DoDEA Administrative Instruction 5205.03

DoDEA Operations Security Program

Originating Division: Security Management

Effective: August 17, 2018

Releasability: Cleared for public release. Available on the DoDEA Policy Website

Approved by: Thomas M. Brady, Director

Purpose: This Issuance establishes policy, assigns responsibility, and identifies procedures for the Department of Defense Education Activity (DoDEA) operations security (OPSEC) Program.

- This Issuance is designed to meet the Department of Defense requirements recognized in DoD Directive 5205.02E.
- Identifies criteria for the critical information list (CRIL).
- Addresses the need for OPSEC to disrupt aggressors from collecting critical information.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This Issuance applies to the Office of the Director, DoDEA; the Principal Deputy Director and Associate Director for Academics, DoDEA; the Associate Director for Financial and Business Operations, DoDEA; the Chief of Staff, DoDEA; the Director for Student Excellence, DoDEA Americas/Associate Director for Performance and Accountability (formerly the Director, Domestic Dependent Elementary and Secondary Schools, and Department of Defense Dependents Schools, Cuba (DDESS/DoDDS-Cuba)); the Director for Student Excellence, DoDEA Europe (formerly the Director, Department of Defense Dependents Schools, Europe (DoDDS-E)); the Director for Student Excellence, DoDEA Pacific (formerly the Director, Department of Defense Dependents Schools, Pacific, and Domestic Dependent Elementary and Secondary Schools, Guam (DoDDS-P/DDESS-Guam)); (referred to collectively in this issuance as "DoDEA Region Directors for Student Excellence"); and all DoDEA region, district, and community school leadership and support staff.

b. Private companies and personnel employed as contractors.

1.2. POLICY. It is DoDEA policy to identify critical and sensitive unclassified information, assist in risk prioritization, prevention, reduction, and mitigation in accordance with National Security Decision Directive 298 and DoD Directive 5205.02E.

a. DoDEA employees and contractors handle information on a daily basis that contributes to accomplishing the DoD mission.

b. OPSEC is an integral process of force protection (FP), helping protect Service members, civilian employees, contractors, family members, facilities, and equipment at all locations and in all situations.

c. Unclassified information may be critical if aggregated to create a larger picture.

d. This Issuance authorizes the production of additional issuances to support the OPSEC program.

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. Establishes a DoDEA OPSEC Program in accordance with DoD Directive 5205.02E.

b. Appoints, in writing, the DoDEA FP Program Manger as the OPSEC Program Manager.

2.2. DODEA FORCE PROTECTION PROGRAM MANAGER. The FP Program Manager:

a. Serves as the DoDEA OPSEC Program Manager.

b. Ensures OPSEC assessments are conducted, independently or integrated into the FP Assessment, and provides results to the Office of the Under Secretary of Defense (Intelligence).

c. Identifies, assesses, and captures critical information to establish a CRIL.

d. Works with the DoDEA Office of Communications to thwart the public from aggregating open source information in accordance with DoD Directive 5230.09.

e. Assesses the DoDEA mission to determine threats to operations and potential loss of critical information annually.

2.3. DODEA CHIEF INFORMATION OFFICER. The DoDEA Chief Information Officer ensures:

a. Intranet, extranet, and classified Web sites supporting directorates and other customers, meet DoD requirements for posting official DoD information.

b. OPSEC is integrated into the planning, developing, and implementing stages of net-centric programs and operating environments.

2.4. DODEA CHIEF PROCUREMENT. The DoDEA Chief Procurement Office ensure:

a. OPSEC is included in DoDEA performance statements of work and solicitations lists.

b. Once the contract has been awarded, provides the contractors with the pertinent information to meet OPSEC requirements.

c. Determines if procurement personnel consider taking the Defense Acquisition University OPSEC course.

2.5. DODEA DESIGNATED OFFICIAL. The DoDEA Designation Official is the Principal, Assistant Principal, Administrative Officer, or highest ranking person assigned to the building,

which hereafter is collectively referred to as Designated Official. The DoDEA Designated Official:

a. Tracks and ensures subordinates complete initial and annual OPSEC training.

b. Establishes a facility OPSEC Awareness Program.

c. Lists local OPSEC procedures within the standardized facility FP plan, received from the District Force Protection Officer (FPO) in accordance with Volume 1 of DoDEA Administrative Instruction 5705.01.

2.6. DODEA DISTRICT FORCE PROTECTION OFFICERS. The DoDEA District FPOs:

a. Provide OPSEC guidance and assistance to District or Community Superintendents and Designated Officials.

b. Serve as OPSEC Program Coordinators and, where feasible, establish a relationship with Installation OPSEC Working Groups.

c. Review contracts for the inclusion of OPSEC in the acquisition process, when possible.

2.7. DODEA EMPLOYEES AND CONTRACTORS. DoDEA Employees and Contractors complete OPSEC awareness training on an annual basis in accordance with DoD Directive 5205.02E.

SECTION 3: PROGRAM MANAGEMENT

3.1. DODEA OPERATIONS SECURITY PROGRAM.

a. The DoDEA OPSEC Program operates on a non-attribution basis. Inadvertent, unauthorized disclosures of critical unclassified information will **not** result in punitive actions.

b. DoDEA subcomponents, such as educational and support facilities, have a Level I OPSEC Program. In accordance with DoD Manual 5205.02-M, this level is the lowest OPSEC Program level, requiring minimal management or resources.

c. The District FPO is the OPSEC Program Coordinator for DoDEA facilities within their area of responsibility.

d. The DoDEA OPSEC Program is customized to meet the needs of the organization, but the execption is that policy and procedures will be applied systemically to protect the assets and population of the Activity.

3.2. ASSESSMENTS.

a. DoDEA Operations Security Assessment.

(1) A DoDEA OPSEC assessment is an annual, customized, agency assessment generated from program reviews conducted at the Headquarters (HQ) and subcomponent level.

(2) The DoDEA OPSEC assessment is used to determine if critical information may be inadvertently disclosed through the performance of normal operations and if sufficient countermeasures are in place to protect critical information.

(3) The assessment will generated by the FP Program Manager. When needed, the FP Program Manager will create a team that should include counterintelligence, security, operations, communications, and public affairs to conduct the annual assessment.

b. Program Review.

(1) The DoDEA OPSEC Program review will be:

(a) Conducted at the same time and as part of the FP Assessment.

(b) Used to complete the OPSEC assessment.

(2) The District FPO will ensure the FP Assessment is conducted on all facilities within their area of responsibility in accordance with Volume 1 of DoDEA Administrative Instruction 5705.01 and report the findings to the FP Program Manager.

c. Survey.

(1) As identified in DoD Directive 5205.02E, only particular activities require OPSEC surveys. DoDEA does not meet any of the listed items nor does it prepare, sustain, or employ Military Services over the range of military operations.

(2) DoDEA HQ survey is included in the Mark Center Campus vulnerability assessments as part of the Pentagon Reservation conducted by the Pentagon Force Protection Agency.

3.3. CRITICAL INFORMATION LIST.

a. Critical information is knowledge or data DoD activities, intentions, capabilities, or limitations that an adversary seeks in order to gain a military, political, diplomatic, economic, or technological advantage, and that the organization has determined is valuable to an adversary.

b. When disclosing the CRIL:

(1) Ensure the individual has a "need-to-know."

(2) Use caution when disseminating electronic communications.

(3) Mark correspondence as For Official Use Only (FOUO) and encrypt, if possible.

(4) Never send CRIL to private e-mail accounts, e.g., Gmail, Hotmail, and Yahoo.

c. The CRIL will be approved by the DoDEA Director, distributed to the DoDEA subcomponents, and remain classified as FOUO.

d. The FP Program Manager will:

(1) Develop and update as necessary, the CRIL.

(2) Consider information or knowledge of military activities regarding operations, deployment schedules, new acquisition opportunities, and general administration activities.

e. The District FPO will ensure:

(1) The CRIL is provided to the Designated Officials within their area of responsibility to assist in developing protective measures, as needed.

(2) Report the unauthorized disclosure of critical information.

3.4. DODEA FACILITY OPERATIONS SECURITY PROGRAM.

a. The OPSEC Plan for DoDEA facilities is an enclosure to the FP Plan in accordance with Volume 1 of DoDEA Administrative Instruction 5705.01.

b. Designated Officials will:

(1) Ensure the OPSEC enclosure to the FP Plan:

(a) Meets DoDEA-specific needs and addresses how OPSEC applies to:

1. Daily work and operations.

2. Specifics of site training and awareness programs.

3. Records of site assessments and reports.

(b) Is supported by a continuity book that should contain awareness programs, products, memorandums, assessments, reports, points of contact, awards, training certificates, and any other documentation needed to prove compliance.

(2) Track OPSEC training of facility personnel; provide the results to the District FPO.

(3) Ensure military operational or deployment schedules are **not** displayed in the facility.

(4) Implement an OPSEC Awareness Program to:

(a) Remind the workforce of OPSEC, reinforce training.

(b) Highlight procedures to report OPSEC vulnerabilities, address the importance to control critical information; remind employees of individual responsibilities.

(c) Identify site-specific contact information.

(d) Engage the workforce through awareness campaigns, i.e., posters, site news articles, messages through e-mail, and posting information on common area bulletin boards.

(5) When possible, review the facility website to ensure the CRIL items are not disclosed.

3.5. OPERATIONS SECURITY CONTRACT REQUIREMENTS.

a. The Contracting Officer Repersentative will conduct a OPSEC review of the Performance Work Statement (PWS) for classified and unclassified contracts prior before the Government Contracting Activity releases the PWS to contract bidders.

b. The PWS is a publicly released document that can reveal critical information or indicators of critical information. It is important that Government Contracting Activities work with their OPSEC Program Managers and Coordinators to identify OPSEC requirements for the scope of work to be performed.

c. The PWS should also undergo a formal content review prior to its release to the public. The DoDEA Procurement Office should include the following OPSEC measures within PWS:

(1) Specific OPSEC measures to follow.

(2) OPSEC awareness training.

(3) Participation in the DoDEA OPSEC Program.

(4) Not disclose or use for advertising the contract between the company and Federal government.

SECTION 4: INFORMATION PROTECTION AND DESTRUCTION

4.1. PUBLIC RELEASE.

a. DoDEA must balance mission benefits gained by using the internet and its potential risk of electronically aggregated information accessible to a worldwide audience.

b. Due to the mission, DoDEA may release information as part of normal business operations, i.e., hours of operation; that is not normally released by other agencies.

4.2. DESTRUCTION OF INFORMATION.

a. DoDEA HQ will use burn bags to destroy classified, critical, or unclassified information, sent to the Pentagon Central Destruction facility in accordance with Volumes 3 and 4 of DoD Manual 5200.01.

(1) Documents, compact disks, and diskettes no longer needed, from unclassified to top secret sensitive compartmented information will be placed in burn bags without special markings in accordance with Volume 3 of DoD Manual 5200.01.

(2) DoDEA HQ personnel will ensure burn bags are:

(a) Marked with the highest level of material placed therein, point of contact name, DoD Component and office, and telephone number.

(b) Stored appropriately for the level of material contained therein. Burn bags containing secret information and higher must be stored in a safe.

(c) Less than ten (10) pounds and the top will fold over with a staple every two (2) inches.

(d) Taken to the Mark Center Campus loading dock on Tuesdays and Fridays between 0800 - 0815.

1. A Department of Defense (DD) Form 2843, "Classified Material Destruction Record" will need to be provided with the bags.

2. FOUO bags will be counted as UNCLASSIFIED bags on the DD Form 2843, "Classified Material Destruction Record."

b. Subcomponents or DoDEA educational and support facilities will develop information destruction procedures.

4.3. WEBSITE PROHIBITED INFORMATION. The following is prohibited on DoDEA Web sites and social media:

a. Information restricted by Section 552a of Title 5, United States Code, also known as "The Privacy Act," or identified in DoD Manual 5205.02-M will not be posted on DoDEA Web sites.

b. First, middle, or last name of any DoDEA employee, student, parent, or family member **with the exception** of the "positions commonly known to public." For the purpose of a school Web site:

(1) Teachers and program coordinators may be considered "positions commonly known to the public."

(2) Student names and school may be used when in relation to a specific DoDEA public affairs initiative that recognizes a student(s) for a specific achievement worthy of public recognition with appropriate permission.

c. CRIL, FOUO, or classified information.

GLOSSARY

G.1. ACRONYMS.

CRIL	critical information list
DD	Department of Defense
FOUO	For Official Use Only
FP	force protection
FPO	Force Protection Officer
HQ	headquarters
OPSEC	operations security
PWS	Performance Work Statement

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

critical information. Specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

CRIL. A list of critical information that has been fully coordinated within an organization and approved by the senior decision maker, and is used by all personnel in the organization to identify unclassified information requiring application of OPSEC measures.

Designated Official. The highest ranking Federal employee assigned to a facility, however, also known as the designated official, principal, assistance principal, or administrative officer.

OPSEC. A capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities.

OPSEC survey. A collection effort by a team of subject matter experts to reproduce the intelligence image projected by a specific operation or function simulating hostile intelligence processes.

OPSEC vulnerability. A condition in which friendly actions provide operations security indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making.

positions commonly known to public. The DoDEA Director, Associate Director for Education/Principal Deputy Director, Associate Director for Financial and Business Operations,

Associate Director for Performance and Accountability, Directors for Student Excellence, District Superintendent, principal, and assistant principal.

PWS. In accordance with DoD Dictionary of Military and Associated Terms, a PWS is a statement of work for performance based acquisitions that describe the results in clear, specific, and objective terms with measurable outcomes. The Joint Chiefs of Staff Joint Electronic Library update DoD Dictionary of Military and Associated Terms, found at http://www.jcs.mil/Doctrine/DOD-Terminology/.

DoDEA subcomponent. Also referred to as Subcomponent. A DoDEA school district, region activity, educational facility, support facility, Center for Instructional Learning or Forward Integrated Support Teams facilities, DoDEA organization, or level that reports or receives instructions from DoDEA HQ.

REFERENCES

DD Form 2843, "Classified Material Destruction Record," September 1, 2001

DoD Dictionary of Miliary and assocated Terms, June 2018, available at http://www.jcs.mil/Doctrine/DOD-Terminology/

DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012, as amended

DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008, 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," February 24, 2012, as amended

DoD Manual 5205.02-M, "DoD Operations Security (OPSEC) Program Manual," November 3, 2008, as amended

DoDEA Administrative Instruction 5705.01, Volume 1, "DoDEA Force Protection Program," December 16, 2016

National Security Decision Directive 298, "National Operations Security Program," January 22, 1988

United States Code, Title 5, Section 522a (also known as "The Privacy Act")