SYSTEM NAME AND NUMBER: Data Warehouse Business Intelligence System (DWBIS), N05220-1. (August 28, 2018, 83 FR 43857; corrected September 14, 2018, 83 FR 46711)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: SPAWAR Systems Center Atlantic, Building 3148, 1 Innovation Drive, Hanahan, SC 29410-4200.

SYSTEM MANAGER(S): Commanding Officer, ATTN: Code 80E, SPAWARSYSCEN Atlantic, 1837 Morris Street, Suite 3109B, Norfolk, VA 23511-3498, Spawar_info@navy.mil.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. Chapter 87, Defense Acquisition Workforce; DoD Instruction 5000.66, Defense Acquisition Workforce Education, Training, Experience, and Career Development Program; DoD Manual (DoDM) 5200.02, Procedures for the DoD Personnel Security Program (PSP); DoDM 8570.1, Information Assurance Workforce Improvement Program; SECNAV Manual (SECNAV M) 5239.2, DoN Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual; and SECNAV M-5510.30, Department of Navy Personnel Security Program.

PURPOSE(S) OF THE SYSTEM: This system is used to help SPAWAR manage its workforce education, training, and career development programs needed to support the design, development and deployment of key information warfare, business information technology and space systems for Naval and DoD programs as assigned to this system command. The system will also help SPAWAR document and manage the skills and experience necessary in its Acquisition, Cyber Security, and Information Warfare workforce to staff current and future programs and projects in its primary roles as a technical authority and an acquisition command.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Active duty and Reserve Naval personnel, DoN Civilians, and contractors currently employed by SPAWAR.

CATEGORIES OF RECORDS IN THE SYSTEM: Name, work and alternate work address(es), DoD ID Number, billet number, ID number from the source system, Navy Enterprise Resource Planning (ERP) employee ID number, military rank or government series and grade, military occupation specialty (MOS) employee series and grade, date reported to command, duty station, work location, organizational code, organizational group, supervisor and their contact numbers, position title and pay plan, scheduling (hours per project), defense acquisition workforce coursework planned or completed, position level and continuous learning points required, Cyber Security Workforce membership including credentials, certifications held, and expiration date; contracting officer's representative status, certifications achieved, demonstrated proficiency levels earned under internal competency development model, projects or portfolio work assigned, credentials held on entry to the mid-career leadership program, security clearance held, award(s); education information including college courses applied for, college degrees held and institutions attended, professional certifications held; employee promotion(s), overseas tour begin and end date, number of years at current position or current tour end.

Contractor's information, including user account information in Navy ERP by name and unique ID, government sponsor, and whether they are a current member of the command's Cyber Security Workforce for reporting purposes.

RECORD SOURCE CATEGORIES: SPAWAR Personnel Officers and Administrators, Navy Enterprise Resource Planning (Navy ERP), SPAWAR Directory Services (LDAP), Total Workforce Management Services (TWMS), Total Force Manpower Management System (TFMMS), DoN Director, Acquisition Career Management (eDACM), DoD Defense Civilian Personnel Data System (DCPDS)/Human Resources Link (HRLink), the Navy Enlisted System (NES), Officer Personnel Information System (OPINS).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE 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, the records contained therein 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 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.

c. 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.

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 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.

h. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms there is 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.

i. To another Federal agency or Federal entity, when the DoD determines 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are maintained in electronic storage media, in accordance with the safeguards mentioned below.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: These records are retrieved primarily by name, work and/or (for former employees and contractors) home address, DoD ID Number, employee ID number, and/or unique ID.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are maintained for 1 year after termination of employment or duty station, or when abstracted, or consolidated, whichever is earlier. Per guidance from the Secretary of the Navy M-5210.1 DON Records Management Manual, DoD ID will be retained for the purpose of trend analysis and will be destroyed when no longer needed for reference.

ADMINISTRATIVE, PHYSICAL, AND TECHNICAL SAFEGUARDS: Administrative safeguards: All persons who apply to access to this system are required to have completed annual cybersecurity training and hold an unexpired DoD Common Access Card (CAC) issued by the command. All users must provide a digitally signed OPNAV 5239/14 System Authorization Access Request Navy (SAAR-N) form digitally countersigned by the user's Supervisor or the assigned Contracting Officer's Representative (COR), stating the duty-related justification for access. Users requiring privileged access to maintain the system must complete Command Privacy Act Training and provide a SECNAV 5239/1—Information System Privileged Access Agreement and Acknowledgement (PAA) of Responsibilities form which identifies their credentials and training certifications as a member of the Cyber Security Workforce. All requests for access are independently reviewed by the Command Security Manager; persons requesting non-privileged access must complete a favorably adjudicated Tier 1 (T1) investigation National Agency Check with Written Inquiries (formerly NACI). Privileged access users must complete a favorably adjudicated Tier 3 (T3) investigation (formerly National Agency Check with Law and Credit (formerly ANACI/NACLC)) and be U.S. citizens. Technical safeguards employed for electronic records have data at rest encryption and access is restricted to authorized users holding specific electronic credentials and having a need to know. Physical access to terminals, terminal rooms, buildings, and surroundings are controlled by locked terminals and rooms, guards, personnel screening, and visitor registers.

RECORD ACCESS PROCEDURES: Individuals seeking access to records about themselves contained in this system of records should address written and signed inquiries to Commanding Officer, ATTN: Code 80E, SPAWARSYSCEN Atlantic, 1837 Morris Street, Suite 3109B, Norfolk, VA 23511-3498.

The requester must provide their full name, mailing/home address, DoD ID Number, and/or employee ID number.

The system manager may require a DoD Public Key Infrastructure (PKI) signed email as a means of proving the identity of the individual requesting access to the records.

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 following 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 Navy's rules for contesting contents and appealing initial agency determinations are published in Secretary of the Navy Instruction 5211.5; 32 CFR part 701; or may be obtained from the system manager.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether this system of records contains information about themselves should address written and signed inquiries to Commanding Officer, ATTN: Code 80E, SPAWARSYSCEN Atlantic, 1837 Morris Street Suite 3109B, Norfolk, VA 23511-3498.

The requester must provide their full name, mailing/home address, DoD ID Number, and/or employee ID number.

The system manager may require a DoD Public Key Infrastructure (PKI) signed email as a means of proving the identity of the individual requesting access to the records.

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 following 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)."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: December 23, 2015, 80 FR 79869