BILLING CODE: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-YYYY-OS-XXXX]

Privacy Act of 1974; System of Records

AGENCY: Department of Defense (DoD)

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Defense (DoD) is modifying and reissuing a current system of records titled, National Defense University (NDU) Student Data Files," DNDU 01. This system of records was originally established by the Office of the Secretary, DoD/Joint Staff to collect and maintain records on students and track academic enrollment information necessary to complete the mission of the University. This system of records notice (SORN) is being updated to comply with the Office of Management and Budget mandates and to reflect the applicable routine uses.

DATES: This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. The Routine Uses are effective at the close of the comment period.

ADDRESSES: You may submit comments, identified by docket number and title, by either of the following methods:

* Federal Rulemaking Portal: https://www.regulations.gov. Follow the instructions for submitting comments.

* Mail: DoD cannot receive written comments at this time due to the COVID-19 pandemic.

Comments should be sent electronically to the docket listed above.

Instructions: All submissions received must include the agency name and docket number for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at https://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ann Summers, Component Privacy and Civil Liberties Officer, 260 5th Avenue, S.W., Marshall Hall, Building 62, Room 301A, Fort Lesley J. McNair, Washington, DC 20319. whs.mc-alex.esd.mbx.osd-js-foia-requester-service-center@mail.mil.

SUPPLEMENTARY INFORMATION:

I. Background

The National Defense University (NDU) Student Data Files system of records is used to allow the University to collect official transcripts for students and track academic enrollment information necessary to complete the mission of the University. Subject to public comment, the DoD proposes to update this SORN to add the standard DoD routine uses (routine uses A through I). Additionally, the following sections of this SORN are being modified as follows (1) to the Authority for Maintenance of the System section to update citation(s) and add additional authorities; (2) to the Purpose of the System to widen the scope of collection; (3) to the Categories of Individuals Covered by the System section to expand the individuals covered and Categories of Records to clarify how the records relate to the revised Category of Individuals; (4) to the Administrative, Technical, and Physical Safeguards to update the individual safeguards protecting the personal information; (5) to the Retention and Disposal section to reflect the

approved disposition; (6) to the Record Access and Notifications Procedures section to reflect the need for individuals to identify the appropriate DoD office or component to which their request should be directed; (7) to the Contesting Records Procedures section to update the appropriate citation for contesting records; and (8) to the System Manager and System Location sections to update the addresses and office names. Furthermore, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

DoD SORNs have been published in the Federal Register and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Defense Privacy, Civil Liberties, and Transparency Division website at https://dpcld.defense.gov/privacy.

II. Privacy Act

Under the Privacy Act, a "system of records" is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and OMB Circular No. A-108, DPCLTD has provided a report of this system of records to the Office of Management and Budget (OMB) and to Congress.

Dated:

Aaron T. Siegel,

Alternate OSD Federal Register

Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER: National Defense University Data Files, DNDU 01.

SECURITY CLASSIFICATION: Unclassified

SYSTEM LOCATION: National Defense University, 300 5th Avenue, Building 62, Fort Leslie J. McNair, Washington, D.C. 20319-5066; National Defense University South Campus, 7800 Hampton Boulevard, Norfolk, VA 23511-1702.

SYSTEM MANAGER: The system manager is the Senior Component Official for Privacy, National Defense University, 260 5th Avenue, S.W., Marshall Hall, Building 62, Room 301A, Fort Lesley J. McNair, Washington, DC 20319. whs.mc-alex.esd.mbx.osd-js-foia-requester-service-center@mail.mil.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 2163, Degree Granting Authority for National Defense University; 10 U.S.C. 2165, National Defense University; and E.O. 9397, as amended (SSN).

PURPOSE(S) OF THE SYSTEM:

A. To generate official transcripts for students, facilitate award of degrees and credentials, and track academic enrollments, assignments, progress and assessments.

B. To process visitor requests, and store faculty, staff, and contractor information necessary to complete the mission of the University.

C. To render management, statistical summaries, and reports.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Active Military, Reserve, National Guard, International Military, their delegates and their families, DoD and other Federal civilian employees, military and civilian fellows, contractor, and private industry students attached to NDU or enrolled in courses of instruction at NDU.

CATEGORIES OF RECORDS IN THE SYSTEM:

A. Personal information such as name, Social Security Number (SSN), DoD Identification number, passport number, country of origin, address, date of birth, phone numbers, e-mail addresses, citizenship, race, sex, age, gender, marital status, spouse information.

B. Employment information, to include date of rank (DOR), basic active Service date (BASD), Joint Service experience, command experience, grade/rank, branch of service or civilian agency, years of Federal service, security clearance granted and date, agency/Service, military operations, assignments, attributes pertaining to military personnel, civilian, and disability and limited medical information.

C. Education and academic data, such as Joint Professional Military Education (JPME) Level, degrees granted, student identification number, and inter-agency personnel records related to student course enrollments and final grades.

D. Financial information, such as account number and routing number.

RECORD SOURCE CATEGORIES: Records and information stored in this system of records are obtained from: Individuals, faculty evaluations and reports, or transcripts from educational institutions, and official records pertaining to the individual.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, all or a portion of the records or information contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this system of records.

B. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

C. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

E. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

F. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with

the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

H. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

I. To another Federal, State or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or some other review as authorized by the Inspector General Act.

H. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records may be stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, or digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP).

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by name, SSN, or student identification number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Individual and class academic records are destroyed after 40 years. Records pertaining to extension courses are held indefinitely before being retired to the National Personnel Records Center, St. Louis, MO. Individual training records are destroyed annually; management reports are destroyed when no longer needed. **ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:** The DoD safeguards records in this system of records according to applicable rules, policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, the DoD established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. The DoD routinely employs safeguards such as the following to information systems and paper recordkeeping systems: Multifactor log-in authentication including Common Access Card (CAC) authentication and password; physical token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who will have access; identification, marking, and safeguarding of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities.

RECORD ACCESS PROCEDURES: Individuals seeking access to their records should address written inquiries to the Chief, Freedom of Information Division, Office of the Secretary

of Defense/Joint Staff FOIA Requester Service Center, Office of Freedom of Information, whs.mc-alex.esd.mbx.osd-js-foia-requester-service-center@mail.mil. Signed written requests should contain the name and number of this system of records notice along with full name, current address, and email address of the individual. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the appropriate format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

CONTESTING RECORD PROCEDURES: The DoD rules for accessing records, contesting contents, and appealing initial Component determinations are contained in 32 CFR part 310, or may be obtained from the system manager.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system of records should follow the instructions for Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None

HISTORY: September 21, 2010; 75 FR 57458