

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 single line spacing
- No auto formatted lines before or after the paragraph
- Page numbers in the bottom right corner of the footer
- Section headings are to be **BOLDED** and **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 OF THE SYSTEM**
7. **CATEGORIES OF INDIVIDUALS COVERED BY THE SYTEM**
8. **CATEGORIES OF RECORDS IN THE SYSTEM**
9. **RECORD SOURCE CATEGORIES**
10. **ROUTINE USES OF RECODS MAINTAINED IN THE SYTEM, 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, TECHNICAL, AND PHYSICAL SAFEGUARDS**
15. **RECORDS ACCESS PROCEDURES**
16. **CONTESTING RECORD PROCEDURES**
17. **NOTIFICATION PROCEDURES**
18. **EXEMPTIONS PROMULGATED FOR THE SYSTEM**
19. **HISTORY - NEW REQUIREMENT**

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
 - Limited to 21 positions
 - 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.

SORN ALPHA IDENTIFIER AGENCY 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 a specifically established as a k(1) exemption under the Privacy Act, this will be “Unclassified”

Sample Format:

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION:

The address of the Component responsible for the system, as well as the address of any third-party 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 strongly suggested.

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

List authorities in the following order:

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

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 program effectiveness and conducting research.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Identify in clear, non-technical terms, the specific 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 individuals, 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.
- Explain how each new or modified routine use satisfies the compatibility requirement of the Privacy Act. These explanations should establish why the disclosure 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.
- 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.
- **DPCLTD will update this section relating to compatibility language at a future date.**

- **Note:** Blanket Routine Uses that are listed on the DPCLTD website should no longer be cited collectively in a new or modified SORNs. All routine uses that apply 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 that 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 has been determined that 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]

- 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]

- 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 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 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 approved and applicable National Archives and Records Administration (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 are retained and disposed of according to DoD records maintenance and disposition schedules and the requirements of the National Archives and Records Administration.

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 is language used when the component has submitted a SF115 to NARA. DPCLTD may require a copy of the SF115.]

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 have 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. Database is monitored, access is password protected, and common access card (CAC) enabled. Firewalls and 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, DC 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 a 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, 2005; 73 FR 66852, November 12, 2008, and 75 FR 61135, October 4, 2010.

OMB A-108 SYSTEM OF RECORDS NOTICE TEMPLATES

Appendix II

OFFICE OF THE FEDERAL REGISTER SORN TEMPLATE – 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 elements that are required to be in a SORN. Agencies shall use this template when publishing a new SORN or choosing to publish a revised SORN in its entirety.

Preamble: 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>

[Name of agency]

- Example format: DEPARTMENT OF DEFENSE

Privacy Act of 1974; System of Records

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

- Example format: Department of the Army

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

- Select the appropriate action that applies to the system. The submission will be for either 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.

Example format:

“The Office of the Secretary of Defense proposes to add a new system of records, Spouse Education and Career Opportunities, (SECO) Program, DPR 46 DoD. This program makes available the resources and tools to help military spouses with career exploration and discovery, career education and training, employment readiness, and career connections at any point within the military spouse’s career lifecycle. The records allow the spouse to build a