SORN REFERENCE

Version II

May 2018

Table of Contents

REVISION HISTORY

Changed, “Preamble” to, “Federal Register Notice” (throughout).

Changed, “Information Required by DPCLTD (Not submitted to OMB)” to, “Information Required by DPCLTD (Not required by OMB)” (throughout).

Capitalized, “Federal Government” in all instances (throughout).

Changed, “The DoD Privacy Program is currently administered through the following DoD Issuances: DoD Directive 5400.11, “DoD Privacy Program,” October 29, 2014; DoD Regulation 5400.11, “Department of Defense Privacy Program,” May 14, 2007. To, “The DoD Privacy Program is currently administered through the following DoD Issuances: DoD Directive 5400.11, “DoD Privacy Program,” October 29, 2014; DoD Regulation 5400.11, “Department of Defense Privacy Program,” May 14, 2007. (page 4 previous version, page 6 current version).

Added language to SORN Introduction: “The DoD Component privacy offices submit their completed work products to DPCLTD who ensure: compliance with OMB guidance; notification of Congress regarding the publication if applicable; coordination of the submission with the appropriate internal DoD offices and OMB before publishing in the Federal Register.” (page 4 previous version, page 6 current version).

Changed, “NARRATIVE STATEMENT (ONLY required for Additions and Modifications)” to “NARRATIVE STATEMENT (ONLY required for New and Modified SORNs)” (page 9 previous version, page 11 current version).

Removed Narrative Statement Template (page 13-14 previous version).

Changed, “Use single line spacing” to, “Use double line spacing for Federal Register Notice, SORN, and SORN comparison in “SYSTEM OF RECORDS NOTICE (SORN) Formatting” (page 15 previous version, page 15 current version).

Changed, “Page numbers in the bottom right corner of the footer” to, “Page Numbers in the center of the footer” in “SYSTEM OF RECORDS NOTICE (SORN) Formatting” (page 15 previous version, page 15 new version).

Changed, “PURPOSE OF THE SYSTEM” to, “PURPOSE(S) OF THE SYSTEM” in “SORN SECTIONS” (page 16 previous version, page 16 current version).

Removed, “-NEW REQUIREMENT” after “HISTORY” in “SORN SECTIONS” (page 16 previous version, page 16 current version).

Removed, “Limited to 21 positions” (page 17 previous version, page 17 current version).

Changed, “An organizational email address and telephone number are strongly suggested.” to, “An organizational email address and telephone number are required if available.” in “SYSTEM MANAGER(S)” (page 19 previous version, page 19 current version).

Added Federal Register Notice (Preamble) instructions (page 32 current version).

Removed instructional language from, “OMB A-108 SYSTEM OF RECORDS NOTICE TEMPLATES, Appendix II OFFICE OF THE FEDERAL REGISTER SORN TEMPLATE - FULL NOTICE” (page 32-34 previous version).

Removed instructional language from, “Appendix III, OFFICE OF THE FEDERAL REGISTER SORN TEMPLATE - NOTICE OF REVISION” (page 37 previous version).

Removed instructional language from, “Appendix IV, OFFICE OF THE FEDERAL REGISTER SORN TEMPLATE - NOTICE OF RESCINDMENT” (page 39 previous version).

Added Narrative Statement Template for New and Modified SORNS (pages 41-44 current version).

Changed, “Title of Collection if different” to, “Title of Collection” in the Narrative Statement Templates (page 13 previous, pages 41 and 43 current version).

Changed, “Provide the agency’s evaluation on the probable…” to, “Evaluation of the probable…” in the Narrative Statement template (page 13 previous, pages 41 and 43 current version).

Added Federal Register Notice Template - New SORN (pages 45-47 current version).

Added New/Modified SORN Template (pages 51-61 current version).

INTRODUCTION

The Department of Defense (DoD) is committed to ensuring its systems of records are compliant with the Privacy Act of 1974, as amended, and applicable Office of Management and Budget (OMB) guidance. This reference guide contains information to help DoD Component Privacy Offices prepare Privacy Act system of records notices (SORNs), complete narrative statements for OMB, and prepare Federal Register Notices (also called preambles) submitted with notices to the Federal Register (FR). The DoD Component privacy offices submit their completed work products to DPCLTD who ensure: compliance with OMB guidance; notification of Congress regarding the publication if applicable; coordination of the submission with the appropriate internal DoD offices and OMB before publishing in the Federal Register. The material in this guide reflects DPCLTD's interpretation of OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act* (December 23, 2016, 81 FR 94424), as informed by its experience working directly with OMB. However, this document does not establish policy.

OMB Circular A-108 (December 23, 2016) describes agency responsibilities for implementing the review, reporting, and publication requirements of the Privacy Act. The 2016 circular includes several changes to the SORN format and content to improve public notification about how information in a system of records will be collected, used, and safeguarded. While this reference should help DoD Components comply with OMB Circular A-108, DoD Component Privacy Offices are encouraged to refer to DoD Privacy Program policies,[1] and OMB Circular A-108 for additional guidance. DoD privacy policies and Federal privacy law and guidance can be found in the Authorities and Guidance section on DPCLTD's website at: http://dpcld.defense.gov/Privacy/Authorities-and-Guidance/.

DoD Components are encouraged to take a holistic view of privacy when developing privacy compliance documents. Before submitting a SORN to the DPCLTD for review, DoD Component Privacy Offices should collaborate with appropriate component offices and respective subject matter experts to ensure compliance with other Federal laws, guidance, and DoD policies, including those applicable to the compliance programs mentioned in the next sections.

DoD Components should ensure all applicable compliance documentation is current and should be prepared to provide any requested documentation with each of the above when submitting a SORN package. In many instances, DPCLTD cannot accomplish its review until this information is provided when required.

DoD Components should also be aware that OMB Circular A-108 now requires 30 days advance notice to OMB and Congress and an approval from OMB prior to submitting a SORN action to the Office of the Federal Register (OFR). Notices published in the FR are effective immediately, unless there are new or modified routine uses, which are not effective until the statutory 30-day public comment period has closed and any substantive public comment addressed. SORNs are

[1] The DoD Privacy Program is currently administered through the following DoD Issuances: DoD Directive 5400.11-R, "DoD Privacy Program," October 29, 2014; DoD Regulation 5400.11-R, "Department of Defense Privacy Program," May 14, 2007.

living documents, and should be reviewed continuously. SORNs will need to be updated and re-published to reflect changes to the SORN elements in accordance with OMB Circular A-108 the next time SORNs are substantively modified.

The role of the Components is to ensure compliance with the Privacy Act and OMB requirements established in OMB Circular A-108 and other documents (such as Federal Register publication requirements). DPCLTD recognizes DoD Component Privacy Officers and personnel along with program managers, systems managers, records managers, and information management control officers (IMCOs) are in a far better-placed position to understand the nuances of a component-specific system of records. Components should submit SORN packages compliant with the Privacy Act, OMB Circular A-108, and other associated requirements e.g., if the Paperwork Reduction Act applies and the OMB license is current; if the use of SSNs is documented and approved; and if the SORN reflects a records retention approved by the Archivist of the United States. The role of DPCLTD is to conduct a review of SORN packages to ensure that they are ready to be submitted to the SAOP, OMB, and the OFR.

This document should be used alongside OMB Circular A-108.

Considerations in a SORN Review

Types of SORN Action Requests

There are three (3) types of SORN Action Requests that can be submitted to the DPCLTD for review:

- New: The creation of a new system of records.
- Modification: Significant change altering the content of a system of records (e.g. changes to: categories of individuals about who records are maintained, types of records, purpose, authority, etc.) or changes how the public will interact with the system. Refer to A-108, section 6.b.
- Rescindment: A system of records is no longer being maintained and the SORN is invalidated.

These submissions may require additional documents in addition to the text of the SORN itself and significant changes. Be sure to verify if these additional documents may be required before submitting the SORN to the DPCLTD.

The SORN documents include:

- Narrative Statement (discussed below).
    - **ONLY** required for a New and Modified SORN.
    - The summary of the significant changes being made to a Modified SORN.
- In the case of a Modified SORN, a version with tracked changes showing the difference from the currently published SORN.
- Federal Register Notice (Preamble) (discussed on page 32).
- For systems of records which require compliance with other requirements, be prepared to submit documentation ensuring compliance with the following:

Paperwork Reduction Act (PRA)

- If the categories of individuals covered by the system of records include contractors or members of the public (as determined by OMB) you should consult with your Component's Information Management Control Officer (IMCO) to ensure the SORN is reviewed for PRA requirements before it is submitted to the DPCLTD. Confirmation may be requested so be prepared to provide an email or other coordination documents from the Component IMCO. NOTE: SORNs should only be submitted to DPCLTD when no PRA applies (subject to IMCO confirmation), the 30-day PRA notice is published in the Federal Register, or a currently approved PRA license exists.

- Entry 6 on the Narrative Statement must be completed for a New or Modified SORN.

  ***Reference*:** DoDI 8910.01, Information Collection and Reporting; DoDM 8910.01, Vol 2, DoD Information Collections Manual: Procedures for Public Information Collections for OMB approvals on collections that meet this criteria.

Records Management

- Ensure the records retention and disposition in the SORN covers the lifecycle of the records maintained in the system, consistent with the approved records schedule.

- If it is a new SORN, provide the Standard Form (SF) 115 if the records disposition schedule is pending approval.

- If it is an existing SORN, confirmation of the retention and disposition schedule from the component records manager may be requested.

***Reference*:** DoDI 5015.02, DoD Records Management Program

Privacy Impact Assessment (PIA)

- If the records (or portions thereof) are maintained in an information technology (IT) system, provide a copy of the most recently approved Privacy Impact Statement (PIA), DD Form 2980 dated June 2017.

Reference: DoDI 5400.16, DoD Privacy Impact Assessment (PIA) Guide.

Social Security Number (SSN) Justification Memoranda

- If the system of records identifies the SSN as a category of records in the system, include the current SSN Justification Memorandum, signed by the approving official and coordinated by the component privacy officer. The SSN justification must cite the applicable provisions of DoDI 1000.30. The continued use of this SSN, supported by the justification, must be approved by the Chief, DPCLTD.

- SSN justification must be updated and submitted for approval when there is a modification to the SORN which continues to include SSN as a category of records.

Reference: DoDI 1000.30, Reduction of Social Security Numbers (SSN) Within DoD

Exemptions/Proposed Rule

- Does the system have a published Privacy Act exemption rule?

  - If yes, provide confirmation the Component Office of General Counsel (OGC) reviewed the current exemption rule and verified it is accurate and applicable to the system.

    - Include the FR notice or Code of Federal Regulations (CFR) citation for the exemption.

- If new exemptions or modifications to existing exemptions are proposed for the system of records, include the proposed exemption rule with confirmation of approval from the Component OGC.

NARRATIVE STATEMENT (ONLY required for New and Modified SORNs)

1. System name and number

The proposed (New SORN) or current (Modified SORN) includes the **System Name** followed by the **System Number**.

Sample Format:
"Military Spouse Employment Partnership (MSEP) Career Portal," DPR 47 DoD.

2. Purpose of establishing the system

The intent of this response is to explain to OMB and Congress why the Component is required to collect, use, and maintain the information on individuals in its system of records. This section may also be used in the Federal Register Notice (Preamble), which is published in the Federal Register with the SORN). When well written, it should reduce concerns and the number of comments submitted by the public when the SORN is published. The SORN should not be a duplication of any existing systems of records or SORNs that have already been published in the Federal Register. **It should not repeat the purpose as stated in the SORN.** Your response should address these three questions:

1. What action is being taken?
2. Why is this action necessary?
3. What is the intended effect of this action?

Sample Format: *(DPR 47 DoD)*
The Office of the Secretary of Defense is proposing to establish a system of records that will be the sole web platform utilized to connect military spouses with companies seeking to hire military spouse employees. Participating companies, called MSEP Partners, are vetted and approved participants in the MSEP Program and pledged to recruit, hire, promote and retain military spouses in portable careers. MSEP is a targeted recruitment and employment partnership that connects American businesses with military spouses who possess essential workforce skills and attributes and are seeking portable, fulfilling careers. The MSEP program is part of the overall Spouse Education and Career Opportunities (SECO) program which falls under the auspices of the office of the Deputy Assistant Secretary of Defense for Military Community & Family Policy.

2. (Modified SORN) Nature of proposed modifications for the system

This should be written in the same manner as described above for New SORNs. In addition to expanding the purpose for Modified SORNs, briefly explain the significant changes that are being made to the system of records. The language **MUST NOT** simply reflect a copy and paste of the language in the Purpose section. The response should generally address these three questions:

1. What changes are being made?

2. Why are the changes necessary?

3. What is the intended effect of these changes?

Sample Format: *(DTIC 01)*
This system of records registers and certifies users of Defense Technical Information Center (DTIC) products and services. It ensures that Department of Defense scientific and technological information is appropriately managed to enable scientific knowledge and technological innovations to be fully accessible to authorized recipients while applying appropriate safeguards to assure the information is protected according to national security requirements. This modification reflects a change to the system location, categories of individuals, categories of records, authorities, purpose, routine uses, retrievability, safeguards, system manager and address, notification procedure, record access procedures, contesting record procedures, and record source categories.

3. Specific authority for the maintenance of the system

Cite the specific authority under which the system of records will be maintained (copy and paste the Authorities section from the Proposed SORN section).

Sample Format:
5 U.S.C. 4103, Establishment of training programs; 10 U.S.C. 3013, Secretary of the Army; Department of Defense Directive 1322.18, Military Training; Army Regulation (AR) 350-1, Army Training and Leader Development; AR 600-20, Army Command Policy; AR 600-8-8, The Total Army Sponsorship Program; AR 690-950, Career Management; and E.O. 9397 (SSN), as amended.

4. Evaluation of the probable or potential effect on the privacy of individuals

The OMB Circular A-108 states, "If the agency has conducted one or more privacy impact assessment(s) with respect to information technology that will be used to collect, maintain, or disseminate the information in the system of records, the privacy impact assessment(s) will likely provide the information necessary to meet this requirement, and may be submitted in lieu of drafting a separate evaluation."

If there is no PIA because the records are not stored in an information system (electronic maintenance), list any known or perceived adverse effects on the individual by maintaining the system of records. A risk assessment of the categories of PII can be found in Committee of National Security Systems No. 1253
http://iassecurity.net/Resources/CNSSI_1253.SC%20Controls1.pdf.

Sample Format:
The risk of unauthorized access to records is low due to SECO being hosted on a DoD Information Assurance Certification and Accreditation Process (DIACAP) certified and accredited infrastructure. Records are maintained on a military installation in a secure building

in a controlled area accessible only to authorized personnel. Records are encrypted during transmission to protect session information and at rest.

5. Routine use compatibility

OMB Circular A-108 requires components to explain how each new or modified routine use satisfies the compatibility requirement of the Privacy Act. Routine uses shall be narrowly tailored to address a specific and appropriate use of the records in the system of records. A routine use may be appropriate when the use of the record is necessary for the efficient conduct of government, and when the use is both ***related to*** and ***compatible with*** the original purpose for which the information was collected. The concept of compatibility comprises both functionally equivalent uses of the information as well as other uses of the information that are necessary and proper. DPCLTD will update this section relating to compatibility language at a future date.

Reference: ***OMB Circular A-108***

Explanations of new and modified routine uses, and how they satisfy the compatibility requirement of the Privacy Act only need to be explained in the narrative statement. List only the routine uses themselves in the SORN. This explanation is only required here in the Narrative Statement.

Sample Format:
Routine use compatibility: The routine uses for this system are compatible with the purpose for which there records are collected. (Specific Routine Uses): To civilian educational institutions where the participant is enrolled, for the purposes of ensuring correct enrollment and billing information. This (or the following routine uses) routine use complies with 10 U.S.C. 1784a, Education and training opportunities for military spouses to expand employment and portable career opportunities and is necessary to conduct efficient government business within DoD.

6. OMB public information collection requirements

Consult with your Component IMCO to answer these questions:

OMB collection required: Yes/No

OMB Control Number (if approved): N/A (or number if available)

Title of Collection: N/A (or Title if available)

Date Submitted to OMB if Pending: N/A (or date approved or submitted)

Expiration Date (if approved): N/A (or expiration date)

Reference: Information collections may be searched at http://www.reginfo.gov/public/do/PRAMain. Select "Department of Defense" to search DoD collections, and use the "edit" or "find" functions to search by license number or keyword.

Provide titles of any information collection requests (e.g., forms and number, surveys, etc.) contained in the systems of records: (list the names of any forms or other information collection instruments).

If collecting on members of the public and no OMB approval is required, state the applicable exception(s) or provide the reason for not having an approved OMB collection.

Reference: DoD 8910.1-M, Vol 2

Sample Format:
OMB collection required: Yes
OMB Control Number (if approved): 0704-0000
Title of Collection: Sample Survey
Date Submitted to OMB if Pending: N/A
Expiration Date: July 31, 2018

Provide titles of any information collection requests (e.g., forms and number, surveys, interview scripts, etc.) contained in the system of records: DD Form 123, Title of the Form
My Application Portal

Information Required by DPCLTD (Not required by OMB)

7. Name of Information Technology (IT) System and DITPR Number

Answer this question with the full name of the IT system being used for the system of records.

Enter the DITPR Number.

If the system uses paper records or electronic files that are not maintained in an IT system, state "NONE."

Sample Format:
Defense User Registration System. DITPR Number 4300.

8. Is the system, in whole or in part, being maintained by a contractor?

Answer Yes or No.

A routine use must be established to permit disclosure of records to the contractor operating a system. This can be validated in the PIA as well in the routine uses as modeled later in this document.

Reference: *OMB Circular A-108* (section j)

Sample Format:
Yes.

SYSTEM OF RECORDS NOTICE (SORN)

Formatting

- **Font:** Times New Roman
- **Size:** 12
- **Margins:** 1" throughout the document
- Two (2) spaces after periods or colons
- One (1) space after commas or semi-colons
- Use double line spacing for Federal Register Notice (Preamble), SORN, and SORN comparison document
- No auto formatted lines before or after the paragraph
- Page numbers in the center of the footer
- Section headings are to be **BOLDED** and in **ALL CAPS**
- Spell out acronyms for the first use, use acronym for all subsequent uses
- Write in in plain language, avoid legal and technical jargon (Federal Plain Language Guidelines are available at: http://www.plainlanguage.gov/howto/guidelines/FederalPLGuidelines/index.cfm)
- Use appropriate grammar
- Use spell check **BUT** remember it cannot catch all errors
- Ensure all paragraphs are left justified.
- **DO NOT** underline, *italicize*, or change the wording in the notice section headings
- **DO NOT** use headers
- **DO NOT** put a line break between the section heading and the paragraph provided

SORN Sections

Excluding the introductory language and contact information in the Federal Register notice, there are **19** required sections in every SORN:

1. **SYSTEM NAME AND NUMBER**
2. **SECURITY CLASSIFICATION**
3. **SYSTEM LOCATION**
4. **SYSTEM MANAGER(S)**
5. **AUTHORITY FOR MAINTENANCE OF THE SYSTEM**
6. **PURPOSE(S) OF THE SYSTEM**
7. **CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM**
8. **CATEGORIES OF RECORDS IN THE SYSTEM**
9. **RECORD SOURCE CATEGORIES**
10. **ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES**
11. **POLICIES AND PRACTICES FOR STORAGE OF RECORDS**
12. **POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS**
13. **POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS**
14. **ADMINISTRATIVE, PHYSICAL, AND TECHNICAL SAFEGUARDS**
15. **RECORDS ACCESS PROCEDURES**
16. **CONTESTING RECORD PROCEDURES**
17. **NOTIFICATION PROCEDURES**
18. **EXEMPTIONS PROMULGATED FOR THE SYSTEM**
19. **HISTORY**

SYSTEM NAME AND NUMBER

- The system name should reasonably identify the general purpose or scope of the system.
    - Concise, unambiguous, and clearly identifies the character or function of the system of records.
    - The name should not be excessively long.
    - Acronyms should be spelled out first.
    - Should not be the name of the database or the IT system UNLESS it succinctly describes the system of records.
- The SORN number is assigned by the DoD Component.
    - Required on all notices.
    - The first "alpha" character that precedes the SORN Number is assigned by DPCLTD. All characters following the first "alpha" character are assigned by the DoD Component Privacy Office. The table below lists each agency's SORN alpha identifier.

DoD Component SORN Alpha Identifier List

MILITARY BRANCHES		
Abbreviation	**Full Name**	**SORN Alpha Identifier**
USAF	United States Air Force	F
USA	United States Army	A
USN	United States Navy	N
USMC	United States Marine Corps	M

DEFENSE AGENCIES		
Abbreviation	**Full Name**	**SORN Alpha Identifier**
DCAA	Defense Contract Audit Agency	R
DCMA	Defense Contract Management Agency	P
DeCA	Defense Commissary Agency	Z
DFAS	Defense Finance and Accounting Services	T
DHA	Defense Health Agency	E
DIA	Defense Intelligence Agency	L
DISA	Defense Information Systems Agency	K
DLA	Defense Logistics Agency	S
DoDIG	Department of Defense Inspector General	C
DSS	Defense Security Service	V

DTRA	Defense Threat Reduction Agency	H
JS	Joint Staff	J
MDA	Missile Defense Agency	X
NGA	National Geospatial-Intelligence Agency	B
NSA	National Security Agency	G
NGB	National Guard Bureau	I
NRO	National Reconnaissance Office	Q
OSD	Office of the Secretary of Defense	D
USUHS	Uniformed Services University of the Health Sciences	W

COMBATANT COMMANDS **Alpha identifier reflects the character of the supporting Military Department**		
Abbreviation	**Full Name**	**SORN Alpha Identifier**
USAFRICOM	United States Africa Command	A
USCENTCOM	United States Central Command	F
USEUCOM	United States European Command	A
USNORTHCOM	United States Northern Command	F
USPACOM	United States Pacific Command	A
USSOUTHCOM	United States Southern Command	A
USSOCOM	United States Special Operations Command	F
USSTRATCOM	United States Strategic Command	F
USTRANSCOM	United States Transportation Command	F

Reference: *DoD 5400.11-R, Department of Defense Privacy Program*

Sample Format:
SYSTEM NAME AND NUMBER: Defense User Registration System (DURS) Records, DTIC 01.

SECURITY CLASSIFICATION

An indication of whether any information in the system is classified or unclassified.

Reference: *OMB Circular A-108 (page 37)*

Unless the system has specifically established a k(1) exemption under the Privacy Act, this will be "Unclassified"

Sample Format:
SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION

The complete mailing address to include the nine digit zip code of the Component responsible for the system, as well as the complete mailing address of any third-party service provider (e.g., cloud service provider).

Reference: *OMB Circular A-108 (page 37)*

Sample Format:
SYSTEM LOCATION: Defense Technical Information Center (DTIC), Directorate of User Services, Communications and Customer Access Division, ATTN: DTIC-UC, 8725 John J. Kingman Road, Fort Belvoir, VA 22060-6218.

SYSTEM MANAGER(S)

The title, business address, and contact information of the agency official who is responsible for the system.

- An organizational email address and telephone number are required if available.

Reference: *OMB Circular A-108 (page 38)*

Sample Format:
SYSTEM MANAGER(S): Chief, Customer Access and Communications Division, DTIC-UC, 8725 John J. Kingman Road, Fort Belvoir, VA 22060-6218.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM

Cite the specific provision of the Federal statute or Executive Order (citation and descriptive title) that authorizes the maintenance of the system. Statutes, Executive Order of the President, or agency regulations may be cited as authorities for maintenance of the system. The authorities used must correspond with the individuals covered by the system and the categories of records therein.

- **Do not** list, "5 U.S.C. 301, Departmental Regulations," as this authority is generally too broad for purposes of a DoD system of records notice.

- Each SORN must include at least one statute or Executive Order. However, only include DoD Directives, Instructions, Manuals and Regulations with primary program relevance to the system of records at issue. Do not list DoD issuances with only minimal or peripheral relevance.

List authorities in the following order:

1. Statutes
2. Executive Orders
3. DoD Directives
4. DoD Instructions
5. DoD Publications/Manuals
6. DoD Component Regulations
7. E.O. 9397 (SSN), as amended (Note: Use only if the SSN is in the categories of records)

Reference: *DoD 5400.11-R (page 59, C6.3.7); OMB Circular A-108 (page 38)*

Sample Format:
AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 4103, Establishment of training programs; 10 U.S.C. 3013, Secretary of the Army; Department of Defense Directive 1322.18, Military Training; Army Regulation (AR) 350-1, Army Training and Leader Development; AR 600-20, Army Command Policy; AR 600-8-8, The Total Army Sponsorship Program; AR 690-950, Career Management; and E.O. 9397 (SSN), as amended.

PURPOSE(S) OF THE SYSTEM

State the purpose(s) for which the system of records was established and uses of the information which are internal to the Department. Purpose must be supported by the authorities cited.

References: *DoD 5400.11-R (page 59, C6.3.8); OMB Circular A-108 (page 38)*

Sample Format:
PURPOSE(S) OF THE SYSTEM: The SECO Program is administered through a government website as the primary source of education, career and employment counseling for all military spouses. The SECO website delivers the resources and tools necessary to assist military spouses with career exploration/discovery, career education and training, employment readiness, and career connections at any point within the military spouse's career lifecycle.

Records may also be used as a management tool for statistical analysis, tracking, reporting, evaluation of program effectiveness and conducting research.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM

Identify in clear, non-technical terms, the individuals about whom records are being maintained in the system.

- The language, when relevant, can include generalized descriptions such as, "all military personnel," "all civilians," or "Marine civilians." Foreign nationals should not be listed as a separate group since they do not meet the Privacy Act's definition of "individual."

References: *DoD 5400.11-R (page 58, C6.3.5); OMB Circular A-108 (page 38)*

Sample Format:
CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Participating spouses of members of the United States Armed Forces (military spouses).

CATEGORIES OF RECORDS IN THE SYSTEM

Describe in clear, non-technical terms the types of records maintained in the system. List the information most unique to the individual (e.g., name, SSN, passport number, etc.), followed by broader groupings (e.g., gender, race, ethnicity, employment and, education information, etc.), with broader categories listed third (e.g., personal contact information, work contact information, education information, employment information).

NOTE: If the system will maintain information from other systems, and/or data elements from multiple forms it should be noted in this section and in the Record Source category. The language can, when appropriate, include phrases such as "including but not limited to" or "may include" to allow for more flexibility.

Sample Format:
CATEGORIES OF RECORDS IN THE SYSTEM: Military spouse's name, DoD ID number, date of birth, gender, mailing and home address, years as military spouse, personal email address, personal cell and home telephone number, employment and education information, certificates and licenses, skills, abilities, and competencies.

NOTE: The name and number of the form must be listed in narrative statement, item 6.

References: *DoD 5400.11-R (page 58, C6.3.6); OMB Circular A-108 (page 38)*

RECORD SOURCE CATEGORIES

Describe where the Component obtained the information (source documents and other agencies) maintained in the system. Describe the record sources in general terms. "The individual" should always be listed first whenever information is collected from the individual who is the subject of the record.

References: *DoD 5400.11-R (page 62, C6.3.15); OMB Circular A-108 (page 38)*

Sample Format:
RECORD SOURCE CATEGORIES: The individual, security personnel, the Defense Manpower Data Center, Department of Defense Person Search (DMDC DPS), and the electronic Official Personnel Folder (eOPF).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES

List each authorized routine use (permitted disclosure) of the information outside the DoD which maintains the system of records. Each routine use should identify the third party to whom disclosure is authorized, the type of information to be disclosed, and the purpose for the disclosure.

- When writing specific routine uses, avoid general statements such as, "to other Federal agencies as required," or, "to any other appropriate Federal agency."
- List routine uses in this order: specific, those using model language for routine uses, and standard (required) routine uses.
- Routine uses will be identified alphabetically (e.g., a, b, c, d…).
- If a contractor maintains, accesses, collects PII, etc., on behalf of the Federal Government, include the model language for that routine use.

- ***Note:*** Blanket Routine Uses listed on the DPCLTD website should no longer be cited collectively in a New or Modified SORN. All applicable routine uses must be published in a SORN. Include each applicable model language routine use and all standard routine uses.

- List the routine uses in this order: Specific, those using model language, and standard.

The format for Specific Routine Uses must be:

To … for the purpose of …

Model Language for Routine Uses

The following reflects model language for routine uses. Note these are not "blanket" routine uses, nor should all of the model language included in this section be summarily copied into every system of records notice (SORN). Rather, model language is provided that should be used once it is determined a ***particular*** routine use is both related to and compatible with a particular system of records and appropriate for inclusion in the corresponding SORN. In some instances, the Component Office of General Counsel or Judge Advocate General should be consulted when considering establishing or making a disclosure from a record pursuant to any of these routine uses. Each new or modified routine use must include an explanation of how it satisfies the compatibility requirement of the Privacy Act. Any new or significantly modified routine uses require a minimum of 30 days after publication in the Federal Register before that routine use is effective. Once the 30 day criterion has been met, the routine use serves the basis for disclosure of any record in the system.

- 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.

- To designated officers and employees of Federal, State, local, territorial or tribal, international, or foreign agencies maintaining civil, criminal, enforcement, or other pertinent information, such as current licenses, if necessary to obtain information relevant and necessary to a DoD Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

- To designated officers and employees of Federal, State, local, territorial, tribal, international, or foreign agencies in connection with the hiring or retention of an employee, the conduct of a suitability or security investigation, the letting of a contract, or the issuance of a license, grant or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter and the Department deems appropriate.

- To contractors whose employees require suitability determinations, security clearances, and/or access to classified national security information, for the purpose of ensuring that

the employer is appropriately informed about information that relates to and/or may impact a particular employee or employee applicant's suitability or eligibility to be granted a security clearance and/or access to classified national security information.

- To a former DoD employee for the purpose of responding to an official inquiry by a Federal, State, local, territorial or tribal entity or professional licensing authority, in accordance with applicable DoD regulations; or for the purpose of facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the DoD requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

- To foreign or international law enforcement, security, or investigatory authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements, including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

- To unions recognized as exclusive bargaining representatives under the Civil Service Reform Act of 1978, 5 U.S.C. §§ 7111 and 7114, the Merit Systems Protection Board, arbitrators, the Federal Labor Relations Authority, and other parties responsible for the administration of the Federal labor-management program for the purpose of processing any corrective actions, or grievances, or conducting administrative hearings or appeals.

- To the Merit Systems Protection Board and the Office of the Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems; review of Office of Personnel Management or component rules and regulations; investigation of alleged or possible prohibited personnel practices, including administrative proceedings involving any individual subject of a DoD investigation.

- To the Office of Personnel Management (OPM) for the purpose of addressing civilian pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.

- To State and local taxing authorities with which the Secretary of the Treasury has entered into agreements under 5 U.S.C. §§ 5516, 5517, or 5520 and only to those state and local taxing authorities for which an employee or military member is or was subject to tax, regardless of whether tax is or was withheld. The information to be disclosed is information normally contained in Internal Revenue Service (IRS) Form W-2.

- To appropriate Federal, State, local, territorial, tribal, foreign, or international agencies for the purpose of counterintelligence activities authorized by U.S. law or Executive Order, or for the purpose of executing or enforcing laws designed to protect the national security or homeland security of the United States, including those relating to the sharing of records or information concerning terrorism, homeland security, or law enforcement.

- To any person, organization or governmental entity (e.g., local governments, first responders, American Red Cross, etc.), in order to notify them of or respond to a serious and imminent terrorist or homeland security threat or natural or manmade disaster as is necessary and relevant for the purpose of guarding against or responding to such threat or disaster.

- To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of an investigation or case arising from the matters of which they complained and/or of which they were a victim.

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

- To the news media and the public unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Note: All forms must spell out specific Routine Uses and provide a link to the SORN (in the purpose section of the Privacy Act Statement) to provide access to the remainder of the routine uses (model language and standard).

Standard Routine Uses: List in full the following routine uses that generally should be standard for every SORN and included in the same order for consistency. The Standard Routine Uses identified below have been determined by the SAOP to be necessary and proper:

- 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.

- 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.

- 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.

- 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.

- 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.

- To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that 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.

- 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.

Reference: *OMB Circular A-108*

Sample Format (text in parentheses is for informational purposes only, not included in SORN): **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 herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

[Specific Routine Use]

a. To a domestic or foreign entity that has entered into a public-private partnership with the Defense POW/MIA Accounting Agency (DPAA) as authorized by 10 U.S.C. 1501a, when DPAA determines that such disclosure is necessary to the performance of services DPAA has agreed shall be performed by the partner.

[Model Language Routine Uses]

b. 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.

c. To appropriate Federal, State, local, territorial, tribal, foreign, or international agencies for the purpose of counterintelligence activities authorized by U.S. law or Executive Order, or for the purpose of executing or enforcing laws designed to protect the national security or homeland security of the United States, including those relating to the sharing of records or information concerning terrorism, homeland security, or law enforcement.

[Standard Routine Uses]

d. 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.

e. 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.

f. 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.

g. 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.

h. 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.

i. To appropriate agencies, entities, and persons when (1) The Department of Defense (DoD) suspects or has confirmed that the security or confidentiality of the information in the system of records; (2) the DoD has determined that 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.

j. To another Federal agency or Federal entity, when the Department of Defense (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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS

Indicate the storage medium or media in which the records are maintained, e.g., electronic storage media, paper records, microfiche, etc.

References: DoD 5400.11-R (page 60, C6.3.10.1); OMB Circular A-108 (page 38)

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

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS

Specify how specific records in the system are retrieved, e.g., by name or other personal identifier.

References: DoD 5400.11-R (page 60, C6.3.10.2); OMB Circular A-108 (page 38)

Sample Format:
POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: The records are retrieved primarily by name, work email address, and DoD ID number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS

Indicate how long the record is retained by the Component, if and when records are transferred to a Federal Records Center, time of retention at the Records Center, and, if they are permanent records, when the records are transferred to the National Archives and Records Administration (NARA) or, if temporary, when the records are destroyed in accordance with DoD and NIST guidelines.

- Use plain language.
- Do not cite the Component disposition schedule regulation (e.g., AI-15) or file number (e.g., 202-46.1).
- DoD Components must use an approved and applicable NARA records retention schedule. The SORN must state the length of time the records are maintained by the DoD Component and if deemed permanent records when they are transferred to NARA for permanent retention. This may be coordinated with the Component Records Manager.
- If your Agency has requested NARA approval of the disposition scheduled, use the approved Disposition Pending statement until the Agency receives a final disposition.

References: DoD 5400.11-R (page 60, C6.3.10.4); OMB Circular A-108 (page 38).

Sample Format:
POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:
System records will be retained for 15 years after the service member separates/retires from active duty and then destroyed.

Disposition Pending Sample Format (SF-115 submission required):
Disposition pending until the National Archives and Records Administration has approved the retention and disposition schedule, treat as permanent. [Note: This language is used when the component has submitted an SF-115 to NARA. DPCLTD may require a copy of the SF-115].

ADMINISTRATIVE, PHYSICAL, AND TECHNICAL SAFEGUARDS

Describe the administrative, physical, and technical safeguards currently in place to minimize the risk of unauthorized access to or disclosure of records. Identify the categories of employees who are authorized to access to the records.

- Do not describe safeguards in such detail as to compromise system security.

References: DoD 5400.11-R (page 60, C6.3.10.3); OMB Circular A-108 (page 38)

Sample Format:
ADMINISTRATIVE, PHYSICAL, AND TECHNICAL SAFEGUARDS: Records are maintained in secure, limited access, and monitored areas. The database is monitored, access is password protected, and it is Common Access Card (CAC) enabled. Firewalls and an intrusion detection system are used. Physical entry by unauthorized persons is restricted through the use of locks, guards, passwords, and/or other security measures. Archived data is stored on compact discs, or magnetic tapes, which are kept in a locked, controlled access area. Access to personal information is limited to those individuals who require a need to know to perform their official assigned duties.

RECORD ACCESS PROCEDURES

Describe how an individual can gain access to the records about themselves in the system. The procedural rules should be cited with a brief procedural description of the data needed. DoD Components should provide sufficient information in the notice to allow an individual to exercise his or her rights without referral to the formal rules.

Describe the required proof of identity. Information requested from the individual should also be listed in the categories of records.

- Include the official title and address for requests.
- Identify the offices through which the individual may obtain access.
- Describe any proof of identify required.
- Include "certification" language.

References: DoD 5400.11-R (pp. 61-62, C6.3.13); OMB Circular A-108 (page 38).

Sample Format:
RECORD ACCESS PROCEDURES: Individuals seeking access to information about themselves contained in this system of records should address written requests to the Office of the Secretary of Defense / Joint Staff Freedom of Information Act Requester Service Center, 1155 Defense Pentagon, Washington, D.C. 20701-1155.

Signed, written requests should include the individual's full name, telephone number, street address, email address, and name and number of this system of records notice.

In addition, the requester must provide either a notarized statement or a declaration made in accordance with 28 U.S.C. 1746, using 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

DoD Component procedural rules for contesting a record must be codified in the CFR.

- Provide information on how individuals can locate Component procedural rules.
- Describe how the individual may contest the content of a record pertaining to them in the system.
- Inform the individual if they may also be referred to the system owner to determine the procedures.

References: DoD 5400.11-R (page 62, C6.3.14); OMB Circular A-108 (page 38).

Sample Format:
CONTESTING RECORD PROCEDURES: The Office of the Secretary of Defense (OSD) rules for accessing records, contesting contents, and appealing initial agency determinations are contained in OSD Administrative Instruction 81; 32 CFR part 311; or may be obtained from the system manager.

NOTIFICATION PROCEDURES

Describe how an individual can determine whether records pertaining to themselves are maintained in the system. Procedural rules should be cited, but a brief description should be included. Components should provide sufficient information in the notice to allow an individual to exercise their rights without referral to the formal rules.

- Include the official title and address for requests.
- Describe the specific information required to determine if the individual has records in the system.
- Describe what proof of identify is required with the request.
- Include the "certification" language.

- Other than contact information, information requested from the individual to retrieve or validate a record should also be listed in the categories of records.

References: DoD 5400.11-R (pp. 61, C6.3.12); OMB Circular A-108 (page 38).

Sample Format:
NOTIFICATION PROCEDURES: Individuals seeking to determine if information about themselves is contained in this system should address written inquiries to: Defense Technical Information Center; Attn: DTIC-UC, 8725 John J. Kingman Road, Fort Belvoir, VA 22060-6218.

Signed, written requests should contain the individual's full name, telephone number, street address, email address, and name and number of this system of records notice.

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

If no exemption has been established for the system, indicate "None." Exemptions must be aligned with the purpose and the authorities cited in the notice.

If an exemption is claimed under subsection (j) or (k) of the Privacy Act, cite the exemption and identify the CFR section containing the exemption rule for the system. Use the three-paragraph model, in which the first paragraph identifies the specific sections of the Privacy Act from which the System of Records is exempt. The second paragraph identifies the specific exemption for which the rule is established, and the third paragraph reflects compliance with the Administrative Procedures Act.

- All exemption rules must be approved through your Component/Agency Office of General Counsel.

- Provide a copy of the exemption rule as published in the FR or CFR (if previously published).

    - Reference: www.federalregister.gov or http://www.ecfr.gov/cgi-bin/ECFR?page=browse.

- Provide a copy of the Proposed Rule in the SORN package (if being proposed with the New or Modified SORN).

References: DoD 5400.11-R (page 62, C6.3.16); OMB Circular A-108 (page 38)

Sample Format:
EXEMPTIONS PROMULGATED FOR THE SYSTEM: The Department of Defense has exempted [is exempting] records maintained in [SORN Name and ID], from subsections [identify each applicable subsection from which an exemption is claimed] of the Privacy Act pursuant to 5 U.S.C. 552a [identify applicable exemption section].

[Paragraph(s) explaining the nature of the exemption cited, e.g., Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.]

An exemption rule for this system has been promulgated in accordance with requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e) and published in 32 CFR part 311. For additional information contact the system manager.

HISTORY

Citation(s) to the last full Federal Register notice that includes all of the elements that are required to be in a SORN, as well as any subsequent notices of partial revisions. List in order from the oldest (last published in full), then first modification, second modification, etc.

Reference: OMB Circular A-108 (page 39).

Sample Format:
HISTORY: 70 FR 21181, April 25, 20015; 73 FR 66852, November 12, 2008, and 75 FR 61135, October 4, 2010.

FEDERAL REGISTER NOTICE (PREAMBLE)

The Federal Register Notice, also called a Preamble, summarizes the information the agency submits to request a notice be published in the Federal Register as required by NARA Document Drafting Handbook: Information can be found at: https://www.archives.gov/files/federal-register/write/handbook/ddh.pdf.

DEPARTMENT OF DEFENSE

BILLING CODE:

Office of the Secretary
[This can also be: Department of the Army; Department of the Navy; or Department of the Air Force]

Docket ID: [This can also be: DoD-YYYY-HA-XXXX (DHA); USA-YYYY-XXXX (Army); USN-YYYY-XXXX (Navy); or USAF-YYYY-XXXX (Air Force)].

- **Sample Format: [Docket ID: DoD-2018-OS-XXXX]**

Privacy Act of 1974; System of Records

AGENCY: [Name of agency and, if applicable, agency component].

- **Sample Format:** Defense Logistics Agency, DoD.

ACTION: Notice of a [New/Modified] System of Records, or Rescindment of a System of Records Notice.

- Select the appropriate action that applies to the system. The submission will be for a New, Modified, or Rescindment system of records.

SUMMARY: [A plain-language description of the system. Briefly describe what the system does and the impact the changes will have on the system. Answer these three questions. What action is being taken? Why is this action necessary? What is the intended effect of this action? Use the following guidelines in preparing a summary:

- Use language a non-expert will understand.
- Refer to an act of Congress by the popular name of the act.
- Do not use legal citations, CFR citations, or EOs.
- State what your document does; do not include extensive background.
- Do not include qualifications, exceptions, or specific details.
- Be brief; however, must be more than one sentence.
- A rescindment only includes a simple summary of the system being rescinded].

Sample Format:

"The Office of the Secretary of Defense proposes to add a system of records entitled, "DoD Sexual Assault Prevention and Response Office Victim Assistance Data Systems, DHRA 18 DoD." This system is used to track victim-related inquiries received by the Sexual Assault Prevention and Response Office (SAPRO) via e-mail, SAPRO.mil, the DoD Safe Helpline, phone, or mail. Once received, inquiries are referred to the appropriate agency POC and or to the DoD IG for any complaints concerning the Military Criminal Investigative Organization in order to address the matter(s) raised and appropriately facilitate a resolution. In addition, the system will track and facilitate unrestricted and anonymous notifications of sexual abuse and harassment in Military Correctional Facilities, in accordance with the Prison Rape Elimination Act (PREA)."

DATES: [The deadline to submit comments on the proposal and the date on which any routine uses will be effective].

- DPCLTD will provide this information in this section.

Sample Format:

"DATES: Comments will be accepted on or before [**INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER**]. This proposed action will be effective on the date following the end of the comment period unless comments are received which result in a contrary determination."

ADDRESSES: [Instructions for submitting comments on the proposal, including an email address or a website where comments can be submitted electronically].

- DPCLTD will complete this section.

Sample Format:

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

* Federal Rulemaking Portal: http://www.regulations.gov.

Follow the instructions for submitting comments.

* Mail: Department of Defense, Office of the Chief Management Officer, Directorate of Oversight and Compliance, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350-1700.

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 http://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: [Instructions for submitting general questions about the system].

- Provide the name, title, office name, mailing address and phone number of the component privacy officer.

Sample Format:

FOR FURTHER INFORMATION CONTACT: Ms./Mr. [name of Component Privacy Officer], Department of the Army Privacy Office, 1234 Any Street, Ste 105, Alexandria, VA 12345-6789 or by calling (703) 123-4567.

SUPPLEMENTARY INFORMATION: [Background information about the proposal, including a description of any changes being made to the system and the purpose(s) of the changes].

- Tell what impact the changes will have on the system. Explain the statutory intent of the system. Tell what would happen if this system did not make this change.

Sample Format:

"SUPPLEMENTARY INFORMATION: The Sexual Assault Prevention and Response Office (SAPRO) is responsible for oversight of the Department's sexual assault policy per DoD Directive 6495.01, "Sexual Assault Prevention and Response (SAPR) Program," and helps ensure compliance with 28 CFR 115, Prison Rape Elimination Act National Standards. The SAPRO works hand-in-hand with the Military Services and the civilian community to develop, educate, and implement innovative sexual assault prevention and response programs to provide additional information to DoD personnel to increase awareness and promote reporting of sexual assaults. The DoD SAPRO Victim Assistance Data Systems provides the SAPRO with the necessary means to process and track victim-related inquires and PREA notifications received by the SAPRO.

The Office of the Secretary of Defense notices for systems of records subject to the Privacy Act of 1974, as amended, 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 http://dpcld.defense.gov/privacy.

The proposed systems reports, as required by of the Privacy Act, as amended, were submitted on [INSERT DATE], to the House Committee on Oversight and Government Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to Section 6 to OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," revised December 23, 2016 (December 23, 2016, 81 FR 94424).

Dated:

Aaron Siegel,
Alternate OSD Federal Register Liaison Officer, Department of Defense.

A-108 SYSTEM OF RECORDS NOTICE

Appendix II

OFFICE OF THE FEDERAL REGISTER SORN - FULL NOTICE

Agencies shall publish all system of records notices (SORNs) in the *Federal Register* using the appropriate format provided in the appendices to this Circular. Agencies shall use the language and section headings provided in the template and replace the language in brackets with the appropriate agency language.

Appendix II provides the Office of the Federal Register SORN template for full notices that include all of the required SORN elements. Agencies shall use this template when publishing a new SORN or choosing to publish a revised SORN in its entirety.

Federal Register Notice: This summarizes the information the agency submits to request a notice be published in the Federal Register as required by NARA Document Drafting Handbook. Information can be found at: https://www.archives.gov/files/federal-register/write/handbook/ddh.pdf. Please see page 32 for Federal Register Notice completion instructions.

SYSTEM NAME AND NUMBER: [A name for the system that is unambiguous and clearly identifies the purpose or character of the system, and the number of the system].

SECURITY CLASSIFICATION: [An indication of whether any information in the system is classified].

SYSTEM LOCATION: [The address of the agency and/or component responsible for the system, as well as the address of any third-party service provider].

SYSTEM MANAGER(S): [The title, business address, and contact information of the agency official who is responsible for the system].

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: [The specific authority that authorizes the maintenance of the records in the system].

PURPOSE(S) OF THE SYSTEM: [A description of the agency's purpose(s) for maintaining the system].

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: [The categories of individuals on whom records are maintained in the system].

CATEGORIES OF RECORDS IN THE SYSTEM: [The categories of records maintained in the system and, if practicable and useful for public notice, specific data elements].

RECORD SOURCE CATEGORIES: [The categories of sources of records in the system].

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: [Each routine use of the records contained in the system, including the categories of users and the purpose of such use].

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: [The policies and practices of the agency regarding the storage of records].

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: [The policies and practices of the agency regarding retrieval of records].

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: [The policies and practices of the agency regarding retention and disposal of records].

ADMINISTRATIVE, PHYSICAL, AND TECHNICAL SAFEGUARDS: [A description of the administrative, physical, and technical safeguards to which the system is subject].

RECORD ACCESS PROCEDURES: [The agency procedures whereby an individual can be notified at his or her request how he or she can gain access to any record pertaining to him or her in the system].

CONTESTING RECORD PROCEDURES: [The agency procedures whereby an individual can be notified at his or her request how he or she can contest the content of any record pertaining to him or her in the system].

NOTIFICATION PROCEDURES: [The agency procedures whereby an individual can be notified at his or her request if the system contains a record pertaining to him or her].

EXEMPTIONS PROMULGATED FOR THE SYSTEM: [Any Privacy Act exemptions promulgated for the system].

HISTORY: [Citation(s) to the last full *Federal Register* notice including all of the required SORN elements, as well as any subsequent notices of revision].

Appendix III

OFFICE OF THE FEDERAL REGISTER SORN - NOTICE OF REVISION

Agencies shall publish all system of records notices (SORNs) in the *Federal Register* using the format provided in the appendices to this Circular. Agencies shall use the language and section headings provided in the template and replace the language in brackets with the appropriate agency language.

Appendix III provides the Office of the Federal Register SORN template for revised notices that describe a modified system of records when the agency chooses not to publish the revised SORN in its entirety. The elements provided in the template are required to appear in any notice of a modified system of records. Elements omitted from the template shall be included in a notice of a modified system of records if there are revisions to those elements.

Federal Register Notice: This summarizes the information the agency submits to request a notice be published in the Federal Register as required by NARA Document Drafting Handbook. Information can be found at: https://www.archives.gov/files/federal-register/write/handbook/ddh.pdf. Please see page 32 for Federal Register Notice completion instructions.

SORN

The remainder of the Appendix should be followed in accordance with the SORN section below.

SYSTEM NAME AND NUMBER: [A name for the system that is unambiguous and clearly identifies the purpose or character of the system, and the number of the system.]

SECURITY CLASSIFICATION: [An indication of whether any information in the system is classified].

SYSTEM LOCATION: [The address of the agency and/or component responsible for the system, as well as the address of any third-party service provider.]

SYSTEM MANAGER(S): [The title, business address, and contact information of the agency official who is responsible for the system].

[Agencies shall review the other elements in the full SORN template in Appendix II to this Circular and include elements for which revisions are necessary. For example, if an agency is modifying the categories of records in the system, the agency shall include that element in the notice of revision.]

HISTORY: [Citation(s) to the last full *Federal Register* notice that includes all of the required SORN elements, as well as any subsequent notices of revision.]

Appendix IV

OFFICE OF THE FEDERAL REGISTER SORN - NOTICE OF RESCINDMENT

Agencies are required to publish a notice of rescindment in the *Federal Register* whenever they stop maintaining a previously established system of records. Agencies shall publish all notices of rescindment using the format provided in Appendix IV to this Circular. Agencies shall use the language and section headings provided in the template and replace the language in brackets with the appropriate agency language.

Federal Register Notice: This summarizes the information the agency submits to request a notice be published in the Federal Register as required by NARA Document Drafting Handbook. Information can be found at: https://www.archives.gov/files/federal-register/write/handbook/ddh.pdf. Please see page 32 for Federal Register Notice completion instructions.

SORN

The remainder of the Appendix should be followed in accordance with the SORN section below.

SYSTEM NAME AND NUMBER: [The name and number of the system that is being discontinued].

HISTORY: [Citation(s) to the last full *Federal Register* notice that includes all of the required SORN elements, as well as any subsequent notices of revision].

TEMPLATES

NARRATIVE STATEMENT TEMPLATE - NEW SORN

DEPARTMENT OF DEFENSE
Office of the Secretary of Defense
Narrative Statement for a New System of Records
Under the Privacy Act of 1974

1. System name and number: Spouse Education and Career Opportunities (SECO) Program, DPR 46 DoD.

2. Purpose of establishing the system: This system will deliver the resources and tools necessary to assist spouses of members of the United States Armed Forces (military spouses) with career exploration and discovery, career education and training, employment readiness, and career connections at any point within the military spouse's military career. Without this system of records, the military spouses would not have the tools necessary to further their education and training. Records may also be used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness, and conducting research.

3. Specific authority under which the system of records is maintained: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 1784, Employment opportunities for military spouses; 10 U.S.C. 1784a, Education and training opportunities for military spouses to expand employment and portable career opportunities; and DoD Instruction 1342.22, Military Family Readiness.

4. Evaluation of the probable or potential effect on the privacy of individuals: Unauthorized access to records is low due to SECO being hosted on a DoD Risk Management Framework life-cycle cybersecurity infrastructure. Records are maintained on a military installation in a secure building in a controlled area accessible only to authorized personnel. Records are encrypted during transmission to protect session information and at rest.

5. Routine use compatibility: The routine uses are consistent with the purpose for which the information was collected and have been determined to be necessary and proper for this system of records.

6. OMB public information collection requirements:
OMB collection required: Yes
OMB Control Number (if approved): 0704-0556
Title of Collection: Spouse Education and Career Opportunities Program
Date Submitted to OMB if Pending: N/A
Expiration Date (if approved): 8/31/2019

Provide titles of any information collection requests (e.g. forms and number, surveys, etc.) contained in the system of records: SECO Web Portal

If collecting on members of the public and no OMB approval is required, state the applicable exception(s): N/A.

Information Required by DPCLTD: (Not required to OMB)

7. Name of IT system (state NONE if paper records only): Spouse Education and Career Opportunities, DITPR #16792.

8. Is the system, in whole or in part, being maintained, (maintained, collected, used, or disseminated) by a contractor? No.

NARRATIVE STATEMENT TEMPLATE - MODIFIED SORN

DEPARTMENT OF DEFENSE
Defense Information Systems Agency
Narrative Statement for a Modified System of Records
Under the Privacy Act of 1974

1. System name and number: DoD Enterprise Portal Service (DEPS), K890.21.

2. Nature of proposed modifications for the system: Defense Information Systems Agency is proposing to modify the system of records. The change will expand the types categories of records in the system**,** authority for maintenance of the system, routine uses of records maintained in the system, including categories of users and the purposes of such uses, retention and disposal, system manager(s) and address, notification procedure, and records assess procedures, record source categories.

3. Specific authority under which the system of records is maintained: 5 U.S.C. 301, Departmental Regulations; Pub. L. 106-229, Electronic Signatures in Global and National Commerce; OASD(C3I) Policy Memorandum dated August 12, 2000, subject: Department of Defense (DoD) Public Key Infrastructure (PKI), OASD (C3I) Memorandum dated Jan 2001, subject: Common Access Card (CAC), and Government Paperwork Elimination Act 5 U.S.C. 301, Departmental Regulations, and E.O. 9397 (SSN), as amended.

4. Evaluation of the probable or potential effect on the privacy of individuals: In updating this SORN, the DEPS reviewed the safeguards established for the system to ensure they are compliant with the DoD requirements and are appropriate to the sensitivity of the information stored within the system.

5. Routine use compatibility: The first two routine uses are consistent with the purpose for which the information was collected. The remaining six routine uses have been determined to be necessary and proper.

6. OMB public information collection requirements:
OMB collection required: No
OMB Control Number (if approved): N/A
Title of Collection: N/A
Date Submitted to OMB if pending: N/A
Expiration Date (if approved): N/A

If collecting on members of the public and no OMB approval is required, state the applicable exception(s): Paragraph 8.a. (1) of Enclosure 3 in DoD Manual 8910.01 - Volume 1. There are also no internal collection requirements for this SORN.

Information Required by DPCLTD: (Not required by OMB)

7. Name of IT system (state NONE if paper records only): DEPS, DITPR ID# 12970.

8. Is the system, in whole or in part, being maintained, (maintained, collected, used, or disseminated) by a contractor? Yes.

FEDERAL REGISTER NOTICE TEMPLATE - NEW SORN

DEPARTMENT OF DEFENSE **BILLING CODE: 5001-06**

Office of the Secretary

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

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary, DoD.

ACTION: Notice of a New System of Records.

SUMMARY: The Office of the Secretary of Defense proposes to add a system of records entitled, "DoD Sexual Assault Prevention and Response Office Victim Assistance Data Systems, DHRA 18 DoD." This system is used to track victim-related inquiries received by the Sexual Assault Prevention and Response Office (SAPRO) via e-mail, SAPRO.mil, the DoD Safe Helpline, phone, or mail. Once received, inquiries are referred to the appropriate agency POC and or to the DoD IG for any complaints concerning the Military Criminal Investigative Organization in order to address the matter(s) raised and appropriately facilitate a resolution. In addition, the system will track and facilitate unrestricted and anonymous notifications of sexual abuse and harassment in Military Correctional Facilities, in accordance with the Prison Rape Elimination Act (PREA).

DATES: Comments will be accepted on or before [**INSERT 30 DAYS FROM DATE OF PUBLICATION IN THE FEDERAL REGISTER**]. This proposed action will be effective the date following the end of the comment period unless comments are received which result in a contrary determination.

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

* Federal Rulemaking Portal: http://www.regulations.gov.

Follow the instructions for submitting comments.

* Mail: Department of Defense, Office of the Chief Management Officer, Directorate for Oversight and Compliance, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350-1700.

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 http://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Luz D. Ortiz, Chief, Records, Privacy and Declassification Division (RPDD), 1155 Defense Pentagon, Washington, D.C. 20301-1155, or by phone at (571) 372-0478.

SUPPLEMENTARY INFORMATION: The Sexual Assault Prevention and Response Office (SAPRO) is responsible for oversight of the Department's sexual assault policy per DoD Directive 6495.01, “Sexual Assault Prevention and Response (SAPR) Program,” and helps ensure compliance with 28 CFR 115, Prison Rape Elimination Act National Standards. The SAPRO works hand-in-hand with the Military Services and the civilian community to develop, educate, and implement innovative sexual assault prevention and response programs to provide additional information to DoD personnel to increase awareness and promote reporting of sexual assaults. The DoD SAPRO Victim Assistance Data Systems provides the SAPRO with the necessary means to process and track victim-related inquires and PREA notifications received by the SAPRO.

The Office of the Secretary of Defense notices for systems of records subject to the Privacy Act of 1974, as amended, 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 http://dpcld.defense.gov/privacy.

The proposed systems reports, as required by of the Privacy Act, as amended, were submitted on [INSERT DATE], to the House Committee on Oversight and Government Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to Section 6 to OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," revised December 23, 2016 (December 23, 2016, 81 FR 94424).

Dated:

Aaron Siegel,
Alternate OSD Federal Register Liaison Officer, Department of Defense.

FEDERAL REGISTER NOTICE TEMPLATE - SORN RESCINDMENT

DEPARTMENT OF DEFENSE **BILLING CODE: 5001-06**

Office of the Secretary

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

Privacy Act of 1974; System of Records

AGENCY: Defense Information Systems Agency, DoD.

ACTION: Rescindment of a System of Records Notice.

SUMMARY: The Defense Information Systems Agency is rescinding a system of records, Incident Report Records, KEUR.03. These files were used by the Command Support Division, EUI.

DATES: Comments will be accepted on or before [**INSERT 30 DAYS FROM DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This proposed action will be effective the date following the end of the comment period unless comments are received which result in a contrary determination. The specific date for when this system ceased to be a Privacy Act System of Records is unknown; however, no actions involving private relief legislation have been processed by the Command Support Division, EU1 since 2015.

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

* Federal Rulemaking Portal: http://www.regulations.gov.

Follow the instructions for submitting comments.

* Mail: Department of Defense, Office of the Chief Management Officer, Directorate for Oversight and Compliance, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350-1700.

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 http://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: To submit general questions about the rescinded system, please contact Ms. Jeanette M. Weathers-Jenkins, DISA Privacy Officer, 6916 Cooper Ave, Fort Meade, MD 20775, or by phone at (301) 225-8158.

SUPPLEMENTARY INFORMATION: Based on a recent review, it was determined the Command Support Division, Defense Information Systems Agency no longer maintains a Privacy Act system of records for Incident Report Records. Legislative bills are tracked by bill number, rather than personal identifier.

The Office of the Secretary systems of records notices subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, 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 http://dpcld.defense.gov/.

The proposed changes to the record system being amended are set forth in this notice. The proposed amendment is not within the purview of subsection (r) of the Privacy Act of 1974 (5 U.S.C. 552a), as amended, which requires the submission of a new or altered system report.

Dated:

Aaron Siegel,
Alternate OSD Federal Register Liaison Officer, Department of Defense

SORN TEMPLATE - NEW SORN

SYSTEM NAME AND NUMBER: Facilities Access Electronic Information System (OnGuard, formerly Diamond II/Argus), MDA X01.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: MDA, 5222 Martin Road, Redstone Arsenal, AL 35898.

SYSTEM MANAGER(S): Deputy Chief Information Officer, Enterprise Network Operations, MDA, 730 Irwin Ave, Schriever AFB, CO, 80912, 719-721-8826, email: MDAPrivacyOffice@mda.mil.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Executive Order 10450 Security requirements for Government employment and E.O. 9397 (SSN), as amended.

PURPOSE(S) OF THE SYSTEM: The system's purpose is to collect information to verify the security clearance of persons accessing MDA facilities. The information may be shared with other Federal, State, and local agencies for investigation purposes only. This information is used in the performance of official duties related to determining the eligibility of individuals for access to facilities and classified information.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: All MDA government, contractors, and visitors accessing MDA secured facilities.

CATEGORIES OF RECORDS IN THE SYSTEM: Name(s), SSN, DoD ID Number, and security clearance information.

RECORD SOURCE CATEGORIES: Individuals.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: To MDA facility security managers for verifying the security clearance of persons accessing facilities. The

information is used in the performance of official duties related to determining the eligibility of individuals for access to facilities and classified information. The information may be shared with other Federal, State, and local agencies for investigation purposes only.

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

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: The records are retrieved primarily by name and DoD ID number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Visitor control files are temporary and destroyed 5 years after final entry or 5 years after date of document, as appropriate. Expired data is purged.

ADMINISTRATIVE, PHYSICAL, AND TECHNICAL SAFEGUARDS: Administrative: backups secured off-site, encryption of backups, methods to ensure only authorized personnel access to PII, periodic security audits, and regular monitoring of users' security practices. Technical: Common Access Card, DoD public key infrastructure certificates, encryption of data at rest, encryption of data in transit, firewall, intrusion detection system, least privilege access, role-based access control, used only for privileged (elevated roles), virtual private network, and encrypted database. Physical safeguards: cipher locks, closed circuit TV, key cards, and security guards.

RECORDS ACCESS PROCEDURES: Individuals seeking access to information about themselves contained in this system of records should address written requests to the Office of the Secretary of Defense/Joint Staff Freedom of Information Act Requester Service Center, 1155 Defense Pentagon, Washington, D.C. 20701-1155.

Signed written requests should include the individual's full name, telephone number, street address, email address, and name and number of this system of records notice.

In addition, the requestor must provide either a notarized statement or a declaration made in accordance with 28 U.S.C. 1746, using 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 Office of the Secretary of Defense (OSD) rules for accessing records, contesting contents, and appealing initial agency determinations are contained in OSD Administrative Instruction 81; 32 CFR part 311; or may be obtained from the system manager.

NOTIFICATION PROCEDURES: Individuals seeking to determine if information about themselves is contained in this system should address written inquiries to MDA; Attn: ICT, Deputy Chief Information Officer, Enterprise Network Operations, 730 Irwin Ave, Schriever AFB, CO 80912.

Signed, written requests should contain the individual's full name, telephone number, street address, email address, and name and number of this system of records notice.

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: N/A

SORN TEMPLATE - MODIFIED SORN

SYSTEM NAME AND NUMBER: Data Warehouse Business Intelligence System (DWBIS), N05220-1.

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: Naval service members assigned to SPAWAR, SPAWAR civilian employees and government contractors directly supporting SPAWAR.

CATEGORIES OF RECORDS IN THE SYSTEM: Name, work and home mailing address, 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 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.

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 US 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.