DoDEA Administrative Instruction 8510.01

Risk Management Framework for DoDEA Information Technology

Originating Division:	Information Technology
Effective:	October 29, 2019
Releasability:	Cleared for public release. Available on the DoDEA Policy Webpage.
Approved by:	Thomas M. Brady, Director

Purpose: This Issuance implements the Risk Management Framework (RMF) for the Department of Defense Education Activity (DoDEA) in accordance with the DoD Instruction 8510.01; DoDEA Administrative Instruction 8500.01; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37; Subchapter III of Chapter 35 of Title 44, United States Code (also known and referred to as the "Federal Information Security Management Act of 2002" and in this Issuance as FISMA); the Committee on National Security Systems Instruction (CNSSI) 1253; and NIST SP 800-53.

This Issuance also:

- Establishes associated DoDEA cybersecurity policy, and assigns responsibilities for executing and maintaining the RMF.

- Provides procedural guidance for the implementation of the RMF for DoDEA Information Systems (ISs) and Platform Information Technology (PIT), collectively, Information Technology (IT).

- Establishes a DoDEA Information Security Continuous Monitoring (ISCM) strategy for all DoDEA IT systems.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION 4
1.1. Applicability. 4
1.2. Policy. 4
1.3. Information Collection. 5
SECTION 2: RESPONSIBILITIES 6
2.1. DoDEA Director. 6
2.2. DoDEA Chief Information Officer. 6
2.3. DoDEA Senior Component Official for Privacy. 7
2.4. DoDEA Senior Information Security Officer. 8
2.5. DoDEA Authorizing Official. 8
2.6. DoDEA Authorizing Official Designated Representative. 9
2.7. DoDEA Security Control Assessor. 9
2.8. DoDEA Information System Owner. 10
2.9. DoDEA Risk Management Program Manager. 11
2.10. DoDEA Information System Security Manager. 11
2.11. DoDEA Information System Security Officer. 12
2.12. DoDEA User Representative. 13
SECTION 3: RISK MANAGEMENT FRAMEWORK APPOINTMENTS AND SEPARATION OF DUTIES...... 14
3.1. Risk Management Framework Role Appointment. 14
3.2. Separation of Duties. 14
SECTION 4: RISK MANAGEMENT FRAMEWORK PROCEDURES 16
4.1. Overview. 16
4.2. Forms of DoD Information Techology. 16
a. Assess and Authorize. 16
b. Assess Only. 16
c. Type Authorization. 17
4.3. Risk Management Framework Steps. 17
4.4. Regulatory Requirements. 21
a. Registrations. 21
b. Reviews. 21
4.5. Information Security Continuous Monitoring. 22
4.6. Required Documentation. 22
a. Privacy Impact Assessment. 22
b. System Security Plan. 22
c. Security Assessment Plan. 23
d. Security Assessment Report. 23
e. Plan of Action and Milestones. 23
f. Security Authorization Decision Document. 23
g. Risk Acceptance Form. 23
h. Risk Assessment Report. 24
i. Minimum Reporting Requirements. 24
4.7. Authorization Updates. 24
a. Ongoing Authorization. 24

b. Reauthorization. 24
GLOSSARY 26
G.1. Acronyms. 26
G.2. Definitions. 28
REFERENCES 32
APPENDIX 34
Appendix 1: Internal Controls Evaluation Checklist 34

TABLES

Table 1: Appointment of Risk Management Framework Roles 14

FIGURES

Figure 1: Risk Management Framework Steps 18
Figure 2: DoDEA Risk Management Framework Process Flow: Assess & Authorize 19
Figure 3: DoDEA Risk Management Framework Process Flow: Assess Only 20

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This Issuance applies to:

a. This Issuance applies to the DoDEA Headquarters Organization, the DoDEA Americas Region, the DoDEA Europe Region, the DoDEA Pacific Region, and to include all schools under the DoDEA authority, and when applicable, volunteers, students, support personnel, student teachers, contractors, and sponsors/parents.

b. All personnel affiliated with other DoD Components whose systems are hosted at a DoDEA data center or vendors who provide direct support to DoDEA-hosted IT.

c. This Issuance applies to all DoDEA IS. In accordance with DoDEA Administrative Instruction 8500.01, this includes enclaves, major applications, PIT, PIT systems, Industrial Control Systems (ICSs), and server and workstation software applications, hereinafter referred to collectively as "systems" or "IT/PIT system."

d. This Issuance applies to all DoDEA IT that receive, process, store, display, or transmit DoDEA information. This includes IT supporting research, development, test and evaluation, and DoDEA-controlled IT operated by a contractor or other entity on behalf of DoDEA.

1.2. POLICY. It is DoDEA policy that:

a. All DoDEA-funded IT will comply with DoD Instruction 8510.01 and this Issuance to implement the RMF process and obtain authorization for use.

b. The RMF must be consistent with the principles established in NIST SP 800-37 and satisfy the requirements and policies in accordance with DoD Instruction 8510.01.

c. All DoDEA IT assets must be categorized in accordance with CNSSI 1253, implement a corresponding set of security controls from NIST SP 800-53, be assessed and authorized, and receive an Authorization to Operate (ATO) in order to be compliant.

d. In accordance with NIST SP 800-18, all DoDEA IT systems to be assessed and authorized must develop a system security plan (SSP). DoDEA requires all systems utilize a SSP that complies with Section 4.6.b. of this Issuance. The DoDEA System Security Plan Template is available from the Office of the DoDEA Chief Information Officer (CIO).

e. Pursuant to Enclosure 5, Section 1.c. of DoD Instruction 8510.01, all DoDEA IT security authorization documentation and evidence must be posted and tracked in the DoD Enterprise Mission Assurance Support Service (eMASS).

f. Pursuant to Enclosure 3, Section 9.a.(1)(d) of DoD Instruction 8500.01, all DoDEA IT systems requiring an ATO must be registered in the DoD Information Technology Portfolio Repository (DITPR).

g. Pursuant to Enclosure 3, Section 9.b.(6) of DoD Instruction 8500.01, all ports, protocols, and services utilized by a DoDEA IT system must be registered and maintained in the Defense Information Systems Agency (DISA) Ports, Protocols, and Services Management (PPSM) Registry in accordance with DoD Instruction 8551.01.

h. Pursuant to DoD Instruction 8510.01, all DoDEA ISs will comply with the requirements of the DoDEA ISCM, including system configuration and installation of appropriate monitoring agents.

i. Nothing in this Issuance alters or supersedes the existing authorities and policies of the DoD CIO, laws, and regulations regarding the establishment of a DoD cybersecurity program to protect and defend DoD information and IT.

1.3. INFORMATION COLLECTION. This Issuance may result in the collection of information due to its policy and procedures. Any collection of information must follow all applicable Federal, DoD, and DoDEA regulations, policies, and guidance.

SECTION 2: RESPONSIBILITIES

2.1. DODEA DIRECTOR. The DoDEA Director:

a. Complies with the responsibilities of the DoD Component Head as established in DoD Instruction 8510.01 and Section 2.1. of DoDEA Administrative Instruction 8500.01.

b. Appoints a trained and qualified Authorizing Official (AO) in writing for all DoDEA IT operating within or on behalf of the DoDEA.

c. Appoints a trained and qualified Senior Component Official for Privacy (SCOP) in writing for all DoDEA ISs and PIT systems operating within or on behalf of the DoDEA.

2.2. DODEA CHIEF INFORMATION OFFICER. The DoDEA CIO:

a. Complies with the responsibilities of the DoD Component CIO established in Enclosure 4, Section 1.b.(2) of DoD Instruction 8510.01, and the responsibilities of the DoDEA CIO in Section 2.2. of DoDEA Administrative Instruction 8500.01.

b. The DoDEA CIO is responsible for the administration of the RMF within the DoDEA cybersecurity program.

c. Ensures an annual assessment of the DoDEA Risk Management Framework Program is conducted.

d. Appoints a DoDEA Senior Information Security Officer (SISO) in writing to direct and coordinate the DoDEA cybersecurity program.

e. Appoints an Information System Security Manager (ISSM) in writing for each DoDEA IT/ PIT system.

f. Appoints Information System Security Officers (ISSOs) in writing for each DoDEA IT/PIT system, as required.

g. Appoints personnel occupying cybersecurity positions in writing and ensures they are trained in accordance with DoD Directive 8140.01 and DoD Manual 8570.01-M.

h. Appoints a Program Manager (PM) in writing for each DoDEA IS or PIT system.

i. Appoints an Information System Owner (ISO) in writing for each DoDEA IS or PIT system. The ISO will be the Directorate or Division Head responsible for the overall procurement, development, integration, modification, operation, maintenance, and disposal of an IS or information.

j. Maintains visibility of assessment and authorization status of DoDEA IT systems.

k. Ensures contracts with third party providers of ISs or PIT systems will stipulate that the third party provider will assume responsibility for supplying the necessary information or deliverables for their system required by the RMF process and will comply with all aspects of this Issuance.

l. Ensures appropriate DoDEA IT/PIT systems are registered in DITPR.

m. Establishes and maintains processes and procedures to manage DoDEA Plans of Actions & Milestones (POA&Ms).

n. Reviews and documents concurrence on all ATOs issued for DoDEA IT/PIT systems with a level of risk of "Very High" or "High."

o. Ensures an effective ISCM program is established and implemented for DoDEA by establishing expectations and requirements for the DoDEA ISCM program.

2.3. DODEA SENIOR COMPONENT OFFICIAL FOR PRIVACY. The DoDEA SCOP:

a. Complies with all the privacy requirements and responsibilities of the SCOP established in DoD Directive 5400.11.

b. Complies with all the privacy requirements and responsibilities of the Senior Agency Official for Privacy established in NIST SP 800-53.

c. Develops, implements, and maintains a DoDEA-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and ISs.

d. Monitors Federal privacy laws and policies for changes that affect the privacy program.

e. Allocates sufficient resources to implement and operate the DoDEA-wide privacy program.

f. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures.

g. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, ISs, or technologies involving PII.

h. Reviews and approves Privacy Impact Assessments (PIAs) for ISs, programs, or other activities that pose a privacy risk in accordance with applicable law, Office of Management and Budget (OMB) policy, or any existing organizational policies and procedures.

i. Ensures the development of Systems of Records Notices (SORNs) and their publication in the Federal Register and on the DoDEA public website.

j. Develops, disseminates, and updates reports to the OMB, United States Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

2.4. DODEA SENIOR INFORMATION SECURITY OFFICER. The DoDEA SISO:

a. Complies with the responsibilities established in Enclosure 4, Section 1.b.(3) of DoD Instruction 8510.01, and Section 2.3. of DoDEA Administrative Instruction 8500.01.

b. Retains the authority and responsibility for security controls assessment and must establish and manage a coordinated security assessment process for information technologies governed by the DoDEA Cybersecurity Program.

c. Acts as the Security Control Assessor (SCA) or formally delegates in writing the security control assessment role for DoDEA IT/ PIT systems.

d. Establishes, implements, and maintains the DoDEA ISCM program; develops DoDEA program guidance (i.e., policies and procedures) for continuous monitoring of the security program and ISs.

e. Ensures completion of continuous monitoring security control assessments.

f. Implements and enforces the RMF within the DoDEA cybersecurity program.

g. Tracks the assessment and authorization status of IT/PIT systems governed by the DoDEA cybersecurity program.

h. Ensures vulnerability mitigation and incident response and reporting capabilities are in accordance with DoD policy and procedures.

i. Establishes and oversees a team of cybersecurity professionals qualified in accordance with DoD Directive 8140.01 and DoD Manual 8570.01-M, responsible for conducting security assessments. The DoDEA SISO may task, organize, staff, and centralize or direct assessment activities to representatives, as appropriate.

2.5. DODEA AUTHORIZING OFFICIAL. The DoDEA AO:

a. Complies with the responsibilities established in Enclosure 4, Section 1.c.(1) of DoD Instruction 8510.10, and Section 2.4 of DoDEA Administrative Instruction 8500.01.

b. Assumes responsibility for operating DoDEA IT/PIT under their purview at an acceptable level of risk to organizational operations, assets, individuals, other organizations, and national security.

c. Ensures DoDEA IT/PIT is properly assessed and authorized based on its environment of operation, security impact levels and required security controls, and properly documented in the DoDEA instance of eMASS.

d. Monitors and tracks overall execution of system-level POA&Ms.

e. Reviews the Security Assessment Report (SAR) in light of mission and information environment indicators and determines a course of action that will be provided to the responsible CIO or SISO for reporting requirements described in FISMA. An AO may downgrade or revoke an authorization decision at any time if risk conditions or concerns so warrant.

f. Assumes responsibility for ensuring the DoDEA ISCM program is applied with respect to a given system.

g. Appoints an Authorizing Official Designated Representative (AODR), if deemed necessary. The AODR cannot be delegated to make the authorization decision nor sign the associated decision document.

2.6. DODEA AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE. The DoDEA AODR:

a. Acts on behalf of the AO to coordinate and conduct required day-to-day activities associated with the security authorization process.

b. Prepare the final authorization package, obtain the authorizing official’s signature on the authorization decision document, and transmit the authorization package to appropriate organizational officials, if applicable to the package.

2.7. DODEA SECURITY CONTROL ASSESSOR. The DoDEA SCA:

a. Obtains and maintains Information Assurance Manager (IAM) Level III certification in accordance with DoD Manual 8570.01-M.

b. Performs tasks as required in NIST SP 800-37 and the RMF Knowledge Service (KS), located at https://rmfks.osd.mil.

c. Reviews and approves SSP for categorization and control set selection in accordance with CNSSI 1253.

d. Evaluates threats and vulnerabilities to DoDEA IT/PIT systems to ascertain the need for additional safeguards.

e. Develops, reviews, and approves the Security Assessment Plan (SAP), a plan to assess the security controls.

f. Ensures security assessments are completed for each system in accordance with the assessment procedures defined in the SAP.

g. Assesses systems or program management security controls for the DoDEA ISCM program.

h. At the conclusion of each security assessment activity, prepares the final SAR documenting the issues, findings, and recommendations from the security control assessment.

i. Assigns a vulnerability severity value for all non-compliant controls as part of the security control analysis to indicate severity associated with the identified vulnerability.

j. Determines and documents a risk level for every non-compliant security control in the SAR.

k. Reviews POA&Ms to ensure identified weaknesses are identified in the POA&M, planned mitigation strategies and timelines are acceptable and on track, and provides recommendations to the AO regarding matters related to the POA&M.

l. Evaluates security assessment documentation and provides written recommendations for security authorization to the AO.

m. Develops recommendation for authorization and submits the security authorization package to the AO.

n. Assesses proposed changes to DoDEA IT/PIT systems, their environment of operation, and mission needs that could affect system authorization. Record results of all security control assessments in the SAR.

2.8. DODEA INFORMATION SYSTEM OWNER. The DoDEA ISO:

a. Complies with the responsibilities established in Section 2.5 of DoDEA Administrative Instruction 8500.01.

b. Is responsible for categorization of the IT/PIT in accordance with CNSSI 1253.

c. Appoints a User Representative (UR) for each system under their purview.

d. Develops, maintains, and tracks the SSP for their respective systems.

e. Establishes processes and procedures in support of system-level implementation of the DoDEA ISCM program and documents in the SSP.

f. Ensures the system is registered with the appropriate organizational program/management offices and with the DITPR.

g. Identifies applicable common control providers, security controls, and overlays; documents in the SSP.

h. Implements security controls specific in the SSP.

i. Documents the security control implementation, as appropriate, in eMASS, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs).

j. Conducts initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassesses remediated control(s), as appropriate.

k. Prepares the POA&M based on the findings and recommendations of the security assessment report excluding any remediation actions taken.

l. Provides for continuous monitoring of security control assessment activities for their respective systems.

m. Performs annual review of systems listed in DITPR and certifies accuracy.

n. Initiates PIAs for each IS under their purview, pursuant to DoD Instruction 5400.16.

2.9. DODEA RISK MANAGEMENT PROGRAM MANAGER. The DoDEA Risk Management PM, also referred to in this Issuance as PM:

a. Complies with the responsibilities established in Section 2.c.(2)(b) of Enclosure 4 of DoD Instruction 8510.10.

b. Implements the RMF for assigned DoDEA systems.

c. Enforces AO authorization decisions for hosted or interconnected systems.

d. Ensures POA&M development, tracking, and resolution.

e. Ensures periodic reviews, testing, and assessment of assigned systems are conducted at least annually.

2.10. DODEA INFORMATION SYSTEM SECURITY MANAGER. The DoDEA ISSM:

a. Complies with the responsibilities established in Section 2.6 of DoDEA Administrative Instruction 8500.01 and Section 2.c.(2)(d) of Enclosure 4 of DoD Instruction 8510.01.

b. Must obtain and maintain IAM Level II or IAM Level III certification in accordance with DoD Manual 8570.01-M dependent on scope of effort.

c. Maintains and reports IT/PIT assessment and authorization status and issues in accordance with this Issuance.

d. Provides oversight of ISSOs to ensure that they are following established cybersecurity policies and procedures, in accordance with DoD Instruction 8500.01.

e. Monitors compliance with cybersecurity policy, as appropriate, and reviews the results of such monitoring.

f. Supports the ISO on the continuous monitoring security control assessment procedures to complete security responsibilities.

g. Ensures annual security control assessments are performed and the results entered into eMASS.

h. Ensures all users have the requisite security clearances and access authorization, and are aware of their cybersecurity responsibilities for DoD IS under their purview before being granted access to those systems.

i. Ensures that cybersecurity inspections, tests, and reviews are synchronized and coordinated with affected parties and organizations.

j. Acts as the primary cybersecurity technical advisor to the AO for DoD IT/ PIT systems under their purview.

2.11. DODEA INFORMATION SYSTEM SECURITY OFFICER. The DoDEA ISSO:

a. Complies with the responsibilities established in Section 2.7. of DoDEA Administrative Instruction 8500.01.

b. Must obtain and maintain IAM Level II or IAM Level III certification in accordance with DoD Manual 8570.01-M dependent on scope of effort.

c. Assists the ISSMs in meeting their duties and responsibilities of their respective systems.

d. Performs control correlation identifier (CCI) assessments of applicable security controls.

e. Supports the DoDEA ISCM program by assisting the ISO in completing ISCM responsibilities and by participating in the configuration management process for their respective systems, ensuring completion and reporting annually.

f. Provides an assessment and recommendation to the ISO and AO as to the need for reaccreditation as a result of a significant change to the system identified during continuous monitoring.

g. If required to perform the duties of a Control Assessment Validator (referred to as "Validator" within eMASS), acts as a trusted agent of the SCA and their role is to review the test results, artifacts, any entered vulnerabilities for non-compliant controls or CCIs, and status of each CCI of a security control.

2.12. DODEA USER REPRESENTATIVE. The DoDEA UR:

a. Represents operational and functional requirements of the user community for a particular system during the RMF process.

b. Understands the operating environment, system mission criticality, reliability/survivability requirements, etc., of the system.

c. Supports the security controls assignment, implementation, and assessment to ensure user community needs are met.

SECTION 3: RISK MANAGEMENT FRAMEWORK APPOINTMENTS AND SEPARATION OF DUTIES

3.1. RISK MANAGEMENT FRAMEWORK ROLE APPOINTMENT. See Table 1: Appointment of RMF Roles of this Issuance that identifies the appropriate authority for the appointment of RMF roles.

Table 1: Appointment of Risk Management Framework Roles

Role	Appointed By
DoDEA CIO	DoDEA Director
AO (formerly known as the Designated Accrediting Authority (DAA))	DoDEA Director
AODR	AO
DoDEA SISO (formerly known as the Chief Information Security Officer (CISO))	DoDEA CIO
SCA	DoDEA SISO is the Component SCA, but may formally delegate the SCA role as appropriate
PM	DoDEA CIO
ISO (for DoDEA systems)	DoDEA CIO
ISSM (formerly IAM)	DoDEA CIO
ISSO (formerly known as the Information Assurance Officer (IAO))	DoDEA CIO
UR	ISO

3.2. SEPARATION OF DUTIES.

a. The CIO can act as the AO, but cannot perform any other roles in the RMF process.

b. The AO cannot perform any other roles in the RMF process.

c. The PM, ISSM, and ISSO cannot be the AO.

d. The AO cannot report to the PM, ISSM, or ISSO.

e. There can be multiple individuals fulfilling the ISSO and Validator roles in eMASS on any given system authorization package. However, the ISSO and Validator cannot be the same person for the same control.

f. The Validator role is assumed by individuals who are appointed as an ISSO and are qualified for the level of the system being authorized.

g. Whoever is appointed the SCA over a system will also be assigned the Certifying Agent (CA) Representative role within eMASS.

h. The SCA appointed to a system cannot perform the ISSO, ISSM, or Validator roles on that system.

i. The ISO assumes the PM role or can delegate in writing to an appropriately qualified individual with the requisite certifications for IAM Level II for network systems and IAM Level III for enclaves in accordance with DoD Manual 8570.01-M.

j. The ISSM and ISSO can only be performed by individuals with the requisite certifications in accordance with DoD Manual 8570.01-M: IAM Level II for network systems and IAM Level III for enclaves.

SECTION 4: RISK MANAGEMENT FRAMEWORK PROCEDURES

4.1. OVERVIEW. As a component of the DoD and a Federal Activity, DoDEA must comply with DoD cybersecurity requirements for establishing a RMF process to protect all DoDEA IT assets from cybersecurity vulnerabilities. All DoDEA IT assets must be assessed for effectiveness of security controls and receive an ATO in order to be compliant.

4.2. FORMS OF DOD INFORMATION TECHOLOGY. Pursuant to DoD Instruction 8510.01, effective October 1, 2016, no DoD Information Assurance Certification and Accreditation Process (DIACAP) ATOs can be issued or extended. All systems must be reassessed and authorized under the RMF. Additionally, DoDEA IT assets can no longer be comprehensively covered under simply four (4) enclave ATOs; per RMF, ATOs require greater distinction (i.e., DoD Instruction 8510.01 and NIST SP 800-18). DoDEA IT, as defined in DoDEA Administrative Instruction 8500.01, can follow either the “Assess and Authorize” (A&A) process or the “Assess Only” process.

a. Assess and Authorize. The types of DoDEA IT that are subject to A&A must follow all steps of the RMF process (see Section 4.3 and Figure 2: DoDEA RMF Process Flow - Assess & Authorize of this Issuance), and include:

(1) Enclaves.

(2) Major Applications.

(3) PIT systems (ICSs on the DoDEA network).

(4) Operational common control providers such as general support services, a common network, the enterprise backbone, etc.

b. Assess Only. Unlike A&A, DoDEA IT under “Assess Only” does not require an ATO. Rather, it receives an approval letter from the AO allowing the IT to be installed on or used with a system that received an ATO. The first four (4) steps and step six (6) of the RMF process are common for both the A&A and Assess Only processes (see Section 4.3 and Figure 3: DoDEA RMF Process Flow - Assess Only of this Issuance). The only real difference is in Step 5, where there are fewer requirements for approving an Assess Only system than obtaining an ATO for an A&A system. The types of DoDEA IT that can be assessed only include:

(1) PIT (ICSs that are not on the DoDEA network nor connected to the internet).

(2) Software (a software program installed on a user workstation).

(3) Applications (e.g., software program hosted by a server, minor applications, such as web applications or the DoDEA Micro Applications hosted on the Remote Desktop Services (RDS) server).

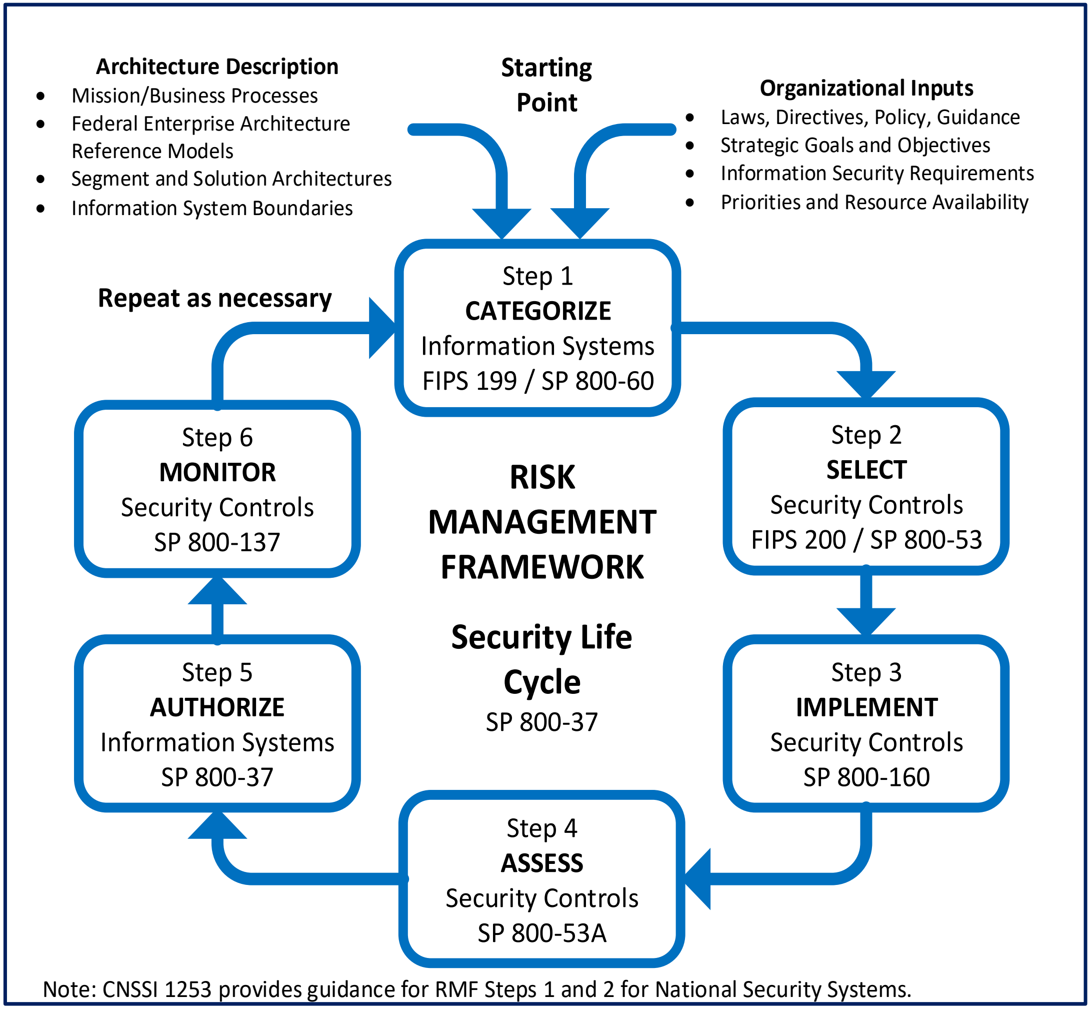
(4) Non-operational common control providers that solely reference policies, procedures, definitions, values (parameters), etc.

c. Type Authorization. The type authorization is used to deploy identical copies of an IT or PIT system in specified environments. This method allows a single security authorization package to be developed as an archetype for the common version of a system. The system can then be deployed to multiple locations with a set of installation, security control and configuration requirements, or operational security needs that will be provided by the hosting enclave. ICSs, such as building environmental, communications, and safety (fire alarm) systems are examples of PIT systems that would benefit from type authorization.

4.3. RISK MANAGEMENT FRAMEWORK STEPS.

a. In accordance with NIST SP 800-37, the RMF consists of the steps depicted in Figure 1: Risk Management Framework Steps of this Issuance. The RMF process parallels the system life cycle, with the RMF activities being initiated at program or system inception (e.g., documented during capabilities identification or at the implementation of a major system modification). However, failure to initiate the RMF at system or program inception is not a justification for ignoring or not complying with the RMF. All systems must be brought into compliance, and those systems without ATOs must initiate the RMF in accordance with DoD Instruction 8510.01 and this Issuance. Chapter 3 of NIST SP 800-37 details the steps of the RMF, and paragraphs 2a through 2f of Enclosure 6 of DoD Instruction 8510.01 provide amplifying DoD implementation guidance for those steps.

Figure 1: Risk Management Framework Steps


Architecture Description
Mission/Business Processes
Federal Enterprise Architecture Reference Models
Segment and Solution Architectures
Information System Boundaries
Starting Point
Organizational Inputs
Laws, Directives, Policy, Guidance
Strategic Goals and Objectives
Information Security Requirements
Priorities and Resource Availability
Repeat as necessary
Step 1 CATEGORIZE Information Systems FIPS 199 / SP 800-60
Step 2 SELECT Security Controls FIPS 200 / SP 800-53
Step 3 IMPLEMENT Security Controls SP 800-160
Step 4 ASSESS Security Controls SP 800-53A
Step 5 AUTHORIZE Information Systems SP 800-37
Step 6 MONITOR Security Controls SP 800-137
RISK MANAGEMENT FRAMEWORK
Security Life Cycle
SP 800-37

Note: CNSSI 1253 provides guidance for RMF Steps 1 and 2 for National Security Systems.

b. Per DoD Instruction 8510.01, all DoDEA IT/PIT must be categorized in accordance with CNSSI 1253, based upon information type mapping provided by Volumes I and II of NIST SP 800-60. The latter two (2) volumes allow for a process to determine the appropriate system categorization impact level (low, moderate, or high) for each of the security objectives (confidentiality, integrity, or availability), based on the types of information within the system. Using the results from that analysis, CNSSI 1253 provides guidance on the baseline security control set and overlays to implement for the system.

c. Although there are minor differences between the implementation of RMF by the DoD and NIST SP 800-18; NIST SP 800-30; NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; and Volumes I and II of NIST SP 800-60, the steps are the same, as is the end result – authorizing ISs under RMF and utilization of continuous monitoring techniques. Figure 2: DoDEA RMF Process Flow: Assess & Authorize of this Issuance provides the process flow for the implementation of RMF at DoDEA.

Figure 2: DoDEA Risk Management Framework Process Flow: Assess & Authorize

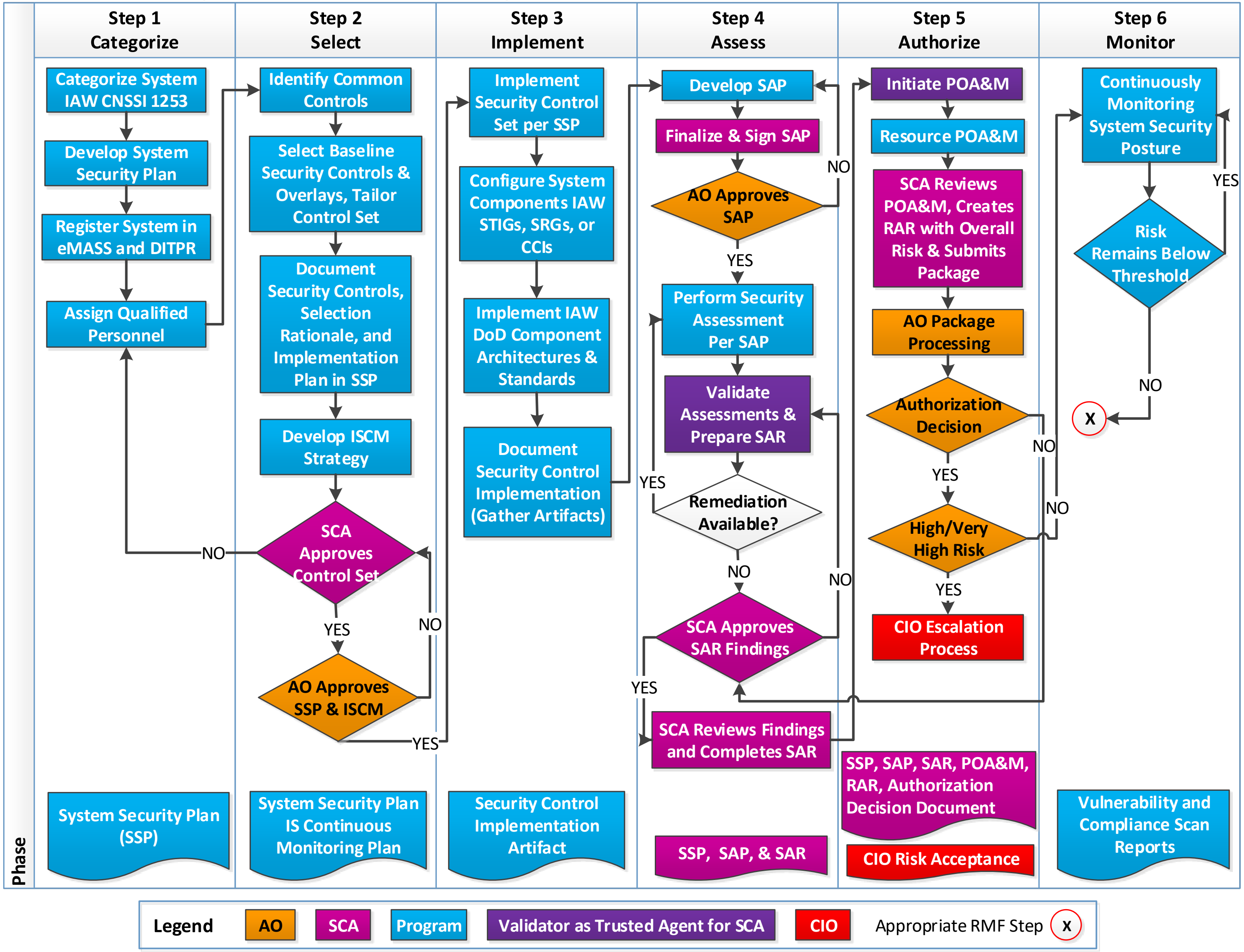
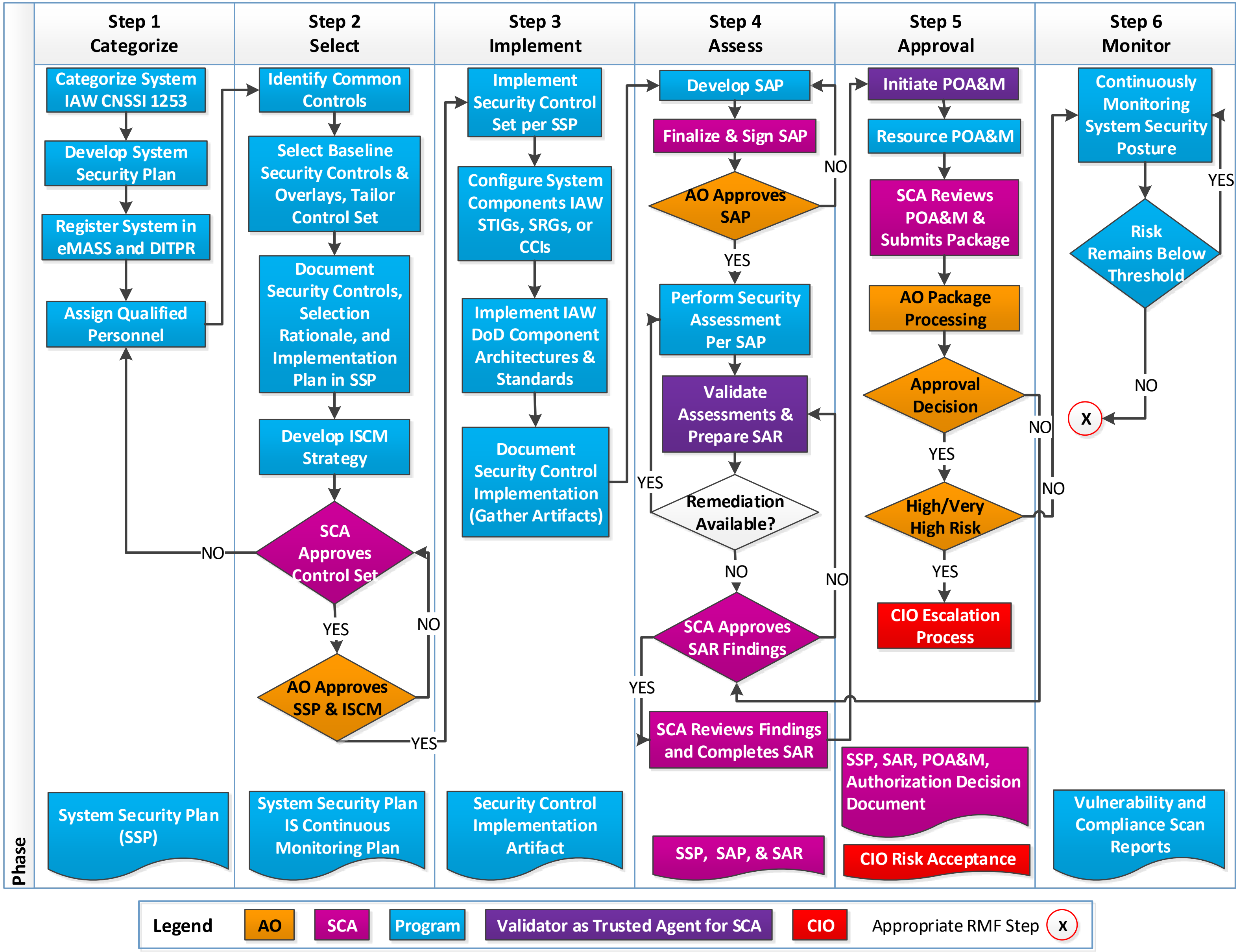

Phase
Step 1
Categorize
Step 2
Select
Step 3
Implement
Step 4
Assess
Step 5
Authorize
Step 6
Monitor
Categorize System IAW CNSSI 1253
Develop System Security Plan
Register System in eMASS and DITPR
Assign Qualified Personnel
System Security Plan (SSP)
Identify Common Controls
Select Baseline Security Controls & Overlays, Tailor Control Set
Document Security Controls, Selection Rationale, and Implementation Plan in SSP
Develop ISCM Strategy
SCA Approves Control Set
NO
YES
AO Approves SSP & ISCM
NO
YES
System Security Plan IS Continuous Monitoring Plan
Implement Security Control Set per SSP
Configure System Components IAW STIGs, SRGs, or CCIs
Implement IAW DoD Component Architectures & Standards
Document Security Control Implementation (Gather Artifacts)
Security Control Implementation Artifact
Develop SAP
Finalize & Sign SAP
AO Approves SAP
NO
YES
Perform Security Assessment Per SAP
Validate Assessments & Prepare SAR
YES
Remediation Available?
NO
SCA Approves SAR Findings
NO
YES
SCA Reviews Findings and Completes SAR
SSP, SAP, & SAR
Initiate POA&M
Resource POA&M
SCA Reviews POA&M, Creates RAR with Overall Risk & Submits Package
AO Package Processing
Authorization Decision
NO
YES
High/Very High Risk
NO
YES
CIO Escalation Process
SSP, SAP, SAR, POA&M, RAR, Authorization Decision Document
CIO Risk Acceptance
Continuously Monitoring System Security Posture
Risk Remains Below Threshold
YES
NO
X
Vulnerability and Compliance Scan Reports
Legend
AO
SCA
Program
Validator as Trusted Agent for SCA
CIO
Appropriate RMF Step
X

Figure 3: DoDEA Risk Management Framework Process Flow: Assess Only


Phase
Step 1
Categorize
Step 2
Select
Step 3
Implement
Step 4
Assess
Step 5
Approval
Step 6
Monitor
Categorize System IAW CNSSI 1253
Develop System Security Plan
Register System in eMASS and DITPR
Assign Qualified Personnel
System Security Plan (SSP)
Identify Common Controls
Select Baseline Security Controls & Overlays, Tailor Control Set
Document Security Controls, Selection Rationale, and Implementation Plan in SSP
Develop ISCM Strategy
SCA Approves Control Set
NO
YES
NO
AO Approves SSP & ISCM
YES
System Security Plan IS Continuous Monitoring Plan
Implement Security Control Set per SSP
Configure System Components IAW STIGs, SRGs, or CCIs
Implement IAW DoD Component Architectures & Standards
Document Security Control Implementation (Gather Artifacts)
Security Control Implementation Artifact
Develop SAP
Finalize & Sign SAP
AO Approves SAP
NO
YES
Perform Security Assessment Per SAP
Validate Assessments & Prepare SAR
Remediation Available?
YES
NO
SCA Approves SAR Findings
NO
YES
SCA Reviews Findings and Completes SAR
SSP, SAP, & SAR
Initiate POA&M
Resource POA&M
SCA Reviews POA&M & Submits Package
AO Package Processing
Approval Decision
NO
YES
High/Very High Risk
NO
YES
CIO Escalation Process
SSP, SAR, POA&M, Authorization Decision Document
CIO Risk Acceptance
Continuously Monitoring System Security Posture
Risk Remains Below Threshold
YES
NO
X
Vulnerability and Compliance Scan Reports
Legend
AO
SCA
Program
Validator as Trusted Agent for SCA
CIO
Appropriate RMF Step
X

4.4. REGULATORY REQUIREMENTS.

a. Registrations. There are Federally mandated registration requirements for DoDEA IT/PIT systems. The following DoD systems, DoD Information Technology Investment Portal (DITIP), Select and Native Programming – Information Technology (SNaP-IT), DITPR, PPSM, and eMASS, require very similar information that is addressed in a SSP as defined in NIST SP 800-18, and as implemented in the DoDEA SSP Template. Access to these systems requires approved accounts, which is limited for administrative purposes. DITPR, PPSM, and eMASS registration will be under the guidance of the DoDEA SISO, while DITIP and SNaP-IT will be under the guidance of the DoDEA IT Information Resource Management Branch.

(1) Pursuant to Section 2222 of Title 10, United States Code and the direction in the DoD Deputy Chief Management Officer (DCMO) Defense Business Systems Investment Management Guidance, every Defense Business System (DBS) that has a total cost in excess of $1,000,000 or more over the period of the current future-years defense program (FYDP) must be reviewed and certified by the Investment Review Board (IRB) and approved by the Defense Business Council (DBC).

(2) Pursuant to DoD Financial Management Regulation 7000.14-R, each DoD Component will manage their IT investments through DITIP. DITIP is the system of record for the four (4) Fiscal Year 2019 National Defense Authorization Act (NDAA) DBS data elements: Business Enterprise Architecture (BEA) Code, BEA Version, Business Process Re-engineering (BPR) Code and Category Critical Capability (CATBC) Code.

(3) Pursuant to DoD Financial Management Regulation 7000.14-R, all DoD IT budget information and the FYDP will be managed using the SNaP-IT system.

(4) OMB Circular A-130 require that all major ISs must be maintained by an inventory system. The September 28, 2005 DoD CIO Memorandum and DoD Instruction 8500.01 identifies the DITPR as the DoD authoritative inventory system and requires all authorized systems to be registered. DoD Financial Management Regulation 7000.14-R requires each DITPR line to be aligned against an active SNaP-IT Unique Investment Identifier (UII).

(5) DoD Instruction 8500.01 requires following the NIST RMF as implemented by DoD Instruction 8510.01 for systems to be assessed and authorized.

(6) DoD Instruction 8510.01 requires all DoD IS to be registered with the PPSM per DoD Instruction 8551.01. This is a requirement for each system, individually, not an entire enclave or DoDEA in total.

(7) DoD Instruction 8510.01 requires that systems to be authorized must be registered and tracked in eMASS.

b. Reviews. In accordance with FISMA requirements, each system owner will review their respective systems at least annually for compliance, including review of DITPR, DITIP, and eMASS records. Any proposed changes to a system must be reviewed for the impact to the security posture of that system prior to the change being implemented, and any applicable updates made to the DITPR, DITIP, and eMASS records.

4.5. INFORMATION SECURITY CONTINUOUS MONITORING.

a. Pursuant to Section 4.d.5. of Appendix 1 of OMB Circular A-130, and in accordance with NIST SP 800-137 and Sections 2.b.(3) and 2.b.(4) of Enclosure 6 of DoD Instruction 8510.01, all DoDEA ISs will develop and document a system-level strategy for the continuous monitoring of the effectiveness of all applicable security controls. Pursuant to Section 4.d.9. of Appendix I of OMB Circular A-130, the ISCM strategy must include the appropriate NIST SP 800-53 privacy controls. The overall strategy must include the plan for annual assessments of a subset of implemented security controls and must be documented in the SSP, including the detail of the controls requiring annual assessment, as well as those to be assessed in the second and third year of the assessment cycle.

b. In addition to system level security control monitoring, and in order to protect the DoDEA network, DoDEA will implement the guidance provided by DISA with their Continuous Monitoring and Risk Scoring (CMRS) program utilized by systems hosted on the Nonsecure Internet Protocol Router Network (NIPRNet) and Secure Internet Protocol Router Network (SIPRNet). In particular, DoDEA will utilize the following:

(1) The Assured Compliance Assessment Solution (ACAS) to scan for security vulnerabilities including Security Technical Implementation Guide (STIG), Information Assurance Vulnerability Management (IAVM) vulnerability, and patch compliance.

(2) Install DISA-required Host Based Security System (HBSS) endpoint products, to include, but not limited, to antivirus management, Asset Configuration Compliance Module (ACCM), Data Loss Prevention (DLP), Host Intrusion Prevention System (HIPS), and Policy Auditor (PA).

4.6. REQUIRED DOCUMENTATION. A critical component to the authorization process is proper documentation of the IS. Each step in the RMF process generates documentation, as required by NIST SP 800-37, NIST SP 800-53, and DoD Instruction 8510.01. Although NIST SP 800-53 requires an extensive list of policies and procedures, the documents listed here are those required by RMF in order to make an authorization decision.

a. Privacy Impact Assessment. Pursuant to Section 208 of *Public Law 107-347,* also known and referred to as the “E-Government Act of 2002,” all Federal Agencies must conduct a PIA and complete Defense of Department (DD) Form 2930A, “Adapted Privacy Impact Assessment (Adp-PIA)” before a system is authorized to operate or when changes to the system create new privacy risks. OMB Memorandum M-03-22 extends that to require all ISs.

b. System Security Plan. All DoDEA IS must have a SSP that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The SSP must be approved and digitally signed by the ISO, SCA, and AO. In order to ensure capture of all relevant information required by the registration and authorization processes, all DoDEA IS must utilize an SSP that complies with NIST SP 800-18 and contains the following: Detailed network diagram of the IS and its authorization boundary, hardware/software component lists, data flow diagram, PPSM Registry information, and a list of user groups and roles. The DoDEA IT Division maintains the DoDEA SSP Template that complies with this Issuance and has been approved by the DoDEA CIO. The DoDEA SSP Template is available from the DoDEA IT Division.

c. Security Assessment Plan. The SAP provides the objectives for the security control assessment, a detailed roadmap of how to conduct such an assessment, and assessment procedures, and is a standard report in eMASS. The SAP must be approved and digitally signed by the ISO, SCA, and AO.

d. Security Assessment Report. The results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the SAR, which can be created in eMASS. The SAR must be digitally signed by the SCA prior to submission to the AO for the authorization decision.

e. Plan of Action and Milestones. All non-compliant (NC) controls must have a vulnerability associated with them, either at the CCI level, or at the control level itself, which must be added to the system POA&M. At a minimum, a system POA&M must provide all information requested in the DoD System Level POA&M Template (located at https://www.disa.mil/-/media/Files/DISA/Services/DISN-Connect/References/SystemLevel-POAM-Sample.xlsx) and contain all NC, not applicable (N/A), and risk accepted controls, and digitally signed by the AO.

f. Security Authorization Decision Document. The authorization decision document conveys the final security authorization decision from the AO to the ISO or common control provider, and other organizational or DoD agency officials, as appropriate.

(1) The authorization decision document contains the following information: Authorization decision; terms and conditions for the authorization; and authorization termination date (ATD). The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the IS or inherited controls that must be followed by the system owner or common control provider.

(2) In accordance with DoD Instruction 8510.01, the security authorization decision indicates to the ISO whether the system receives one of the following types of authorization: ATO; ATO with Conditions; Interim Authorization to Test (IATT); or Denied Authorization to Operate (DATO).

g. Risk Acceptance Form. If NC controls with a level of risk of “Very High” or “High” exist that cannot be corrected or mitigated immediately, but overall system risk is determined to be acceptable due to mission criticality, then the authorization decision will be issued in the form of an ATO with conditions and only with permission of the DoDEA CIO. If required by the CIO, this decision will be documented through the completion of a DoDEA Form 8510, “Risk Acceptance Form,” and approved and digitally signed by the ISSM, SISO, and AO.

h. Risk Assessment Report. Risk assessment reports (RARs) provide decision makers with an understanding of the information security risk to organizational operations and assets, individuals, other organizations, or the United States that derive from the operation and use of organizational ISs and the environments in which those systems operate. DoDEA does not develop separate RARs for systems registered in eMASS. Rather, the Risk Assessment module within eMASS is utilized to perform the individual control risk assessments, which are then included in the SAR that is generated by eMASS.

i. Minimum Reporting Requirements. In accordance with DoD Instruction 8510.01 and NIST SP 800-37, the SSP, SAR, and the POA&M are the minimum documents required to be submitted to the AO for an authorization decision. For Assess Only approvals, DoDEA will follow this guidance. However, for an A&A decision, DoDEA requires that the RAR and any applicable DoDEA Form 8510, "Risk Acceptance Form" must also be included in the authorization package.

4.7. AUTHORIZATION UPDATES. After the initial ATO is issued, there are two (2) possible subsequent authorization events.

a. Ongoing Authorization. This is an event-driven authorization, in that the system must be reassessed should at least one (1) of the below events be triggered. If any one of the events occur, a reassessment of the applicable security control families must be conducted. If there is no material change to the security posture of the system, then the relevant documents should be updated and uploaded to eMASS. If the security posture has changed, then the system must be resubmitted for an authorization decision. The triggering events are:

(1) New threat/vulnerability/impact information.

(2) An increased number of findings/weaknesses/deficiencies from the ISCM program.

(3) New missions/business requirements.

(4) A change in the authorizing official.

(5) A significant change in risk assessment findings.

(6) Significant changes to the IS, common controls, or the environment of operation.

(7) Organizational thresholds being exceeded.

b. Reauthorization. This is the static, single point-in-time risk determination and risk acceptance decision that occurs after the initial authorization. As long as no ongoing authorization event is triggered, DoDEA will adhere to a three-year schedule for authorizations. A subset of the applicable security controls must be reassessed each year, such that all security controls will be assessed over the three-year period, according to the schedule documented in the SSP. If there is no material change to the security posture of the system during one of the intervening year's assessments, then the relevant documents (i.e., evidence) should be updated and uploaded to eMASS and the appropriate registrations, such as in DITPR, updated to reflect the reassessment. However, if there is any material change to the security posture of the system identified during security control reassessment during the intervening years, that constitutes an ongoing authorization event and the system must be submitted for a new authorization decision. At the end of the third year's assessment, a new authorization decision must be made by the AO.

GLOSSARY

G.1. ACRONYMS.

A&A	Assess and Authorize
ACAS	Assured Compliance Assessment Solution
ACCM	Asset Configuration Compliance Module
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
ATD	Authorization Termination Date
ATO	Authorization to Operate
BEA	Business Enterprise Architecture
BPR	Business Process Re-engineering
CA	Certifying Agent
CATBC	Category Critical Capability
CCI	control correlation identifier
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMRS	Continuous Monitoring and Risk Scoring
CNSSI	Committee on National Security Systems Instruction
DAA	Designated Accrediting Authority
DATO	Denied Authorization to Operate
DBC	Defense Business Council
DBS	Defense Business System
DCMO	Deputy Chief Management Officer
DD	Department of Defense
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DITIP	DoD Information Technology Investment Portal
DITPR	DoD Information Technology Portfolio Repository
DLP	Data Loss Prevention
eMASS	Enterprise Mission Assurance Support Service
FIPS	Federal Information Processing System
FISMA	Federal Information Security Management Act
FYDP	future-years defense program
HBSS	Host Based Security System
HIPS	Host Intrusion Prevention System
IAM	Information Assurance Manager

IAO	Information Assurance Officer
IATT	Interim Authority to Test
IAVM	Information Assurance Vulnerability Management
ICS	industrial control system
IRB	Investment Review Board
IS	information system (may be IT or PIT)
ISCM	Information Security Continuous Monitoring
ISO	Information System Owner
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	information technology
KS	Knowledge Service
N/A	not applicable
NC	non-compliant
NDAA	National Defense Authorization Act
NIPRNet	Nonsecure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PA	Policy Auditor
PIA	Privacy Impact Assessment
PII	personally identifiable information
PIT	platform information technology
PM	Program Manager
POA&M	plan of action and milestones
PPSM	ports, protocols, and services management
RAR	Risk Assessment Report
RDS	Remote Desktop Services
RMF	Risk Management Framework
SAP	Security Assessment Plan
SAR	Security Assessment Report
SCA	Security Control Assessor
SCOP	Senior Component Official for Privacy
SIPRNet	Secure Internet Protocol Router Network
SISO	Senior Information Security Officer
SNaP-IT	Select and Native Programming – Information Technology
SORN	Systems of Records Notice
SP	Special Publication
SSP	System Security Plan
STIG	Security Technical Implementation Guide

UII	unique investment identifier
UR	User Representative
WAN	wide area network

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this Issuance.

application. An information resource (information and IT) hosted by an IS used to satisfy a specific set of user requirements.

authorization boundary. As defined in CNSSI 4009, all components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

AO. As defined in DoD Instruction 8510.01, a senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

AODR. As defined in DoD Instruction 8510.01, previously, this position was titled as the DAA Representative. However, with the move to RMF, the position is now the AODR and is an organizational official acting on behalf of an AO in carrying out and coordinating the required activities associated with security authorization.

ATO. As defined in DoD Instruction 8510.01, a risk-based authorization decision granted by the AO to operate a system.

boundary. As defined in CNSSI 4009, a physical or logical perimeter of a system.

boundary protection. As defined in NIST SP 800-53, the monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., gateways, routers, firewalls, guards, encrypted tunnels).

common control. As defined in NIST SP 800-37, a security control that is inherited by one (1) or more organizational information systems. See security control inheritance.

common control provider. As defined in NIST SP 800-37, an organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems).

CCI. As defined in DoD Instruction 8500.01, a CCI is a decomposition of a NIST control into a single, actionable, measurable statement.

DBS. The term “defense business system” as defined in Section 2222(j)(1) of Title 10, United States Code means an information system, other than a national security system, operated by, for, or on behalf of the DoD, including financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management. The term “covered defense business system” as defined at Section 2222(j)(2) of Title 10 United States Code means any defense business system program that is expected to have a total cost in excess of $1,000,000 over the current future-years defense program submitted to the United States Congress under Section 221 of Title 10, United States Code.

DIACAP. This is the process utilized by DoD prior to RMF to certify and accredit systems and authorize to operate.

enclave. As defined in CNSSI 4009, a set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.

enclave boundary. As defined in CNSSI 4009, the point at which an enclave’s internal network service layer connects to an external network’s service layer, i.e., to another enclave or to a wide area network (WAN).

general support services. As defined in Appendix III of OMB Circular No. A-130, an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

inherited controls. As defined in NIST SP 800-53A, a situation in which an IS or application receives protection from security controls (or portions of security controls) that are developed, implemented, and assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See common control.

interconnected system. As defined in NIST SP 800-47, the direct connection of two (2) or more information systems for the purpose of sharing data and other information resources.

IS. As defined in Section 3502 of Title 44 United States Code, a discrete set of information resources/applications, within a distinct authorization boundary, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. This applies to both IT and PIT.

IRB. The IRB reviews and certifies the planning, design, acquisition, development, deployment, operation, maintenance, modernization, and project cost benefits and risks of covered defense business systems programs.

ISO. The ISO assumes the PM role or can delegate to an appropriately qualified individual.

logical perimeter. As defined in CNSSI 4009, a conceptual perimeter that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system without a reliable human review by an appropriate authority. The location of such a review is commonly referred to as an “air gap”.

major application. As defined in CNSSI 4009, an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

minor application. As defined in NIST SP 800-18, an application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications include micro applications and are typically included as part of a general support system.

mitigation. Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

overlay. As defined in NIST SP 800-53, a specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.

PII. As defined in NIST SP 800-122, any information about an individual maintained by an agency, including: (1) Any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

PIT. As defined in DoD Instruction 8500.01, PIT is IT, both hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems.

PIT system. As defined in DoD Instruction 8500.01, a collection of PIT within an identified boundary under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

remediation. Actions taken to eliminate an identified risk.

RMF. The RMF provides a disciplined and structured process that combines IS security and risk management activities into the system development life cycle and authorizes their use within

DoD. The RMF has six (6) steps: Categorize system; select security controls; implement security controls; assess security controls; authorize system; and monitor security controls.

SCA. Under DIACAP, this position was the CA. In addition there is currently a CA Representative role in eMASS, but this role is not utilized by DoDEA.

security authorization package. As defined in NIST SP 800-37, documents the results of the security control assessment and provides the authorizing official with essential information needed to make a risk-based decision on whether to authorize operation of an information system or a designated set of common controls.

security control assessment. As defined in NIST SP 800-37, the testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

security controls. As defined in Federal Information Processing Standards (FIPS) Publication 199, the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

STIG. As defined in DoD Instruction 8500.01, STIGs are based on DoD policy and security controls. Implementation guide geared to a specific product and version. Contains all requirements that have been flagged as applicable for the product which have been selected on a DoD baseline.

type authorization. As defined in NIST SP 800-37, an official authorization decision to employ identical copies of an IS or subsystem (including hardware, software, firmware, and/or applications) in specified environments of operation.

REFERENCES

Committee on National Security Systems Instruction Number 1253, "Security Categorization and Control Selection for National Security Systems," March 27, 2014

Committee on National Security Systems Instruction Number 4009, "Committee on National Security Systems (CNSS) Glossary," April 6, 2015

DD Form 2930A, "Adapted Privacy Impact Assessment (Adp-PIA)," August 2011

DoD Deputy Chief Management Officer (DCMO), "Defense Business Systems Investment Management Guidance," current edition, located at https://cmo.defense.gov/Resources/Defense-Business-Council

DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Information Technology (IT) Registry Merger Into the DoD IT Portfolio Repository (DITPR)," September 28, 2005

DoD Directive 5400.11, "DoD Privacy and Civil Liberties Program," January 29, 2019

DoD Directive 8140.01, "Cyberspace Workforce Management," August 11, 2015, as amended

DoD Financial Management Regulation 7000.14-R, "Department of Defense Financial Management Regulation (FMRS)," current edition

DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015, as amended

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014

DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended

DoD Instruction 8551.01, "Ports, Protocols, and Service Management (PPSM)," May 28, 2014, as amended

DoD Manual 8570.01-M, "Information Assurance Workforce Improvement Program," December 19, 2005, as amended

DoDEA Administrative Instruction 8500.01, "DoDEA Cybersecurity Program," October 28, 2019

DoDEA Form 8510, "Risk Acceptance Form," October 2019

Federal Information Processing Standards Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004, located at https://csrc.nist.gov/publications

National Institute of Standards and Technology Special Publication 800-18, "Guide for Developing Security Plans for Federal Information Systems," February 24, 2006, as amended, located at https://csrc.nist.gov/publications

National Institute of Standards and Technology Special Publication 800-30, Guide for Conducting Risk Assessments," September 17, 2012, as amended, located at https://csrc.nist.gov/publications

National Institute of Standards and Technology Special Publication 800-37, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," as amended, located at https://csrc.nist.gov/publications

National Institute of Standards and Technology Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” as amended, located at https://csrc.nist.gov/publications

National Institute of Standards and Technology Special Publication 800-53A, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans,” as amended, located at https://csrc.nist.gov/publications

National Institute of Standards and Technology Special Publication 800-60, Volume I, “Guide for Mapping Types of Information and Information Systems to Security Categories,” as amended, located at https://csrc.nist.gov/publications

National Institute of Standards and Technology Special Publication 800-60, Volume II, “Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices,” as amended, located at https://csrc.nist.gov/publications

National Institute of Standards and Technology Special Publication 800-122, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),” April 2010, located at https://csrc.nist.gov/publications

National Institute of Standards and Technology Special Publication 800-137, “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,” September 2011, located at https://csrc.nist.gov/publications

Office of Management and Budget Circular Number A-130, “Managing Federal Information as a Strategic Resource,” current edition

Office of Management and Budget Memorandum M-03-22, “OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,” September 26, 2003

Public Law 107-347, “E-Government Act of 2002,” December 17, 2002

United States Code, Title 10

United States Code, Title 44, Section 3502

United States Code, Title 44, Subchapter III of Chapter 35 (also known as the “Federal Information Security Management Act of 2002” and referred to in this Issuance as “FISMA”)

APPENDIX

APPENDIX 1: INTERNAL CONTROLS EVALUATION CHECKLIST

In accordance with Section 2.2.c. of this Issuance, the DoDEA Director, or their designee, shall ensure that DoDEA compliance with this Issuance is reviewed on an annual basis. The key areas to be audited include, but are not limited, to those shown in the checklist.

Section	Requirement	Completed
2.1.b.	A trained and qualified AO has been appointed in writing for all DoDEA ISs and PIT systems.	
2.1.c.	A trained and qualified SCOP has been appointed in writing for DoDEA.	
2.2.d.	A SISO has been appointed.	
2.2.h.	A PM has been appointed for each DoDEA IS or PIT system	
2.2.i.	An ISO has been appointed for each DoDEA IS or PIT system.	
3.2.	DoDEA RMF Role assignments are in adherence with Separation of Duties.	
4.	All DoDEA IT systems are authorized or approved in accordance with this Issuance, and in compliance with all Federal regulations.	
4.4.a.(4)	Each ISO reviews the DITPR registration for accuracy for their respective systems on an annual basis.	
4.4.a.(6)	Each ISO reviews the DoD PPSM for accuracy upon any change to their respective systems.	
4.4.a.(7)	Every DoDEA system that requires authorization or approval has been registered in eMASS.	
4.5	Every DoDEA system that requires authorization or approval has a System-Level Information Security Continuous monitoring Strategy.	
4.6.	Every DoDEA system that has been authorized or approved has all the required documentation maintained by eMASS or uploaded into eMASS as artifacts.	
4.7.	Every DoDEA system that has been authorized or approved is reassessed on the appropriate schedule.	