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Classification requirements dictate separate networks, not subnets.				

SC-7(23)	**BOUNDARY PROTECTION | *DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE***				
	The information system disables feedback to senders on protocol format validation failure.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Low applicability to weapon systems due to architecture and typical install on classified networks.				

SC-8	**TRANSMISSION CONFIDENTIALITY AND INTEGRITY**
	Control: The information system protects the [*Selection (one or more): confidentiality; integrity*] of transmitted information.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Typically for weapon systems, this is addressed by COMSEC requirements for classified data. Needs to be accessed for all platforms. Platforms with no external communications would tailor out this control.				

SC-8(1)	**TRANSMISSION CONFIDENTIALITY AND INTEGRITY | *CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION***				
	The information system implements cryptographic mechanisms to [*Selection (one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-8(2)	**TRANSMISSION CONFIDENTIALITY AND INTEGRITY | *PRE / POST TRANSMISSION HANDLING***				
	The information system maintains the [*Selection (one or more): confidentiality; integrity*] of information during preparation for transmission and during reception.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Addressed by other controls on the handling of classified data for NAVAIR weapon systems.				

SC-8(3)	**TRANSMISSION CONFIDENTIALITY AND INTEGRITY | *CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS***
	The information system implements cryptographic mechanisms to protect message externals unless

	otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	This is required by Transmission Security (TRANSEC) for critical data going over public transmission media. This is the addition of black packet routing typically done pre/post bulk encryptors.				

SC-8(4)	**TRANSMISSION CONFIDENTIALITY AND INTEGRITY | *CONCEAL / RANDOMIZE COMMUNICATIONS***				
	The information system implements cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	The ability to randomize communications is nearly impossible to achieve in a weapon system; however, there is value in concealing data, especially from traffic analysis techniques.				

SC-9 – Withdrawn

SC-9(1) – Withdrawn

SC-9(2) – Withdrawn

SC-10	**NETWORK DISCONNECT**				
	Control: The information system terminates the network connection associated with a communications session at the end of the session or after [*Assignment: organization-defined time period*] of inactivity.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	M	L	M
Difficulty w/Legacy	Moderate				

Comments/ Rationale	Internal to aircraft connections do not need to be explicitly terminated. Mitigated by power cycling aircraft.

SC-11	**TRUSTED PATH**				
	Control: The information system establishes a trusted communications path between the user and the following security functions of the system: [*Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	M	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Aircraft have local authentication not centralized. Some application in UAS Control Segments. Possible usage in Support Equipment and Shipboard.				

SC-11(1)	**TRUSTED PATH | *LOGICAL ISOLATION***				
	The information system provides a trusted communications path that is logically isolated and distinguishable from other paths.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	M	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-12	**CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**				
	Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/	Crypto deployment and use is policy-mandated for all classified systems and unclassified weapon				

Rationale	systems. Key Management Plan fulfills the intent.

SC-12(1)	**CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | *AVAILABILITY***				
	The organization maintains availability of information in the event of the loss of cryptographic keys by users.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

SC-12(2)	**CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | *SYMMETRIC KEYS***				
	The organization produces, controls, and distributes symmetric cryptographic keys using [*Selection: NIST FIPS-compliant; NSA-approved*] key management technology and processes.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

SC-12(3)	**CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | *ASYMETRIC KEYS***				
	The organization produces, controls, and distributes asymmetric cryptographic keys using [*Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Refer to base control.				

SC-12(4) – Withdrawn

SC-12(5) – Withdrawn

SC-13	**CRYPTOGRAPHIC PROTECTION**				
	Control: The information system implements [*Assignment: organization-defined cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Crypto deployment and use is policy-mandated for all classified systems and unclassified weapon systems. Key Management Plan fulfills the intent.				

SC-13(1) – Withdrawn

SC-13(2) – Withdrawn

SC-13(3) – Withdrawn

SC-13(4) – Withdrawn

SC-14 – Withdrawn

SC-15	**COLLABORATIVE COMPUTING DEVICES**				
	Control: The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]; and b. Provides an explicit indication of use to users physically present at the devices.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Weapon systems will not have these types of collaboration systems.				

SC-15(1)	COLLABORATIVE COMPUTING DEVICES | *PHYSICAL DISCONNECT*				
	The information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

SC-15(2) – Withdrawn

SC-15(3)	COLLABORATIVE COMPUTING DEVICES | *DISABLING / REMOVAL IN SECURE WORK AREAS*				
	The organization disables or removes collaborative computing devices from [*Assignment: organization-defined information systems or information system components*] in [*Assignment: organization-defined secure work areas*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

SC-15(4)	COLLABORATIVE COMPUTING DEVICES | *EXPLICITLY INDICATE CURRENT PARTICIPANTS*				
	The information system provides an explicit indication of current participants in [*Assignment: organization-defined online meetings and teleconferences*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

SC-16	TRANSMISSION OF SECURITY ATTRIBUTES				
	Control: The information system associates [*Assignment: organization-defined security attributes*] with information exchanged between information systems and between system components.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Policy directed; deals with classification markings (or FOUO, PII). Technical execution of AC-16. Note: neither AC-16 nor SC-16 would be pulled in by CNSSI 1253. AC-16 would be captured by Classified Overlay, but SC-16 would not. Easy to miss association needed to get full security attribute capability.				

SC-16(1)	TRANSMISSION OF SECURITY ATTRIBUTES | *INTEGRITY VALIDATION*				
	The information system validates the integrity of transmitted security attributes.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Policy directed; deals with classification markings (or FOUO, PII). Technical execution of AC-16.				

SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES				
	Control: The organization issues public key certificates under an [*Assignment: organization-defined certificate policy*] or obtains public key certificates from an approved service provider.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	N/A	L	N/A	L
Difficulty w/Legacy	High				
Comments/ Rationale	Many weapon systems will not use PKI due to disconnected architectures. Applicable in cases in which a platform has SIPR or off-board NIPR connectivity.				

SC-18	MOBILE CODE				
	Control: The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Not applicable to weapon systems. Any external resources accessed would already be trusted.				

SC-18(1)	MOBILE CODE | *IDENTIFY UNACCEPTABLE CODE / TAKE CORRECTIVE ACTIONS*				
	The information system identifies [*Assignment: organization-defined unacceptable mobile code*] and takes [*Assignment: organization-defined corrective actions*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

SC-18(2)	MOBILE CODE | *ACQUISITION / DEVELOPMENT / USE*				
	The organization ensures the acquisition, development, and use of mobile code to be deployed in the information system meets [*Assignment: organization-defined mobile code requirements*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

SC-18(3)	MOBILE CODE | *PREVENT DOWNLOADING / EXECUTION*				
	The information system prevents the download and execution of [*Assignment: organization-defined unacceptable mobile code*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

SC-18(4)	MOBILE CODE | *PREVENT AUTOMATIC EXECUTION*				
	The information system prevents the automatic execution of mobile code in [*Assignment: organization-defined software applications*] and enforces [*Assignment: organization-defined actions*] prior to executing the code.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

SC-18(5)	MOBILE CODE | *ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS*				
	The organization allows execution of permitted mobile code only in confined virtual machine environments.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

SC-19	VOICE OVER INTERNET PROTOCOL

	Control: The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	L	M	N/A	L
Difficulty w/Legacy	Low				
Comments/ Rationale	For systems that have an operational requirement for VOIP this is valid; tailor out if no VOIP in system. VOIP usage restrictions should be tied to operational requirements.				

SC-20	**SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)**				
	Control: The information system: a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Most systems with external connections will be leveraging trusted DNS connections on ship/NIPR/SIPR, which would be inherited. In cases where a LAN- level DNS is being used (probably not a good idea), there needs to be some thought as to the manner in which it is implemented. Domain Name System Security Extensions (DNSSEC) deployment could be very powerful, but needs to be done at the DISA level to be effective.				

SC-20(1) – Withdrawn

SC-20(2)	**SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)| *DATA ORIGIN / INTEGRITY***				
	The information system provides data origin and integrity protection artifacts for internal name/address resolution queries.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded

					Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control. This is where DNSSEC would come in.				

SC-21	**SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)**				
	Control: The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Most systems with external connections will be leveraging trusted DNS connections on ship/NIPR/SIPR, which would be inherited. In cases in which a LAN level DNS is being used (not a good idea), there needs to be some thought on the manner in which it is implemented. DNSSEC deployment could be very powerful, but needs to be done at the DISA level to be effective.				

SC-21(1) – Withdrawn

SC-22	**ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE**				
	Control: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Most systems with external connections will be leveraging trusted DNS connections on ship/NIPR/SIPR and this would be inherited. In the cases in which a LAN level DNS is being used (not a good idea), there needs to be some thought on the manner in which it is implemented. DNSSEC deployment could be very powerful, but needs to be done at the DISA level to be effective.				

SC-23	SESSION AUTHENTICITY				
	Control: The information system protects the authenticity of communications sessions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Tunneling over TLS or other mechanisms is best practice.				

SC-23(1)	SESSION AUTHENTICITY | *INVALIDATE SESSION IDENTIFIERS AT LOGOUT*				
	The information system invalidates session identifiers upon user logout or other session termination.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Invalidating tickets after termination is best practice.				

SC-23(2) – Withdrawn

SC-23(3)	SESSION AUTHENTICITY | *UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION*				
	The information system generates a unique session identifier for each session with [*Assignment: organization-defined randomness requirements*] and recognizes only session identifiers that are system-generated.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Using random session ID's is best practice.				

SC-23(4) – Withdrawn

SC-23(5)	SESSION AUTHENTICITY | *ALLOWED CERTIFICATE AUTHORITIES*				
	The information system only allows the use of [*Assignment: organization-defined certificate authorities*] for verification of the establishment of protected sessions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	This control has limitations as PKI on disconnected systems. Weapon systems may benefit from using self-signed certificates for internal communication security, which would not meet this control. Should be allowed internally.				

SC-24	FAIL IN KNOWN STATE				
	Control: The information system fails to a [*Assignment: organization-defined known-state*] for [*Assignment: organization-defined types of failures*] preserving [*Assignment: organization-defined system state information*] in failure.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Failing to a known state is good practice; key for system stability and safety.				

SC-25	THIN NODES				
	Control: The organization employs [*Assignment: organization-defined information system components*] with minimal functionality and information storage.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	N/A	M	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Thin nodes can be useful; should be driven by architecture and operational needs.				

SC-26	HONEYPOTS

	Control: The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	This is not NAVAIR's core mission. Honeypots could potentially be used as intrusion sensors, but there is a lot of overhead associated with honeypot maintenance and deployment.				

SC-26(1) – Withdrawn

SC-27	**PLATFORM-INDEPENDENT APPLICATIONS**				
	Control: The information system includes: [*Assignment: organization-defined platform-independent applications*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	This is a business decision, not a cybersecurity function.				

SC-28	**PROTECTION OF INFORMATION AT REST**				
	Control: The information system protects the [*Selection (one or more): confidentiality; integrity*] of [*Assignment: organization-defined information at rest*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Data at Rest (DAR) protections need to be considered in system design. DoD mandated by policy for classified systems; DON mandated for all systems.				

SC-28(1)	**PROTECTION OF INFORMATION AT REST | *CRYPTOGRAPHIC PROTECTION***

	The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [*Assignment: organization-defined information*] on [*Assignment: organization-defined information system components*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-28(2)	**PROTECTION OF INFORMATION AT REST | *OFF-LINE STORAGE***				
	The organization removes from online storage and stores off-line in a secure location [*Assignment: organization-defined information*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Off line storage is often infeasible for weapon systems.				

SC-29	**HETEROGENEITY**				
	Control: The organization employs a diverse set of information technologies for [*Assignment: organization-defined information system components*] in the implementation of the information system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	The concept of heterogeneity has some validity, but it is very difficult and expensive to implement. Supportability and logistics challenges. It forces additional Sys Admin skills (different company) for consistent operation. Can lead to poorly configured systems. Linked to PL-8(2).				

SC-29(1)	**HETEROGENEITY | *VIRTUALIZATION TECHNIQUES***

	The organization employs virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-30	**CONCEALMENT AND MISDIRECTION**				
	Control: The organization employs [*Assignment: organization-defined concealment and misdirection techniques*] for [*Assignment: organization-defined information systems*] at [*Assignment: organization-defined time periods*] to confuse and mislead adversaries.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	N/A	L
Difficulty w/Legacy	High				
Comments/ Rationale	This control can be powerful, but incurs a large overhead in terms of configurations and deployment. In most cases, NAVAIR weapon systems will not tolerate the likely reliability hit.				

SC-30(1) – Withdrawn

SC-30(2)	**CONCEALMENT AND MISDIRECTION | *RANDOMNESS***				
	The organization employs [*Assignment: organization-defined techniques*] to introduce randomness into organizational operations and assets.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	N/A	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-30(3)	**CONCEALMENT AND MISDIRECTION | *CHANGE PROCESSING / STORAGE LOCATIONS***

	The organization changes the location of [*Assignment: organization-defined processing and/or storage*] [*Selection:* [*Assignment: organization-defined time frequency*]*; at random time intervals*]].].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Similar to an Alternate Processing Site, this concept is illogical for weapon systems.				

SC-30(4)	**CONCEALMENT AND MISDIRECTION | *MISLEADING INFORMATION***				
	The organization employs realistic, but misleading information in [*Assignment: organization-defined information system components*] with regard to its security state or posture.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	This is a dangerous practice in general and typically requires significant approvals for DoD. Needs to be avoided even if it looks cool.				

SC-30(5)	**CONCEALMENT AND MISDIRECTION | *CONCEALMENT OF SYSTEM COMPONENTS***				
	The organization employs [*Assignment: organization-defined techniques*] to hide or conceal [*Assignment: organization-defined information system components*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	See Base Control and SC-26 (honeypot discussion).				

SC-31	**COVERT CHANNEL ANALYSIS**
	Control: The organization: a. Performs a covert channel analysis to identify those aspects of communications within the information system that are potential avenues for covert [*Selection (one or more): storage;*

	timing] channels; and b. Estimates the maximum bandwidth of those channels.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Covert channels are difficult to find. This control requires hacker artisan skillset to actually have confidence that all covert channel possibilities have been determined.				

SC-31(1)	**COVERT CHANNEL ANALYSIS | *TEST COVERT CHANNELS FOR EXPLOITABILITY***				
	The organization tests a subset of the identified covert channels to determine which channels are exploitable.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-31(2)	**COVERT CHANNEL ANALYSIS | *MAXIMUM BANDWIDTH***				
	The organization reduces the maximum bandwidth for identified covert [*Selection (one or more); storage; timing*] channels to [*Assignment: organization-defined values*].].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-31(3)	**COVERT CHANNEL ANALYSIS | *MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS***
	The organization measures the bandwidth of [*Assignment: organization-defined subset of identified covert channels*] in the operational environment of the information system.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-32	**INFORMATION SYSTEM PARTITIONING**				
	Control: The organization partitions the information system into [*Assignment: organization-defined information system components*] residing in separate physical domains or environments based on [*Assignment: organization-defined circumstances for physical separation of components*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	N/A	L
Difficulty w/Legacy	High				
Comments/ Rationale	This is the physical separation of components typically by classification level (e.g. green/red separation). May be mandated by policy. Often not practical in weapon systems. Low ROI. Typically satisfied by PE-19(1).				

SC-33 – Withdrawn

SC-34	**NON-MODIFIABLE EXECUTABLE PROGRAMS**				
	Control: The information system at [*Assignment: organization-defined information system components*]: a. Loads and executes the operating environment from hardware-enforced, read-only media; and b. Loads and executes [*Assignment: organization-defined applications*] from hardware-enforced, read-only media.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	M	L
Difficulty w/Legacy	High				
Comments/ Rationale	Typically implemented as a Live Boot or Write Blocked OS. Can be useful for systems that are very static in configuration. Difficult to deploy widely.				

SC-34(1)	NON-MODIFIABLE EXECUTABLE PROGRAMS | *NO WRITABLE STORAGE*				
	The organization employs [*Assignment: organization-defined information system components*] with no writeable storage that is persistent across component restart or power on/off.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	M	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-34(2)	NON-MODIFIABLE EXECUTABLE PROGRAMS | *INTEGRITY PROTECTION / READ-ONLY MEDIA*				
	The organization protects the integrity of information prior to storage on read-only media and controls the media after such information has been recorded onto the media.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	M	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-34(3)	NON-MODIFIABLE EXECUTABLE PROGRAMS | *HARDWARE-BASED PROTECTION*				
	The organization: (a) Employs hardware-based, write-protect for [*Assignment: organization-defined information system firmware components*]; and (b) Implements specific procedures for [*Assignment: organization-defined authorized individuals*] to manually disable hardware write-protect for firmware modifications and re-enable the write-protect prior to returning to operational mode				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	M	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-35	HONEYCLIENTS				
	Control: The information system includes components that proactively seek to identify malicious websites and/or web-based malicious code.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Due to disconnected nature, not within NAVAIR's mission.				

SC-36	DISTRIBUTED PROCESSING AND STORAGE				
	Control: The organization distributes [*Assignment: organization-defined processing and storage*] across multiple physical locations.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Similar to an Alternate Processing Site, concept is illogical for weapon systems.				

SC-36(1)	DISTRIBUTED PROCESSING AND STORAGE | *POLLING TECHNIQUES*				
	The organization employs polling techniques to identify potential faults, errors, or compromises to [*Assignment: organization-defined distributed processing and storage components*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

SC-37	OUT-OF-BAND CHANNELS

	Control: The organization employs [*Assignment: organization-defined out-of-band channels*] for the physical delivery or electronic transmission of [*Assignment: organization-defined information, information system components, or devices*] to [*Assignment: organization-defined individuals or information systems*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Critical improvement for out of band hashing of software loads when digital signatures are not possible. Typically digital signatures are preferred, but operational limitations could exist to drive toward out of band.				

SC-37(1)	**OUT-OF-BAND CHANNELS | *ENSURE DELIVERY / TRANSMISSION***				
	The organization employs [*Assignment: organization-defined security safeguards*] to ensure that only [*Assignment: organization-defined individuals or information systems*] receive the [*Assignment: organization-defined information, information system components, or devices*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-38	**OPERATION SECURITY**				
	Control: The organization employs [*Assignment: organization-defined operations security safeguards*] to protect key organizational information throughout the system development life cycle.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by policy and operational procedures. Refer to Physical and Environmental/Personal Security (PE/PS) and similar controls. OPSEC in DoD acquisition currently mandated, but could be better employed.				

SC-39	PROCESS ISOLATION				
	Control: The information system maintains a separate execution domain for each executing process.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Implemented by default in most modern operating systems with process specific memory access pages. Many embedded systems will not support process separation. Good practice if applicable, should avoid driving costs and requirements.				

SC-39(1)	PROCESS ISOLATION | *HARDWARE SEPARATION*				
	The information system implements underlying hardware separation mechanisms to facilitate process separation.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Hardware separation is likely very expensive in weapon systems.				

SC-39(2)	PROCESS ISOLATION | *THREAD ISOLATION*				
	The information system maintains a separate execution domain for each thread in [*Assignment: organization-defined multi-threaded processing*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-40	WIRELESS LINK PROTECTION

	Control: The information system protects external and internal [*Assignment: organization-defined wireless links*] from [*Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Some validity in this control, but most of this will be driven by operational / performance requirements (e.g. anti-jam needs) rather than cybersecurity. Care must be taken to not unduly drive cost. Many tactical data links will implement these for Transmission Security/Communications Security (TRANSEC/COMSEC) reasons that could be inherited.				

SC-40(1)	**WIRELESS LINK PROTECTION | *ELECTROMAGNETIC INTERFERENCE***				
	The information system implements cryptographic mechanisms that achieve [*Assignment: organization-defined level of protection*] against the effects of intentional electromagnetic interference.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-40(2)	**WIRELESS LINK PROTECTION | *REDUCE DETECTION POTENTIAL***				
	The information system implements cryptographic mechanisms to reduce the detection potential of wireless links to [*Assignment: organization-defined level of reduction*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-40(3)	**WIRELESS LINK PROTECTION | *IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION***

	The information system implements cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-40(4)	**WIRELESS LINK PROTECTION | *SIGNAL PARAMETER IDENTIFICATION***				
	The information system implements cryptographic mechanisms to prevent the identification of [*Assignment: organization-defined wireless transmitters*] by using the transmitter signal parameters.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-41	**PORT AND I/O DEVICE ACCESS**				
	Control: The organization physically disables or removes [*Assignment: organization-defined connection ports or input/output devices*] on [*Assignment: organization-defined information systems or information system components*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	USB lockers, physical port lockers, and software based (BIOS) disabling all fit this control. Related to SC-7(14).				

SC-42	**SENSOR CAPABILITY AND DATA**

	Control: The information system: a. Prohibits the remote activation of environmental sensing capabilities with the following exceptions: [*Assignment: organization-defined exceptions where remote activation of sensors is allowed*]; and b. Provides an explicit indication of sensor use to [*Assignment: organization-defined class of users*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Note: this control would only apply to weapon systems that contain mobile devices (e.g., tablet). Systems utilizing mobile devices should address this through the STIGS or configuration settings.				

SC-42(1)	**SENSOR CAPABILITY AND DATA | *REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES***				
	The organization ensures the information system is configured so data or information collected by the [*Assignment: organization-defined sensors*] is only reported to authorized individuals or roles.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-42(2)	**SENSOR CAPABILITY AND DATA | *AUTHORIZED USE***				
	The organization employs the following measures: [*Assignment: organization-defined measures*], so that data or information collected by [*Assignment: organization-defined sensors*] is only used for authorized purposes.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-42(3)	SENSOR CAPABILITY AND DATA | *PROHIBIT USE OF DEVICES*				
	The organization prohibits the use of devices possessing [*Assignment: organization-defined environmental sensing capabilities*] in [*Assignment: organization-defined facilities, areas, or systems*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SC-43	USAGE RESTRICTIONS				
	Control: The organization: a. Establishes usage restrictions and implementation guidance for [*Assignment: organization-defined information system components*] based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of such components within the information system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Covered by other controls (e.g. SC-7, CM-6, user training). No value added.				

SC-44	DETONATION CHAMBERS				
	Control: The organization employs a detonation chamber capability within [*Assignment: organization-defined information system, system component, or location*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Due to disconnected nature of weapon systems and associated overhead, this is not a useful control.				

SYSTEM AND INFORMATION INTEGRITY

SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES				
	Control: The organization: a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and b. Reviews and updates the current: 1. System and information integrity policy [*Assignment: organization-defined frequency*]; and 2. System and information integrity procedures [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	**Tier I (satisfied by existing DoD policy and guidance)** All -1 are Medium; covered by policy.				

SI-2	FLAW REMEDIATION				
	Control: The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Critical to have a flaw remediation strategy. Needs to be tailored to aviation and weapon system timelines and updates.				

SI-2(1)	FLAW REMEDIATION | *CENTRAL MANAGEMENT*				
	The organization centrally manages the flaw remediation process.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C	Applicable Unmanned A/C	Applicable Support	Applicable Shipboard

		Vehicle	Control Station	Equipment	Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	As long as the PMA is in charge of the flaw remediation and fulfills central management, this is a solid practice. Needs to include appropriate regression testing.				

SI-2(2)	**FLAW REMEDIATION | *AUTOMATED FLAW REMEDIATION STATUS***				
	The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to determine the state of information system components with regard to flaw remediation.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Automated systems not necessary due to solid configuration management of the weapon systems and software loads.				

SI-2(3)	**FLAW REMEDIATION | *TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS***				
	The organization: (a) Measures the time between flaw identification and flaw remediation; and (b) Establishes [*Assignment: organization-defined benchmarks*] for taking corrective actions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Good practice to measure remediation, but timelines should be expected to be longer than enterprise patch management situations. Also important to know what conditions trigger additional timeline requirements (e.g. periodic software updates vs. ECP).				

SI-2(4) – Withdrawn

SI-2(5)	**FLAW REMEDIATION | *AUTOMATIC SOFTWARE / FIRMWARE UPDATES***				
	The organization installs [*Assignment: organization-defined security-relevant software and firmware updates*] automatically to [*Assignment: organization-defined information system components*].				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	N/A	N/A	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Typically automated update mechanisms should be tailored out for safety critical and mission critical systems. Updates should be locked in configuration management processes. There are some cases in which this might be applicable, but should generally be avoided.				

SI-2(6)	**FLAW REMEDIATION | *REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE / FIRMWARE***				
	The organization removes [*Assignment: organization-defined software and firmware components*] after updated versions have been installed.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Good practice. NAVAIR's typical method for updating software loads fulfills this. May need to be enforced at the build level.				

SI-3	**MALICIOUS CODE PROTECTION**				
	Control: The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the information system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources at [*Selection (one or more); endpoint; network entry/exit points*] as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator;* [*Assignment: organization-defined action*]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty	High				

w/Legacy	
Comments/ Rationale	Due to operational limitations, this is typically not a valuable control. Primarily addressed by interface data validation, good configuration management on software loads, and mitigated by limited connectivity at the user level. Signature based detection is of limited value against NAVAIR threat models.

SI-3(1)	**MALICIOUS CODE PROTECTION | *CENTRAL MANAGEMENT***				
	The organization centrally manages malicious code protection mechanisms.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SI-3(2)	**MALICIOUS CODE PROTECTION | *AUTOMATIC UPDATES***				
	The information system automatically updates malicious code protection mechanisms.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SI-3(3) – Withdrawn

SI-3(4)	**MALICIOUS CODE PROTECTION | *UPDATES ONLY BY PRIVILEGED USERS***				
	The information system updates malicious code protection mechanisms only when directed by a privileged user.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty	High				

w/Legacy	
Comments/ Rationale	Refer to base control.

SI-3(5) – Withdrawn

SI-3(6)	**MALICIOUS CODE PROTECTION | *TESTING / VERIFICATION***				
	The organization: (a) Tests malicious code protection mechanisms [*Assignment: organization-defined frequency*] by introducing a known benign, non-spreading test case into the information system; and (b) Verifies that both detection of the test case and associated incident reporting occur.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SI-3(7)	**MALICIOUS CODE PROTECTION | *NON-SIGNATURE-BASED DETECTION***				
	The information system implements non-signature-based malicious code detection mechanisms.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Non-signature based detection much more useful in defending NAVAIR systems. Lack of solutions that work in embedded systems.				

SI-3(8)	**MALICIOUS CODE PROTECTION | *DETECT UNAUTHORIZED COMMANDS***				
	The information system detects [*Assignment: organization-defined unauthorized operating system commands*] through the kernel application programming interface at [*Assignment: organization-defined information system hardware components*] and [*Selection (one or more): issues a warning; audits the command execution; prevents the execution of the command*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems

	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Could be difficult to implement this control. Better to address through robust application of least privilege and access control. Some cases could exist where this would be useful.				

SI-3(9)	**MALICIOUS CODE PROTECTION | *AUTHENTICATE REMOTE COMMANDS***				
	The information system implements [*Assignment: organization-defined security safeguards*] to authenticate [*Assignment: organization-defined remote commands*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Most weapon systems will not have remote commands and this should be tailored out. If the system does have such commands, control should be included.				

SI-3(10)	**MALICIOUS CODE PROTECTION | *MALICIOUS CODE ANALYSIS***				
	The organization: (a) Employs [*Assignment: organization-defined tools and techniques*] to analyze the characteristics and behavior of malicious code; and (b) Incorporates the results from malicious code analysis into organizational incident response and flaw remediation processes.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	For weapon systems, the platform owners should not be trying to perform malware analysis. There are other groups (such as NAVAIR Cyber Incident Response Team (CIRT) and IC) that perform this function based on national security requirements.				

SI-4	**INFORMATION SYSTEM MONITORING**
	<u>Control</u>: The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [*Assignment: organization-defined monitoring objectives*]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [*Assignment: organization-defined*

	techniques and methods]; c. Deploys monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides [*Assignment: organization-defined information system monitoring information*] to [*Assignment: organization-defined personnel or roles*] [*Selection (one or more): as needed;* [*Assignment: organization-defined frequency*]].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Having good situational awareness on the system is critical. Typically this is fulfilled by HBSS; HBSS' one-size fits all design has known limitations weapon system architectures. Still a key requirement for cyber resiliency.				

SI-4(1)	**INFORMATION SYSTEM MONITORING | *SYSTEM-WIDE INTRUSION DETECTION SYSTEM***				
	The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	System, in this case, needs to be well defined. NAVAIR wants to see platform-wide situational awareness on data traffic. Will need to be tailored to weapon system usage and balanced with operational constraints.				

SI-4(2)	**INFORMATION SYSTEM MONITORING | *AUTOMATED TOOLS FOR REAL-TIME ANALYSIS***				
	The organization employs automated tools to support near real-time analysis of events.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C	Applicable Unmanned A/C	Applicable Support	Applicable Shipboard

		Vehicle	Control Station	Equipment	Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Good practice. Unclear if all weapon system solutions would meet intent of real-time analysis. Any reasonable solution would likely have an automated notification component, but personnel available to respond may not be immediately available.				

SI-4(3)	**INFORMATION SYSTEM MONITORING | *AUTOMATED TOOL INTEGRATION***				
	The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Must be balanced with operational constraints.				

SI-4(4)	**INFORMATION SYSTEM MONITORING | *INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC***				
	The information system monitors inbound and outbound communications traffic [*Assignment: organization-defined frequency*] for unusual or unauthorized activities or conditions.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Monitoring inbound/outbound traffic is key. Unlikely signature based methods will work, but detecting malformed data should meet the intent of this control. Must be balanced with latency and operational constraints.				

SI-4(5)	**INFORMATION SYSTEM MONITORING | *SYSTEM-GENERATED ALERTS***
	The information system alerts [*Assignment: organization-defined personnel or roles*] when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined compromise indicators*].

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Good practice to notify operators. Operators need to be trained on what actions to take. Control language does not explicitly state this has to notify operator. Might be meet by logging and notifying maintenance personnel.				

SI-4(6) – Withdrawn

SI-4(7)	**INFORMATION SYSTEM MONITORING | *AUTOMATED RESPONSE TO SUSPICIOUS EVENTS***				
	The information system notifies [*Assignment: organization-defined incident response personnel (identified by name and/or by role)*] of detected suspicious events and takes [*Assignment: organization-defined least-disruptive actions to terminate suspicious events*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Care must be taken on this control. Typically, NAVAIR does not want a weapon system to take automated actions except in some corner cases. Recommend notification/human input level for safety/mission critical systems.				

SI-4(8) – Withdrawn

SI-4(9)	**INFORMATION SYSTEM MONITORING | *TESTING OF MONITORING TOOLS***				
	The organization tests intrusion-monitoring tools [*Assignment: organization-defined frequency*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	General principle to test anything installed in the system. This is often done for IDS by sending known malicious traffic through. Care must be taken not to allow this control to create an attack surface opening. If done, should be performed in DT environment.				

SI-4(10)	INFORMATION SYSTEM MONITORING | *VISIBILITY OF ENCRYPTED COMMUNICATIONS*				
	The organization makes provisions so that [*Assignment: organization-defined encrypted communications traffic*] is visible to [*Assignment: organization-defined information system monitoring tools*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	NAVAIR weapon systems will not sit behind an external Computer Network Defense (CND) site or border gateway that needs to inspect encrypted communications.				

SI-4(11)	INFORMATION SYSTEM MONITORING | *ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES*				
	The organization analyzes outbound communications traffic at the external boundary of the information system and selected [*Assignment: organization-defined interior points within the system (e.g., subnetworks, subsystems)*] to discover anomalies.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	In general this is good practice, but not always feasible due to operational constraints. Requires high confidence on detecting abnormalities.				

SI-4(12)	INFORMATION SYSTEM MONITORING | *AUTOMATED ALERTS*				
	The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined activities that trigger alerts*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Good practice. Alerts need to be throttled and operators trained on how to respond.				

SI-4(13)	INFORMATION SYSTEM MONITORING | *ANALYZE TRAFFIC / EVENT PATTERNS*				
	The organization: (a) Analyzes communications traffic/event patterns for the information system; (b) Develops profiles representing common traffic patterns and/or events; and (c) Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	In general this is good practice, but not always feasible due to operational constraints. Requires high confidence on detecting abnormalities.				

SI-4(14)	INFORMATION SYSTEM MONITORING | *WIRELESS INTRUSION DETECTION*				
	The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Unless IEEE 802.11 technologies are being used, this is not applicable and covered by TEMPEST.				

SI-4(15)	INFORMATION SYSTEM MONITORING | *WIRELESS TO WIRELINE COMMUNICATIONS*				
	The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Unless IEEE 802.11 technologies are being used, this is not applicable and covered by TEMPEST.				

SI-4(16)	INFORMATION SYSTEM MONITORING | *CORRELATE MONITORING INFORMATION*				
	The organization correlates information from monitoring tools employed throughout the information system.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	The disconnected nature of most weapon systems makes this control low value.				

SI-4(17)	INFORMATION SYSTEM MONITORING | *INTEGRATED SITUATIONAL AWARENESS*				
	The organization correlates information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Good practice, but could be huge cost driver. Care needs to be taken to apply at the right levels. NAVAIR CIRT or Intelligence Community (IC) would address investigatory components.				

SI-4(18)	INFORMATION SYSTEM MONITORING | *ANALYZE TRAFFIC / COVERT EXFILTRATION*				
	The organization analyzes outbound communications traffic at the external boundary of the information system (i.e., system perimeter) and at [*Assignment: organization-defined interior points within the system (e.g., subsystems, subnetworks)*] to detect covert exfiltration of information.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Covert channels are difficult to find. This control requires hacker artisan skillsets to actually have confidence all covert channel possibilities have been determined. Closely tied to SC-31.				

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

	The organization implements [*Assignment: organization-defined additional monitoring*] of individuals who have been identified by [*Assignment: organization-defined sources*] as posing an increased level of risk.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Covered by security clearance and other personnel screening requirements.				

SI-4(20)	**INFORMATION SYSTEM MONITORING | *PRIVILEGED USERS***				
	The organization implements [*Assignment: organization-defined additional monitoring*] of privileged users.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Moderate				
Comments/ Rationale	Good practice.				

SI-4(21)	**INFORMATION SYSTEM MONITORING | *PROBATIONARY PERIODS***				
	The organization implements [*Assignment: organization-defined additional monitoring*] of individuals during [*Assignment: organization-defined probationary period*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Low value due to personnel screening and clearance processes. Covered effectively by interim clearance process during indoctrination and training. NAVAIR does not want to imply a probationary period when a new member shows up to a ship or squadron.				

SI-4(22)	**INFORMATION SYSTEM MONITORING | *UNAUTHORIZED NETWORK SERVICES***
	The information system detects network services that have not been authorized or approved by

	[*Assignment: organization-defined authorization or approval processes*] and [*Selection (one or more): audits; alerts* [*Assignment: organization-defined personnel or roles*]].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Good practice. Need a plan if discovered.				

SI-4(23)	**INFORMATION SYSTEM MONITORING | *HOST-BASED DEVICES***				
	The organization implements [*Assignment: organization-defined host-based monitoring mechanisms*] at [*Assignment: organization-defined information system components*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Typically this is fulfilled by HBSS; HBSS' one-size fits all design has known limitations weapon system architectures, but this level of situational awareness is important for cyber resiliency.				

SI-4(24)	**INFORMATION SYSTEM MONITORING | *INDICATORS OF COMPROMISE***				
	The information system discovers, collects, distributes, and uses indicators of compromise.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Good practice. Unclear why this is not captured in Audit controls. The scope of a sensor may be limited due to weapon system configurations.				

SI-5	**SECURITY ALERTS, ADVISORIES, AND DIRECTIVES**
	Control: The organization: a. Receives information system security alerts, advisories, and directives from [*Assignment: organization-defined external organizations*] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary;

	c. Disseminates security alerts, advisories, and directives to: [*Selection (one or more):* [*Assignment: organization-defined personnel or roles*]; [*Assignment: organization-defined elements within the organization*]; [*Assignment: organization-defined external organizations*]]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	This control should be split into two parts. There is a lot of value in ensuring the PMA is connected to the right data sources for emerging threats. This level of alerts should not be auto-pushed to the operational community; rather the PMA should have mechanism to push alerts and directives when needed.				

SI-5(1)	**SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | *AUTOMATED ALERTS AND ADVISORIES***				
	The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Alerts may be manual in weapon systems and still be acceptable.				

SI-6	**SECURITY FUNCTION VERIFICATION**				
	Control: The organization: a. Verifies the correct operation of [*Assignment: organization-defined security functions*]; b. Performs this verification [*Selection (one or more):* [*Assignment: organization-defined system transitional states*]*; upon command by user with appropriate privilege;* [*Assignment: organization-defined frequency*]]; c. Notifies [*Assignment: organization-defined personnel or roles*] of failed security verification tests; and d. [*Selection (one or more): shuts the information system down; restarts the information system;* [*Assignment: organization-defined alternative action(s)*]] when anomalies are discovered.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems

	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Verification of security functions low value, as NAVAIR has solid configuration management controls.				

SI-6(1) – Withdrawn

SI-6(2)	**SECURITY FUNCTION VERIFICATION | *AUTOMATION SUPPORT FOR DISTRIBUTED TESTING***				
	The information system implements automated mechanisms to support the management of distributed security testing.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Automated systems not necessary due to solid configuration management of the weapon systems and software loads.				

SI-6(3)	**SECURITY FUNCTION VERIFICATION | *REPORT VERIFICATION RESULTS***				
	The organization reports the results of security function verification to [*Assignment: organization-defined personnel or roles*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SI-7	**SOFTWARE, FIRMWARE AND INFORMATION INTEGRITY**				
	Control: The organization employs integrity verification tools to detect unauthorized changes to [*Assignment: organization-defined software, firmware, and information*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems

	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	This control is absolutely critical.				

SI-7(1)	**SOFTWARE, FIRMWARE AND INFORMATION INTEGRITY | *INTEGRITY CHECKS***				
	The information system performs an integrity check of [*Assignment: organization-defined software, firmware, and information*] [*Selection (one or more):* at startup; at [*Assignment: organization-defined transitional states or security-relevant events*]; [*Assignment: organization-defined frequency*]].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SI-7(2)	**SOFTWARE, FIRMWARE AND INFORMATION INTEGRITY | *AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS***				
	The organization employs automated tools that provide notification to [*Assignment: organization-defined personnel or roles*] upon discovering discrepancies during integrity verification.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SI-7(3)	**SOFTWARE, FIRMWARE AND INFORMATION INTEGRITY | *CENTRALLY-MANAGED INTEGRITY TOOLS***				
	The organization employs centrally managed integrity verification tools.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H

Difficulty w/Legacy	High
Comments/ Rationale	Refer to base control.

SI-7(4) – Withdrawn

SI-7(5)	**SYSTEM SOFTWARE, FIRMWARE AND INFORMATION INTEGRITY | *AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS***				
	The information system automatically [*Selection (one or more): shuts the information system down; restarts the information system; implements* [*Assignment: organization-defined security safeguards*]] when integrity violations are discovered.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Less value in automated responses; in most cases NAVAIR avoids automated actions.				

SI-7(6)	**SOFTWARE, FIRMWARE AND INFORMATION INTEGRITY | *CRYPTOGRAPHIC PROTECTION***				
	The information system implements cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SI-7(7)	**SOFTWARE, FIRMWARE AND INFORMATION INTEGRITY | *INTEGRATION OF DETECTION AND RESPONSE***				
	The organization incorporates the detection of unauthorized [*Assignment: organization-defined security-relevant changes to the information system*] into the organizational incident response capability.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C	Applicable Unmanned A/C	Applicable Support	Applicable Shipboard

		Vehicle	Control Station	Equipment	Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SI-7(8)	**SOFTWARE, FIRMWARE AND INFORMATION INTEGRITY | *AUDITING CAPABILITY FOR SIGNIFICANT EVENTS***				
	The information system, upon detection of a potential integrity violation, provides the capability to audit the event and initiates the following actions: [*Selection (one or more): generates an audit record; alerts current user; alerts* [*Assignment: organization-defined personnel or roles*]; [*Assignment: organization-defined other actions*]].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SI-7(9)	**SOFTWARE, FIRMWARE AND INFORMATION INTEGRITY | *VERIFY BOOT PROCESS***				
	The information system verifies the integrity of the boot process of [*Assignment: organization-defined devices*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Due to unique weapon system components and configurations, this may be very difficult to achieve.				

SI-7(10)	**SOFTWARE, FIRMWARE AND INFORMATION INTEGRITY | *PROTECTION OF BOOT FIRMWARE***				
	The information system implements [*Assignment: organization-defined security safeguards*] to protect the integrity of boot firmware in [*Assignment: organization-defined devices*].				
Rating	Applicable	Applicable	Applicable	Applicable	Applicable

	Manned A/C	Unmanned A/C Vehicle	Unmanned A/C Control Station	Support Equipment	Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Due to unique weapon system components and configurations this may be very difficult to achieve.				

SI-7(11)	**SOFTWARE, FIRMWARE AND INFORMATION INTEGRITY | *CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES***				
	The organization requires that [*Assignment: organization-defined user-installed software*] execute in a confined physical or virtual machine environment with limited privileges.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Less value in VM isolation due to limited use of weapon systems.				

SI-7(12)	**SOFTWARE, FIRMWARE AND INFORMATION INTEGRITY | *INTEGRITY VERIFICATION***				
	The organization requires the integrity of [*Assignment: organization-defined user-installed software*] be verified prior to execution.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SI-7(13)	**SOFTWARE, FIRMWARE AND INFORMATION INTEGRITY | *CODE EXECUTION IN PROTECTED ENVIRONMENTS***
	The organization allows execution of binary or machine-executable code obtained from sources with limited or no warranty and without the provision of source code only in confined physical or virtual machine environments and with the explicit approval of [*Assignment: organization-defined personnel or roles*].

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	This would be sandboxing software of unknown pedigree (SOUP). Good practice, but not always achievable.				

SI-7(14)	**SOFTWARE, FIRMWARE AND INFORMATION INTEGRITY | *BINARY OR MACHINE EXECUTABLE CODE***				
	The organization: (a) Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and (b) Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Good practice, but overlaps with data rights trade-space and could be a huge cost driver**.**				

SI-7(15)	**SOFTWARE, FIRMWARE AND INFORMATION INTEGRITY | *CODE AUTHENTICATION***				
	The information system implements cryptographic mechanisms to authenticate [*Assignment: organization-defined software or firmware components*] prior to installation.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SI-7(16)	**SOFTWARE, FIRMWARE AND INFORMATION INTEGRITY | *TIME LIMIT ON PROCESS EXECUTION W/O SUPERVISION***
	The organization does not allow processes to execute without supervision for more than [*Assignment:*

	organization-defined time period].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Lower value. Could be integrated into a system situational awareness (SA) scheme effectively, but any automated responses would need to be limited to avoid degrading operations.				

SI-8	**SPAM PROTECTION**				
	Control: The organization: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	SPAM is not a concern for weapon systems.				

SI-8(1)	**SPAM PROTECTION | *CENTRAL MANAGEMENT***				
	The organization centrally manages spam protection mechanisms.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

SI-8(2)	**SPAM PROTECTION | *AUTOMATIC UPDATES***
	The information system automatically updates spam protection mechanisms.

Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

SI-8(3)	**SPAM PROTECTION | *CONTINUOUS LEARNING CAPABILITY***				
	The information system implements spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

SI-9 - Withdrawn

SI-10	**INFORMATION INPUT VALIDATION**				
	Control: The information system checks the validity of [*Assignment: organization-defined information inputs*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Absolutely critical to validate data at key interfaces.				

SI-10(1)	**INFORMATION INPUT VALIDATION | *MANUAL OVERRIDE CAPABILITY***
	The information system: (a) Provides a manual override capability for input validation of [*Assignment: organization-defined*

	inputs]; (b) Restricts the use of the manual override capability to only [*Assignment: organization-defined authorized individuals*]; and (c) Audits the use of the manual override capability.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	For weapon systems, NAVAIR must have a manual override and be able to operate at risk (Battle Short). Needs to be well monitored to avoid abuse.				

SI-10(2)	**INFORMATION INPUT VALIDATION | *REVIEW / RESOLUTION OF ERRORS***				
	The organization ensures input validation errors are reviewed and resolved within [*Assignment: organization-defined time period*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Based on transaction-based system. Not applicable to weapon systems.				

SI-10(3)	**INFORMATION INPUT VALIDATION | *PREDICTABLE BEHAVIOR***				
	The information system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	This is critical for any input validation scheme. Should not be tailored out.				

SI-10(4)	**INFORMATION INPUT VALIDATION | *REVIEW / TIMING INTERACTIONS***
	The organization accounts for timing interactions among information system components in

	determining appropriate responses for invalid inputs.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	L	L	L	L	L
Difficulty w/Legacy	High				
Comments/ Rationale	Overly enterprise centric. Unlikely to have operator bandwidth to deal with data. Low likelihood of finding anything useful.				

SI-10(5)	**INFORMATION INPUT VALIDATION | *REVIEW / RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS***				
	The organization restricts the use of information inputs to [*Assignment: organization-defined trusted sources*] and/or [*Assignment: organization-defined formats*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Absolutely critical to validate data at key interfaces and have trusted sources for data going into weapon systems.				

SI-11	**ERROR HANDLING**				
	Control: The information system: a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [*Assignment: organization-defined personnel or roles*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Good practice. Should be part of an integrated user interface strategy.				

SI-12	**INFORMATION HANDLING AND RETENTION**

	Control: The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	Low				
Comments/ Rationale	Part of security classification process and policies.				

SI-13	**PREDICTABLE FAILURE PREVENTION**				
	Control: The organization: a. Determines mean time to failure (MTTF) for [*Assignment: organization-defined information system components*] in specific environments of operation; and b. Provides substitute information system components and a means to exchange active and standby components at [*Assignment: organization-defined MTTF substitution criteria*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	System reliability should be driven by operational availability (A_O) Key Performance Parameters (KPP). This does not bring enhanced cyber resiliency. For non DoD systems, such as a commercial data center, this control might force some to address reliability from an availability aspect. Should not be applicable to NAVAIR systems.				

SI-13(1)	**PREDICTABLE FAILURE PREVENTION | *TRANSFERRING COMPONENT RESPONSIBILITIES***				
	The organization takes information system components out of service by transferring component responsibilities to substitute components no later than [*Assignment: organization-defined fraction or percentage*] of mean time to failure.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

SI-13(2) – Withdrawn

SI-13(3)	**PREDICTABLE FAILURE PREVENTION | *MANUAL TRANSFER BETWEEN COMPONENTS***				
	The organization manually initiates transfers between active and standby information system components [*Assignment: organization-defined frequency*] if the mean time to failure exceeds [*Assignment: organization-defined time period*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

SI-13(4)	**PREDICTABLE FAILURE PREVENTION | *STANDBY COMPONENT INSTALLATION / NOTIFICATION***				
	The organization, if information system component failures are detected: (a) Ensures that the standby components are successfully and transparently installed within [*Assignment: organization-defined time period*]; and (b) [*Selection (one or more): activates* [*Assignment: organization-defined alarm*]; *automatically shuts down the information system*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				
Comments/ Rationale	Refer to base control.				

SI-13(5)	**PREDICTABLE FAILURE PREVENTION | *FAILOVER CAPABILITY***				
	The organization provides [*Selection: real-time; near real-time*] [*Assignment: organization-defined failover capability*] *for the information system*.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty	N/A				

w/Legacy	
Comments/ Rationale	Refer to base control.

SI-14	**NON-PERSISTENCE**				
	Control: The organization implements non-persistent [*Assignment: organization-defined information system components and services*] that are initiated in a known state and terminated [*Selection (one or more): upon end of session of use; periodically at* [*Assignment: organization-defined frequency*]].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Good practice if viable for a weapon system.				

SI-14(1)	**NON-PERSISTENCE | *REFRESH FROM TRUSTED SOURCES***				
	The organization ensures software and data employed during information system component and service refreshes are obtained from [*Assignment: organization-defined trusted sources*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Refer to base control.				

SI-15	**INFORMATION OUTPUT FILTERING**				
	Control: The information system validates information output from [*Assignment: organization-defined software programs and/or applications*] to ensure that the information is consistent with the expected content.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	N/A	N/A	N/A	N/A	N/A
Difficulty w/Legacy	N/A				

Comments/ Rationale	Not applicable to weapon systems. Valid for internet facing webpages.

SI-16	**MEMORY PROTECTION**				
	Control: The information system implements [*Assignment: organization-defined security safeguards*] to protect its memory from unauthorized code execution.				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	M	M	M	M	M
Difficulty w/Legacy	High				
Comments/ Rationale	Modern operating systems will usually address this through data execution prevention (DEP) and Address Space Layout Randomization (ASLR). Many Real-Time Operating Systems (RTOS) and legacy systems will not support. Should be activated where available, but should not be a cost driver.				

SI-17	**FAIL-SAFE PROCEDURES**				
	Control: The information system implements [*Assignment: organization-defined fail-safe procedures*] when [*Assignment: organization-defined failure conditions occur*].				
Rating	Applicable Manned A/C	Applicable Unmanned A/C Vehicle	Applicable Unmanned A/C Control Station	Applicable Support Equipment	Applicable Shipboard Embedded Systems
	H	H	H	H	H
Difficulty w/Legacy	High				
Comments/ Rationale	Key to have controllable failure states. Must be able to fight through attack.				

APPENDIX 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

CODE	CONTROL FAMILY
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PM	Program Management
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
PM	Program Management

APPENDIX 2: ACRONYMS

ACAS	Assured Compliance Assessment Solution
ADMACS	Aviation Data Management and Control System
A_O	Operational Availability
ASIC	Application-Specific Integrated Circuits
ASLR	Address Space Layout Randomization
CCA	Control Applicability Assessment
CCI	Control Correlation Identifier
CDS	Cross-Domain Solution
CIRT	NAVAIR Computer Incident Response Team
CND	Computer Network Defense
CRA	Cyber Risk Assessment
CTT	Cyber Tabletop
CUI	Controlled Unclassified Information
DAR	Data at Rest
DDOS	Distributed Denial of Service
DEP	Data Execution Prevention
DHCP	Dynamic Host Configuration Protocol
DFIA	Defense-in-Depth Functional Implementation Architecture
DNSSEC	Domain Name System Security Extensions
DT/OT	Developmental Test / Operational Test
EKB	Electronic Kneeboard
EMP	Electromagnetic Pulse
E-STOP	Emergency Stop Switches
FAO	Functional Authorizing Official
FOUO	For Official Use Only
FSCA	Functional Security Control Assessor
GMT	General Military Training | Greenwich Mean Time

HBSS	Host Based Security System
NACMS OS	High Assurance Cyber Military Systems-Operating System
HIL	Hardware in the Loop
KPP	Key Performance Parameters
LSI	Lead System Integrator
NIAP	National Information Assurance Partnership
NALCOMIS	Naval Aviation Logistics Command Management Information System
NATOPS	Naval Air Training and Operating Procedures Standardization
NCDOC	Navy Cyber Defense Operations Command
NCIS	Naval Criminal Investigative Service
NSS	National Security Systems
OEM	Original Equipment Manufacturer
PDS	Protected Distribution System
PII	Personally Identifiable Information
PIV	Personally Identity Verification
PPP	Program Protection Plan
RMF	Risk Management Framework
RTOS	Real Time Operating Systems
SATCOM	Satellite Communications
SETR	Systems Engineering Technical Review
SIL	Software in the loop
SOUP	Software of Unknown Pedigree
STIG	Security Technical Implementation Guide
SWaP	Size, Weight and Power
TRANSEC	Transmission Security
UAS	Unmanned Aircraft System
USEM	Unsupported Extended Maintenance
UN/PW	User Name / Password