# DoDEA Administrative Instruction 8500.01

# DoDEA Cybersecurity Program

| | |
|---|---|
| **Originating Division:** | Information Technology |
| **Effective:** | October 28, 2019 |
| **Releasability:** | Cleared for public release. Available on the DoDEA Policy Webpage. |
| **Approved by:** | Thomas M. Brady, Director |

**Purpose:** This Issuance:

- Establishes a Department of Defense Education Activity (DoDEA) Cybersecurity Program in accordance with DoD Instruction 8500.01 to protect and defend DoDEA information and information technology (IT), including platform IT (PIT).

- Establishes the positions of the DoDEA Authorizing Official (AO) (formerly known as Designated Accrediting Authority) and the DoDEA Senior Information Security Officer (SISO) (formerly known as Senior Information Assurance Officer).

- Adopts the term "cybersecurity" as it is defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23 to be used throughout DoDEA instead of the term "information assurance (IA)."

# TABLE OF CONTENTS

FIGURES

# SECTION 1: GENERAL ISSUANCE INFORMATION

**1.1. APPLICABILITY.** This Issuance applies to:

a. 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. Personnel affiliated with other DoD Components whose systems are hosted at a DoDEA data center, and vendors who provide direct support to DoDEA-hosted IT.

c. 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.

d. DoDEA PIT includes Facility-Related Control Systems, also referred to as Industrial Control Systems (ICSs), such as, but not limited to, physical access control systems, fire alarm and suppression systems, building lighting control systems, and heating, ventilation, and air conditioning (HVAC) systems.

e. DoDEA information in electronic format.

**1.2. POLICY.** It is DoDEA policy that:

a. The DoDEA Cybersecurity Program will comply with DoD Instruction 8500.01.

b. DoDEA-funded IT and PIT will be governed by the DoDEA Cybersecurity Program that manages risk commensurate with the importance of DoDEA missions and the value of potentially affected information or assets.

c. Cybersecurity must be fully integrated into system life cycles and will be a visible element of organizational, joint, and DoDEA IT portfolios.

d. Interconnections of DoDEA IT and PIT, including interconnections with other DoD Components, will be managed to minimize shared risk by ensuring that the security posture of one (1) system is not undermined by vulnerabilities of interconnected systems.

e. DoDEA information in electronic format will be assigned an appropriate level of confidentiality, integrity, and availability that reflects the importance of both information sharing and protection in accordance with the Committee on National Security Systems Instruction (CNSSI) 1253; the Federal Information Processing Standards (FIPS) Publication (PUB) 199; FIPS PUB 200; and Volume 1 and 2 of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60.

f. DoDEA Information Systems (ISs) will be public key-enabled, except for those ISs approved for access by the general public.

g. Cybersecurity workforce functions must be identified, managed, and appropriately screened in accordance with DoD Manual 5200.02, and qualified in accordance with DoD Directive 8140.01 and DoD Manual 8570.01-M.

h. Nothing in this Issuance alters or supersedes the existing authorities and policies of the DoD Chief Information Officer (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 DoD Component Head responsibilities established in DoD Instruction 8500.01.

b. Appoints a trained and qualified AO in writing for all DoDEA ISs and PIT systems operating within or on behalf of DoDEA in accordance with DoD Instruction 8500.01. This role must be assigned to government personnel only, and generally will be assigned to the CIO.

**2.2. DODEA CHIEF INFORMATION OFFICER.** The DoDEA CIO:

a. Complies with the DoD Component CIO responsibilities established in DoD Instruction 8500.01.

b. Ensures that IT under DoDEA purview complies with this Issuance and application of DoD, Committee on National Security Systems (CNSS), and Office of Management and Budget (OMB) issuances and all applicable Executive Orders.

c. Develops, implements, maintains, and enforces a DoDEA Cybersecurity Program that is consistent with the strategy and direction of the DoD SISO and the DoD Cybersecurity Program, and compliant with this Issuance.

d. Ensures that an annual assessment of the DoDEA Cybersecurity Program is conducted.

e. Ensures that IT-related contracts, Memoranda of Agreement (MOAs), and Memoranda of Understanding (MOUs) include specific requirements to provide cybersecurity for DoDEA information and the IT used to process that information in accordance with this Issuance.

f. Ensures all personnel with access to DoDEA IT are appropriately cleared and qualified under the provisions of DoD Instruction 5200.02. DoDEA will provide additional cybersecurity orientation, training, and awareness programs to reinforce the objectives of the DoD enterprise cybersecurity awareness programs to authorized users of ISs. This includes conducting additional in-depth training on DoDEA-specific topics.

g. Appoints personnel occupying cybersecurity positions in writing and ensures they maintain compliance with Section 3.2.b. of this Issuance.

h. Appoints the DoDEA SISO to direct and coordinate the DoDEA Cybersecurity Program.

i. Ensures cybersecurity training and awareness products developed by Defense Information Systems Agency (DISA) will be used to meet the baseline user awareness training required by DoD Directive 8140.01. DoDEA will provide additional cybersecurity orientation, training, and awareness programs to reinforce the objectives of the DoDEA Enterprise cybersecurity awareness programs to authorized users of ISs. This includes conducting additional in-depth training on DoDEA Component-specific topics.

j. Ensures vulnerability assessments and scheduled and unscheduled penetration (PEN) tests are conducted to provide a systemic view of the DoDEA enclave and IS cybersecurity posture.

k. Ensures DoDEA IS contingency plans are developed and exercises conducted to recover IS services following an emergency or IS disruption using guidance found in the NIST SP 800-34.

l. Ensures that all DoDEA IT complies with applicable DISA Security Technical Information Guides (STIGs), security configuration guides, and Security Requirements Guides (SRGs) with any exceptions documented and approved by the responsible AO.

m. Partners with DoDEA procurement executives to ensure that all IT is acquired in accordance with DoDEA Administrative Instruction 8510.01 and that program risk relating to the development of cybersecurity requirements is assessed, communicated to the Milestone Decision Authority and managed early in the system development life cycle, in accordance with DoD Instruction 5000.02.

n. Develops and implements an incident response plan, that is consistent with the requirements of DoD Instruction 8500.01.

**2.3. DODEA SENIOR INFORMATION SECURITY OFFICER.** The DoDEA SISO:

a. Directs and coordinates the DoDEA Cybersecurity Program and, as delegated, carries out the DoDEA CIO responsibilities pursuant to Section 3544 of Title 44, United States Code.

b. Ensures that DoDEA IT is assigned to, and governed by, a DoDEA Cybersecurity Program.

c. Provides guidance and oversight in the development, submission, and execution of the DoDEA Cybersecurity Program budget and advocates for DoDEA-wide cybersecurity solutions throughout the planning, programming, budget, and execution process.

d. Establishes and oversees a team of cybersecurity professionals qualified in accordance with DoD Directive 8140.01, responsible for conducting security assessments. The DoDEA SISO may task, organize, staff, and centralize or direct assessment activities to representatives, as appropriate. Regardless of the adopted model, the DoDEA SISO is responsible for assessing quality, capacity, visibility, and effectiveness.

e. Tracks the assessment and authorization status of ISs governed by the DoDEA Cybersecurity Program.

f. Serves as the single cybersecurity coordination point for joint or DoDEA-wide programs that are deploying information technologies to DoDEA enclaves.

**2.4. DODEA AUTHORIZING OFFICIAL.** The DoDEA AO:

a. Ensures that, for DoDEA ISs under their purview, cybersecurity-related positions are identified in the DoDEA manpower structure in accordance with DoD Directive 8140.01 and DoD 8570.01-M.

b. Ensures appointees to cybersecurity-related positions are given a written statement of cybersecurity responsibilities.

c. Renders authorization decisions for DoDEA ISs under their purview in accordance with DoD Instruction 8510.01.

d. Establishes guidance for and oversees IS-level risk management activities consistent with DoD policy, DoDEA guidance, and direction.

**2.5. DODEA INFORMATION SYSTEM OWNERS.** The DoDEA Information System Owners (ISOs):

a. Plan and budget for security control implementation, assessment, and sustainment throughout the system life cycle, including timely and effective configuration and vulnerability management.

b. Ensure that Systems Security Engineering (SSE) is used to design, develop, implement, modify, and test and evaluate the system architecture in compliance with the cybersecurity component of the DoD Enterprise Architecture in accordance with DoD Directive 8000.01, following the guidance of NIST SP 800-160.

c. Ensure authorized users and support personnel receive appropriate cybersecurity training.

**2.6. DODEA INFORMATION SYSTEM SECURITY MANAGERS.** The DoDEA Information System Security Managers (ISSMs):

a. Develop and maintain an organizational or system-level cybersecurity program that includes cybersecurity architecture, requirements, objectives and policies, cybersecurity personnel, and cybersecurity processes and procedures.

b. Ensure that Information Owners (IOs) and stewards associated with DoDEA information received, processed, stored, displayed, or transmitted on each DoDEA IS and PIT system are identified in order to establish accountability, access approvals, and special handling requirements.

c. Maintain a repository for all organizational or system-level cybersecurity-related documentation.

d. Ensure that DoDEA Information System Security Officers (ISSOs) are appointed in writing and provide oversight to ensure that they are following established cybersecurity policies and procedures.

e. Monitor compliance with cybersecurity policy, as appropriate, and review the results of such monitoring.

f. Ensure that cybersecurity inspections, tests, and reviews are synchronized and coordinated with affected parties and organizations.

g. Ensure implementation of IS security measures and procedures, including reporting incidents to the SISO and appropriate reporting chains and coordinating system-level responses to unauthorized disclosures in accordance with Volume 3 of DoD Manual 5200.01 for classified information or Volume 4 of DoD Manual 5200.01 for controlled unclassified information (CUI).

h. Ensure the handling of possible or actual data spills of classified information resident in ISs are conducted in accordance with Volume 3 of DoD Manual 5200.01.

i. Act as the primary cybersecurity technical advisor to the SISO for DoDEA IS and PIT systems under their purview.

j. Ensure that cybersecurity-related events or configuration changes that may impact DoDEA IS and PIT systems authorization or security posture are formally reported to the SISO and other affected parties, such as ISOs and stewards and AOs of interconnected DoDEA ISs, within 72 hours.

## 2.7. DODEA INFORMATION SYSTEM SECURITY OFFICERS. The DoDEA ISSOs:

a. Assist the DoDEA ISSMs in meeting their duties and responsibilities.

b. Implement and enforce all DoDEA IS and PIT system cybersecurity policies and procedures, as required for Authorizations to Operate (ATOs).

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

d. Initiate protective or corrective measures, in coordination with the DoDEA ISSM, when a cybersecurity incident or vulnerability is discovered and ensure that a process is in place for authorized users to report all cybersecurity-related events and potential threats and vulnerabilities to the DoDEA ISSO.

e. Ensure all DoDEA IS cybersecurity-related documentation is current and accessible to properly authorized individuals.

# SECTION 3: CYBERSECURITY PROGRAM PROCESS

**3.1. GENERAL INFORMATION.** The purpose of the DoDEA Cybersecurity Program is to ensure that IT and PIT can be used in a way that allows mission owners and operators to have confidence in the confidentiality, integrity, and availability of IT, PIT, and DoDEA information, and to make choices based on that confidence. The DoDEA Cybersecurity Program supports a vision of effective operations in cyberspace where:

a. DoDEA missions and operations continue under any cyber situation or condition.

b. DoDEA continues in its goal to comply with the Data Center Optimization Initiative (for more information go to https://datacenters.cio.gov by combining all enterprise systems and services into a single data center.

## 3.2. PERSONNEL.

a. The DoDEA Director, CIO, AO, and SISO must be U.S. citizens and DoDEA officials with the authority to formally assume responsibility for operating DoDEA ISs or PIT systems at an acceptable level of risk to DoDEA operations (including mission, functions, image, or reputation), DoDEA assets, and individuals.

b. All personnel occupying cybersecurity positions must be:

(1) Trained and qualified in accordance with DoD Directive 8140.01 and DoD 8570.01-M.

(2) Assigned a position designation using the criteria found in DoD Instruction 5200.02. The position designation will be documented in the Defense Civilian Personnel Data System (DCPDS).

(3) In compliance with the associated suitability and fitness requirements.

**3.3. CYBERSECURITY.** Cybersecurity makes data ubiquitously accessible while simultaneously restricting access, promotes the safe sharing of information, and prevents attacks by having network protections in place. It provides authorized, authenticated user access without impact from rogue entities, 'hacktivists', nation states, or insider threats.

**a. Cybersecurity Risk Management.** Cybersecurity risk management is a subset of the overall risk management process for all DoDEA acquisitions as defined in DoD Instruction 5000.02, which includes cost, performance, and schedule risk associated with the execution of all programs of record, and all other acquisitions of DoDEA. The risk assessment process extends to the logistics support of fielded equipment and the need to maintain the integrity of supply sources. DoDEA will follow DoDEA Administrative Instruction 8510.01 to address risk management, including issuance of ATOs, for all DoDEA ISs and PIT systems.

**b. Integrated Organization-Wide Risk Management.** Risk management can be viewed as a holistic activity that is fully integrated into every aspect of the organization. In accordance with Enclosure 3 of Section 2 of DoD Instruction 8500.01, DoDEA will follow the DoD Risk Management Framework (RMF) three-tiered approach to risk management that addresses risk-related concerns.

(1) Tier 1: Organization. Tier 1 addresses risk from the DoD perspective and is informed and influenced by risk decisions made in Tier 2.

(2) Tier 2: Mission and Business Processes. Tier 2 addresses risk from the DoDEA mission and business process perspective and is guided by the risk decisions at Tier 1, and informed and influenced by risk decisions made in Tier 3.

(3) Tier 3: Information Systems and Platform Information Technology Systems. Tier 3 addresses risk from the individual DoDEA IS and PIT system perspective and is guided by the risk decisions at Tiers 1 and 2.

(a) Though the need for specific protections is identified at Tiers 1 and 2, it is at Tier 3 where the information protections are applied to the system and its environment of operation for the benefit of successfully enabling mission and business success.

(b) Information protection requirements are satisfied by the selection and implementation of appropriate security controls in NIST SP 800-53.

**c. Risk Management in the System Development Life Cycle.** Risk management tasks begin early in the System Development Life Cycle (SDLC) and are important in shaping the security capabilities of the IS. If these tasks are not adequately performed during the initiation, development, and acquisition phases of the SDLC, the tasks will, by necessity, be undertaken later in the life cycle and will be more costly and time consuming to implement, and could negatively impact the performance of the IS.

**d. Risk Management Framework.** DoDEA uses DoD Instruction 8510.01 as implemented by DoDEA Administrative Instruction 8510.01, which is applicable to all DoDEA ISs and PIT systems. 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 DoDEA. The RMF has six (6) steps: Categorize system, select security controls, implement security controls, assess security controls, authorize system, and monitor security controls.

**e. Risk Assessment.** Risk assessment is a key step in the DoDEA risk management process. Risk assessments will be performed in accordance with the process in NIST SP 800-30, with all of the described risk factors used across DoDEA to ensure ease of sharing risk information. The robustness of the risk assessments may be tailored to accommodate resource constraints and the availability of detailed risk factor information (e.g., threat data). Any tailoring must be clearly explained in risk assessment reports to ensure the AOs understand to what degree they can rely on the results of the risk assessments.

**f. Security Controls.**

(1) In accordance with Enclosure 3 of Section 2.g. of DoD Instruction 8500.01, DoDEA will follow CNSSI 1253 for IT categorization, and will implement a corresponding set of security controls that are published in NIST SP 800-53.

(2) DoDEA will implement a baseline minimum security control set for single-user educational software, web applications, and Remote Desktop Services (RDS) applications in accordance with DoDEA Administrative Instruction 8510.01.

**g. Cybersecurity Service Provider.** All DoDEA IS, regardless of hosting location or supporting network (excluding the headquarters location at the Mark Center), must align to a single DoD-certified Cybersecurity Service Provider (CSSP) to ensure protection, detection, response, and sustainment services are provided for the protection of all DoDEA information twenty-four (24) hours a day, seven (7) days a week. CSSP alignment ensures the ability to detect, isolate, and react to intrusions, disruption of services, or other incidents that threaten the security or function of DoDEA operations, DoDEA IS, or networks.

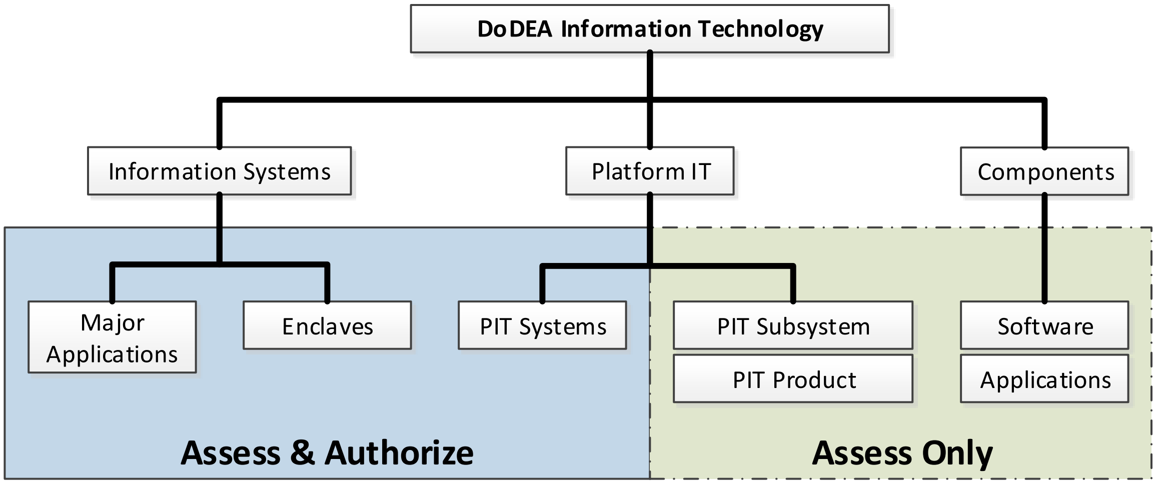
**3.4. ASSESSMENT AND AUTHORIZATION APPROACHES.** DoD Instruction 8510.01 allows for two (2) approaches for IT assets to be operationally allowed:

**a. Assess and Authorize.** With respect to definitions of DoD IT types in DoD Instruction 8500.01, DoDEA will utilize the Assess and Authorize (A&A) process for ISs, and PIT systems. Systems subject to A&A must follow all steps of the RMF process as identified in DoD Instruction 8510.01. It is important to note that, although the NIST SP 800-18 separates IT systems into major applications, general support systems (GSS), and minor applications, being a component of DoD, DoDEA will follow DoD guidelines on system definition. All IT systems that follow the A&A process must obtain their own discrete ATO.

**b. Assess Only.** DoDEA IT that qualifies for Assess Only are not authorized to operate (see RMF Step 5 of DoD Instruction 8510.01), but must be approved for installation on or to be utilized by a system that has obtained an ATO through the A&A process. The DoDEA IT assets eligible for Assess Only include some PIT (e.g., ICS), software, and applications.

**3.5. INFORMATION TECHNOLOGY.** In accordance with Section 11101 of Title 40, United States Code, DoDEA defines IT as any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by DoDEA, if the equipment is used by DoDEA directly or is used by a contractor under a contract with DoDEA that requires the use of that equipment. IT includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware, and similar procedures, services (including support services), and related resources. Cybersecurity applies to all IT, as shown in Figure 1: DoDEA IT of this Issuance.

**Figure 1: DoDEA IT**



**a. Information Systems.** Pursuant to Appendix III to OMB Circular No. A-130; DoD Instruction 8500.01; and Section 3502 of Title 44, United States Code, DoDEA defines an IS as 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. For purposes of authorization and registration, minor (micro) and web applications are not considered systems; they are to be included in the authorization boundary of their host system, the RDS Server or the Web Application Server, respectively. In accordance with DoD Instruction 8500.01, IT ranges in size and complexity from individual hardware and software products to stand-alone systems to massive computing environments, enclaves, and networks. ISs are organized in one (1) of the following three (3) forms; only the first two (2) forms require the full A&A process:

(1) Information Systems Enclave. An enclave is an interconnected set of information resources under the same direct management control that shares common functionality. Enclaves provide standard cybersecurity, such as boundary defense, incident detection and response, and key management, and also deliver common applications, such as office automation and electronic mail. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Both OMB Circular No. A-130 and NIST SP 800-18 utilize the term GSS instead of the DoD IS Enclave. Any Federal authoritative source reference to GSS will be analogous to a reference to a DoDEA IS Enclave.

(2) Major Applications. In accordance with DoD Instruction 8500.01 and NIST SP 800-18, these are defined as applications that require 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.

(3) Minor (Micro) Application. DoDEA will follow NIST SP 800-18 and DoD Instruction 8500.01 guidance with respect to minor applications. NIST categorizes a minor

application as any 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. The April 2017 Under Secretary of Defense (Comptroller)/Chief Financial Officer Guidance regarding Financial Improvement Audit Readiness (FIAR) defines micro applications as spreadsheets, databases, and/or other automated tools used to perform reconciliations, calculations, or other business functions. Further, any Federal authoritative source reference to minor applications will be inclusive of DoDEA micro applications. Examples of minor applications would be the various web applications as well as the Microsoft Access database programs hosted on the RDS system, currently referred to as Micro Applications.

**b. Platform Information Technology.** PIT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as diagnostic test and maintenance equipment, calibration equipment, medical technologies, transport vehicles, buildings, and utility distribution such as water and electric. In accordance with Enclosure 3 of Section 9.(2)(b) DoD Instruction 8500.01, the only platforms within DoDEA are buildings.

(1) Platform Information Technology System. PIT systems are 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. They are analogous to enclaves but are dedicated only to the platforms they support. These systems either have their controller external to the platform, have internet or DoDEA intranet access, or the control is server-based (not embedded). PIT systems must follow the full A&A process.

(2) Platform Information Technology Subsystem. A collection of PIT products that does not rise to the level of a PIT system as determined by the system owner, in consultation with and subject to the approval of the authorizing official. PIT Subsystems follow the Assess Only process and may be integrated into a PIT system.

(3) Platform Information Technology Product. These are individual PIT Components, either hardware or software. Common forms of building PIT Products are ICSs, such as supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and programmable logic controllers (PLCs). The implementation of these devices is internal to the platform and does not connect to the DoDEA network or the internet. Building PIT Products follow the Assess Only process.

**c. Information Technology Components.**

(1) Software. Within DoDEA, this type is specifically relating to workstation-installed software, such as student educational programs.

(2) Applications. In accordance with OMB Circular No. A-130 and NIST SP 800-37, an application is defined as an information resource (information and information technology) hosted by an IS used to satisfy a specific set of user requirements. For DoDEA, this would cover the various individual web applications and the micro apps hosted by the RDS server. According to NIST 800-18, these applications are classified as minor applications, and unless there are

compelling reasons, minor applications will not be assessed and authorized independently. Instead, minor applications are either a supported component of an enclave or a module of a major application.

## 3.6. DODEA FUNDED INFORMATION SYSTEMS.

**a. Overview.** DoDEA funds various ISs to support its mission, that may include, but are not limited to, desktop computers, thin-client and fat-client technology, laptops, servers (stand-alone and rack-mounted), printers, routers, firewalls, switches, tablets, and smartphones. To accomplish this mission, network and/or standalone ISs are funded for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of DoDEA-related information supporting DoDEA and its subcomponents. DoDEA prohibits the direct connection of ISs to an external network without the use of DoD-approved boundary protection devices (e.g., router, firewalls). All DoDEA funded IT must be configured as follows, where applicable:

(1) User-Based Enforcement (UBE) of Public Key Infrastructure (PKI).

(2) Full deployment of DoD mandated Host Based Security System (HBSS).

(3) Full deployment of DoD mandated Assured Compliance Assessment Solution (ACAS).

(4) Application of all applicable DISA STIGs or SRGs to all hardware and software components.

(5) Registration of all Ports, Protocols, and Services utilized by an IS in the DISA Ports, Protocols, and Services Management system (PPSM).

(6) Demilitarized zone (DMZ) whitelist registration of all File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and Web services.

**b. Audit and Accountability.** All DoDEA ISs and network components must enable auditing whenever possible, and the generated audit logs made available to the DoDEA Security Information and Event Management (SIEM) solution. Audit log files are a critical resource in the incident response process and must be protected from accidental or intentional modification or deletion. The principles of least privileges must be followed when authorizing user access to audit logs. Only those Microsoft Windows accounts explicitly granted the "Manage auditing and security log" user rights are allowed full access to audit logs. This user right must be removed from all other privileged accounts, or changed to read-only.

(1) Audit Events. All DoDEA ISs must follow auditing guidelines provided by the appropriate DISA STIG. At a minimum, DoD requires the following audit events:

(a) Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels).

(b) Successful and unsuccessful logon attempts.

(c) Privileged activities or other system level access.

(d) Starting and ending time for user access to the system.

(e) Concurrent logons from different workstations.

(f) Successful and unsuccessful accesses to objects.

(g) All program initiations.

(h) All direct access to the IS.

(i) All account creations, modifications, disabling, and terminations.

(j) All kernel module load, unload, and restart.

(2) Content of Audit Records. All DoDEA IS audit records, at a minimum, should contain the following elements:

(a) Date and time when the event occurred.

(b) The software or hardware component of the IS where the event occurred.

(c) Source of the event (e.g., network address, console).

(d) Type of event that occurred.

(e) Subject identity (e.g., user, device, process context).

(f) The outcome (i.e., success or failure) of the event.

(g) Security-relevant actions associated with processing.

(3) Response to Audit Processing Failure. At a minimum, the DoDEA IS must immediately notify the DoDEA Security Control Assessor (SCA), DoDEA ISSO, and DoDEA Security Operations Center (SOC) in the event of an audit processing failure. If the failure is due to the current audit log file being full, the system must be configured to overwrite the oldest records in order to continue auditing the system.

(4) Audit Storage Capacity. In accordance with DoD requirements, at a minimum, the DoDEA IS must immediately notify the DoDEA ISSO/Program Management Office (PMO) and ISSM when the allocated audit storage volume reaches seventy-five percent (75%) of the maximum capacity.

(5) Audit Review, Analysis, and Reporting. Audit records must be reviewed at least every seven (7) calendar days, or more frequently if required by an alarm event or anomaly. The review should include identification of any inappropriate or unusual activity, assurance that

logging is functioning properly, and there is adherence to logging standards identified in this Issuance. The IS should have the capability of providing audit reports on demand in support of incident response. The results of the review should be reported to the DoDEA ISO, ISSO, ISSM, and the Incident Response Team, if appropriate.

(6) Audit Reduction and Report Generation. The DoDEA IS must provide an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents and does not alter the original content or time ordering of audit records.

(7) Time Stamps. All DoDEA IS must be configured to use internal system clocks to generate time stamps for audit records and to record time stamps that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets the tolerance required to ensure authentication with the domain controllers.

(8) Audit Record Retention. Audit records must be backed up at least weekly to a different system or media than the system being audited. All DoDEA audit records must be retained for at least one (1) year to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

(9) Audit Record Availability. Where feasible, the audit records from all servers and network components must be available to the SIEM for compilation into a system-wide audit trail.

**c. Removable Storage Media.** In accordance with CNSSI 4009, DoDEA defines removable storage media to include universal serial bus (USB) flash drives, memory cards, external hard drives, and writeable compact discs (CDs) or digital versatile discs (DVDs).

(1) General Requirements. HBSS installation is required on all Microsoft Windows machines that will utilize removable storage media. Additionally, DoDEA removable storage media:

(a) Must be on the approved product lists.

(b) Must be DoDEA-purchased and controlled; no personal devices are allowed.

(c) Must only be used with DoDEA-owned computers and peripheral devices.

(d) Must be scanned for vulnerabilities when connected to a DoDEA-owned computer.

(2) Secure Digital Cards. Secure Digital (SD) cards are approved for curricular use (e.g., classroom use), with faculty being accountable for their proper use. All other requirements within DoDEA must receive approval from the DoDEA CIO prior to being used. All uses of SD cards are subject to the General Requirements in Section 3.5.c.(1) of this Issuance, and the following:

(a) Will be purchased from a General Services Administration (GSA) approved source.

(b) Will only contain curricular or DoDEA data.

(c) Will only contain the audio, video, and image files in the following formats as show in Figure 2: Authorized File Formats for SD Cards of this Issuance:

**Figure 2: Authorized File Formats for SD Cards**

| Video File Formats | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| .3g2 | .3gp | .asf | .avchd | .avi | .f4a | .f4b | .f4p | .f4v |
| .flv | .m4p | .m4v | .mov | .mp2 | .mp4 | .mpe | .mpeg | .mpg |
| .mpv | .mts | .nsv | .qt | .rm | .swf | .vob | .webm | .wmv |

| Audio File Formats | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| .3gp | .aac | .aax | .cda | .cfa | .flac | .m4a | .mp4 | .mp3 |
| .pek | .wav | .wma | | | | | | |

| Image File Formats | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| .3ds | .bmp | .crw | .dng | .eps | .gif | .jpeg | .jpg | .nef |
| .nrw | .pdf | .png | .psd | .raw | .tif | .tiff | | |

(3) Universal Serial Bus-Connected Removable Media. Excluding USB-connected SD card readers, these devices must adhere to the General Requirements in Section 3.5.c.(1) of this Issuance, and the following:

(a) All removable storage media must be on the Approved Products List. The removable storage must be registered in HBSS.

(b) The automatic execution of any content by a removable media device is prohibited unless specifically authorized by the DoDEA AO.

(c) Auto-run feature must be disabled on all client machines.

(d) Devices must be encrypted in accordance with FIPS 140-2 requirements.

(e) Devices must be properly labeled with data classification, and serial and identification, when available.

## 3.7. DODEA FUNDED SOFTWARE.

**a. Commercial Off-the-Shelf Software.** In accordance with DoD Instruction 8500.01, DoDEA will comply with the Application Security and Development (AS&D) STIG that prohibits the use of operating systems and/or applications that are no longer supported with security patches and upgrades by the developer, vendor, or manufacturer. This includes public-domain software, other software products with limited or no warranty (i.e., freeware or shareware), and Peer-to-Peer (P2P) file sharing software.

**b. Government Off-the-Shelf Software.** DoDEA-funded U.S. Government off-the-shelf software (GOTS) software, also known as custom software, includes both software developed in-house, and software developed under contract at the contractor's facility. This category of software also includes commercial off-the-shelf (COTS) software that is modified to meet DoDEA requirements. GOTS software must comply with all the requirements in the AS&D STIG.

**c. Open Source Software.** Open Source Software (OSS) refers to software that is available in source code form. Certain software rights normally reserved for copyright holders are routinely provided under software license agreements that permit individuals to study, change, and improve the software. From a security perspective, the major advantage of OSS is that it provides organizations with the ability to examine the source code for possible vulnerabilities. The continuous and broad peer-review of OSS improves software security through the identification and elimination of defects that might otherwise go unrecognized by a more limited development team. Authorized use of OSS to support DoDEA missions must include the ability to review, repair, and extend software support by commercial or U.S. Government program offices. All DoDEA authorized use of OSS must include bidirectional access controls restricting network traffic to use of DoD-approved ports, protocols, and services.

**d. IA and IA-Enabled Software.** The acquisition by DoDEA of COTS, GOTS, or OSS that performs an IA function, or is IA-enabled, will be in accordance with CNSS Policy No. 11.

**e. Exceptions.** Any exceptions to these software restrictions must be explicitly approved by the AO. To obtain an exception, the following must be submitted to the AO:

(1) A complete risk assessment, in accordance with NIST SP 800-30.

(2) A written justification for use of the software, including comparison of alternative products.

(3) A completed DoDEA Form 8510, "Risk Acceptance Form," available from DoDEA IT.

## 3.8. MOBILE CODE USAGE.

**a. Overview.** Mobile code is defined as software programs or parts of programs obtained from remote ISs, transmitted across a network, and executed on a local IS without explicit installation or execution by the recipient. Examples of mobile code include such technologies as Java, JavaScript, ActiveX, .NET Common Language Runtime, Windows Scripting Host, Hypertext Markup Language (HTML) Application Host, and VBScript. DoD has established several categories of risk associated with mobile code technology that are based on functionality, level of access to workstation, server, and remote system services and resources, and the resulting threat to ISs.

**b. Risk Categories.** In accordance with the March 14, 2011 DoD CIO Memorandum, the risk categories are:

(1) Category 1. Allows unmediated access to the workstation, server, and remote system services and resources. There are two (2) subcategories:

(a) Category 1A. This consists of mobile code technologies that differentiate between signed and unsigned mobile code and is configured to allow execution of signed code while simultaneously blocking the execution of unsigned mobile code. The mobile code must be signed with a DoD code-signing certificate or has been designated as trusted by DoDEA. Examples of Category 1A code include, but are not limited to ActiveX controls, JavaScript, VBScript, and browser ActiveX runtime implementation.

(b) Category 1X. This consists of those mobile code technologies that are prohibited from being used in DoDEA ISs because they cannot differentiate between signed and unsigned mobile code or cannot be configured to block the execution of unsigned mobile code while enabling the execution of signed mobile code. Examples of Category 1X code include, but are not limited to HTML applications that download as mobile code, Scrap objects (e.g., .shs and .shb files), Microsoft Disk Operating System (MS-DOS) batch scripts, Unix/Linux shell scripts, and Shockwave movies.

(2) Category 2. This type of mobile code has full functionality, allowing mediated or controlled access to the workstation, server, and remote system services and resources. Unsigned Category 2 mobile code that executes in a constrained execution environment without access to local system and network resources is allowed. Category 2 mobile code that does not execute in a constrained execution environment may only be used if it is digitally signed with a DoD code-signing certificate or the code was downloaded using secure communications protocol from a trusted Web server. Examples of Category 2 code include, but are not limited to Java applets, Visual Basic applications (Microsoft Office macros), .NET Common Runtime language, Portable Document Format (PDF), and Flash animations (e.g., .swf and .spl files) that execute in the Shockwave Flash Plugin.

(3) Category 3. This category supports limited functionality, with no capability for unmediated access to the workstation, server, or remote system services and resources and is allowed. Both JavaScript and VBScript when executing in the browser are included in this category and are allowed in DoDEA systems.

(4) Emerging Mobile Code Technologies. Because of the uncertain risk, the use of emerging mobile code technologies in DoDEA ISs is prohibited.

(5) Mobile Code in E-mail. Due to the significant risk of malicious mobile downloading into user workstations via e-mail, the automatic execution of all categories of mobile code in e-mail bodies and attachments shall be disabled.

**c. Exclusions.** The above categorizations and prohibitions do not apply to script and applets that execute in the context of a Web server. Examples of technologies include Java servlets, Java Server Pages, Common Gateway Interface (CGI), Active Server Pages (ASP); ASP.NET Pages, ColdFusion Markup Language (CFML), PHP:  Hypertext Preprocessor (PHP), Server Side Includes (SSI), and server-side JavaScript.

**3.9. ENCRYPTION.** In accordance with CNSS Policy No. 11, all IA and IA-enabled systems/devices must be compliant with the requirements of the National Information Assurance Partnership (NIAP) program.  In the absence of a NIAP-approved profile, any system/device that relies on cryptography must utilize a cryptography module that has been certified in accordance with the FIPS 140-2 Cryptographic validation program(s).

**a. Data in Transit.** With the exception of network traffic to and from unsecure, public web sites that utilize the hypertext transport protocol (HTTP) over port 80, all DoDEA data in transit will utilize encrypted, secure protocols, leveraging the DoD PKI and DoD-issued Secure Hash Algorithm-256 (SHA-256) Secure Sockets Layer (SSL) certificates.  This requirement not only applies to communications with external entities (excluding public websites as noted), but also applies to all internal network traffic.

**b. Data at Rest.** Data at rest (DAR) is inactive data which is stored physically in any digital form (e.g., databases, data warehouses, spreadsheets, archives, tapes, off-site backups, mobile devices, etc.).  DAR includes, but is not limited to, archived data, data which is not accessed or changed frequently, files stored on hard drives (both internal and external), USB thumb drives, SD cards, files stored on backup tape and disks, and files stored off-site or on a storage area network.

**c. Mobile Devices.** All unclassified DoD data that has not been approved for public release and is stored on mobile computing devices or removable storage media must be encrypted using commercially available encryption technology.  This requirement includes all CUI, For Official Use Only (FOUO), and other unclassified information that has not been reviewed and approved for public release.  This requirement specifically applies to Personally Identifiable Information (PII) and Protected Health Information (PHI).

**d. Web Servers.** DAR for a web server is data on the hosting system storage devices.  Data stored as a backup on tape or stored off-site is no longer under the protection measures covered by the web server.  There are several pieces of data that the web server uses during operation.  The web server must use an accepted encryption method, such as Advanced Encryption Standard (AES) or Rivest-Shamir-Adleman (RSA), to protect the confidentiality and integrity of the information.  All DoDEA web sites, regardless of hosting location, must utilize DoD-issued SHA-256 SSL server certificates; self-signed certificates are prohibited.

# GLOSSARY

## G.1. ACRONYMS.

| | |
|---|---|
| A&A | assess and authorize |
| AES | Advanced Encryption Standard |
| ACAS | Assured Compliance Assessment Solution |
| AO | Authorizing Official |
| AS&D | Application Security and Development |
| ASP | Active Server Pages |
| ATO | Authorization to Operate |
| | |
| CD | compact disc |
| CFML | ColdFusion Markup Language |
| CGI | Common Gateway Interface |
| CIO | Chief Information Officer |
| CNSS | Committee on National Security Systems |
| CNSSI | Committee on National Security Systems Instruction |
| COTS | commercial off-the-shelf |
| CSSP | Cybersecurity Service Provider |
| CUI | controlled unclassified information |
| | |
| DAR | data at rest |
| DCPDS | Defense Civilian Personnel Data System |
| DCS | distributed control system |
| DISA | Defense Information Systems Agency |
| DMZ | demilitarized zone |
| DVD | digital versatile disc |
| | |
| FIAR | Financial Improvement and Audit Readiness |
| FIPS | Federal Information Processing Standard |
| FOUO | For Official Use Only |
| FTP | File Transfer Protocol |
| | |
| GMT | Greenwich Mean Time |
| GOTS | government off-the-shelf |
| GSA | General Services Administration |
| GSS | general support system |
| | |
| HBSS | Host Based Security System |
| HTML | Hypertext Markup Language |
| HTTP | Hypertext Transfer Protocol |
| HVAC | heating, ventilation, and air conditioning |
| | |

| | |
|---|---|
| IA | information assurance |
| ICS | industrial control system |
| IO | Information Owner |
| IS | information system |
| ISO | Information System Owner |
| ISSM | Information System Security Manager |
| ISSO | Information System Security Officer |
| IT | information technology |
| | |
| MOA | memorandum of agreement |
| MOU | memorandum of understanding |
| MS-DOS | Microsoft Disk Operating System |
| | |
| NIAP | National Information Assurance Partnership |
| NIST | National Institute of Standards and Technology |
| | |
| OMB | Office of Management and Budget |
| OSS | open source software |
| | |
| P2P | peer-to-peer |
| PDF | Portable Document Format |
| PEN | penetration |
| PHI | protected health information |
| PHP | PHP: Hypertext Preprocessor |
| PII | personally identifiable information |
| PIT | platform information technology |
| PKI | public key infrastructure |
| PLC | programmable logic controller |
| PMO | Program Management Office |
| PPSM | ports, protocols, and services management |
| PUB | Publication |
| | |
| RDS | Remote Desktop Server |
| RMF | Risk Management Framework |
| RSA | Rivest-Shamir-Adleman |
| | |
| SCA | Security Control Assessor |
| SCADA | supervisory control and data acquisition |
| SD | Secure Digital |
| SDLC | system development life cycle |
| SHA-256 | Secure Hash Algorithm 256 |
| SIEM | security information and event management |
| SISO | Senior Information Security Officer |
| SMTP | Simple Mail Transfer Protocol |
| SOC | Security Operations Center |

| | |
|---|---|
| SP | Special Publication |
| SRG | Security Requirements Guide |
| SSE | systems security engineering |
| SSI | Server Side Includes |
| SSL | Secure Sockets Layer |
| STIG | Security Technical Implementation Guide |
| | |
| UBE | user-based enforcement |
| USB | Universal Serial Bus |
| UTC | Coordinated Universal Time |

**G.2. DEFINITIONS.** Unless otherwise noted, these terms and their definitions are for the purpose of this Issuance.

**AO.** As defined in CNSSI 4009, the role responsible for making credible, risk-based decisions regarding the acceptance and use of systems and the information that they process, store, or transmit.

**ATO.** As defined in CNSSI 4009, 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, and encrypted tunnels).

**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.

**GSS.** 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.

**ISO.** As defined in CNSSI 4009, the ISO or program manager is the official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

**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.

**Milestone Decision Authority.** As defined in DoD Instruction 5000.02, the designated individual with overall responsibility for a program. The Milestone Decision Authority shall have the authority to approve entry of an acquisition program into the next phase of the acquisition process and shall be accountable for cost, schedule, and performance reporting to higher authority, including congressional reporting.

**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 are typically included as part of a general support system.

**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.

**privileged user.** As defined in CNSSI 4009, a user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

**removable storage media.** As defined in CNSSI 4009, portable data storage medium that can be added to or removed from a computing device or network. Includes USB flash drives, memory cards, external hard drives, and writeable CD or DVD.

**security controls.** As defined in FIPS PUB 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.

**SRG.** As defined in DoD Instruction 8500.01, a compilation of control correlation identifiers grouped in more applicable, specific technology areas at various levels of technology and product specificity. Contains all requirements that have been flagged as applicable from the parent level regardless if they are selected on a DoD baseline or not.

**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.

# 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

Committee on National Security Systems (CNSS) Policy Number 11, “National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products,” June 10, 2013

DoD Chief Information Officer Memorandum, “Mobile Code Technologies Risk Category Assignment List Update,” March 14, 2011

DoD Directive 8000.01, “Management of The Department of Defense Information Enterprise (DoD IE),” March 17, 2016, as amended

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

DoD Instruction 5000.02, “Operation of the Defense Acquisition System,” January 7, 2015, as amended

DoD Instruction 5200.02, “DoD Personnel Security Program (PSP),” March 21, 2014, 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 Manual 5200.01, Volume 3, “DoD Information Security Program: Protection of Classified Information,” February 24, 2012, as amended

DoD Manual 5200.01, Volume 4, “DoD Information Security Program: Controlled Unclassified Information (CUI),” February 24, 2012, as amended

DoD Manual, 5200.02, “Procedures for the DoD Personnel Security Program (PSP),” April 3, 2017

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

DoDEA Administrative Instruction 8510.01, “Risk Management Framework for DoDEA Information Technology,” October 29, 2019

DoDEA Form 8510, “Risk Acceptance Form,” October 2019

Federal Information Processing Standards Publication 140-2, “Security Requirements for Cryptographic Modules,” May 25, 2001, as amended, located at https://csrc.nist.gov/publications

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

Federal Information Processing Standards Publication 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006, located at https://csrc.nist.gov/publications

National Security Presidential Directive-54/Homeland Security Presidential Directive-23, "Cybersecurity Policy," January 8, 2008

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

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

National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Federal Information Systems," current edition, 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," current edition, 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," current edition 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," current edition, 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," current edition, located at https://csrc.nist.gov/publications

National Institute of Standards and Technology Special Publication 800-160, Volume 1, "Systems Security Engineering:  Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," current edition, located at https://csrc.nist.gov/publications

Office of Management and Budget Circular Number A-130, "Managing Information as a Strategic Resource," current version

Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer Guidance, "Financial Improvement and Audit Readiness (FIAR) Guidance," April 2017, located at http://comptroller.defense.gov/Portals/45/documents/fiar/FIAR_Guidance.pdf

United States Code, Title 40, Section 11101

United States Code, Title 44

# APPENDIX

## APPENDIX 1: INTERNAL CONTROLS EVALUATION CHECKLIST

In accordance with Section 2.2.d. 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.c.** | A trained and qualified AO has been appointed in writing for all DoDEA ISs and PIT systems. | |
| **2.2.e.** | A SISO has been appointed. | |
| **3.2.** | DoDEA is following DoD and DoDEA policy pertaining to risk management. | |
| **3.4.** | DoDEA is properly classifying IT systems and authorizing or approving according to policy. | |
| **3.5.** | DoDEA is following all DoD mandates pertaining to configuration of IT resources, use of mandated software, and systems are in compliance with appropriate STIGs or SRGs. | |
| **3.5.b.** | DoDEA IT resources implement the minimum level of event auditing, where possible. | |
| **3.5.c.** | Use of Removable Storage Media is in accordance with this Issuance. | |
| **3.7.** | DoDEA monitors and ensures only authorized mobile code is in use. | |
| **3.8.** | Ensure all data in transit and at rest is protected by approved encryption techniques. | |