UNITED STATES SPECIAL OPERATIONS COMMAND

7701 Tampa Point Boulevard

MacDill Air Force Base, Florida 33621–5323

USSOCOM DIRECTIVE

Number 25-53 **XX March 2020**

Information Management – Records Management

PRIVACY ACT PROGRAM – PRIVACY AND CIVIL LIBERTIES

Table of Contents

Table of Contents (Cont.)

SECTION I – GENERAL

1. Purpose. This directive establishes policies, procedures and responsibilities for implementing the U.S. Special Operations Command (USSOCOM) PA Program governing collecting, safeguarding, maintaining, using, accessing, amending, and disseminating personal information maintained by USSOCOM System of Records. This is a supplement to the Department of Defense Instruction (DODI) 5400.11, *DOD Privacy Program,* 29 January 2019.

2. Applicability. This directive applies to Headquarters (HQ), USSOCOM, U.S. Army Special Operations Command, Naval Special Warfare Command, Air Force Special Operations Command, U.S. Marine Corps Forces Special Operations Command, Joint Special Operations Command, Special Operations Command Central, Special Operations Command South, Special Operations Command North, Special Operations Command Europe, Special Operations Command Africa, Special Operations Command Pacific, and Special Operations Command Korea, collectively referred to as the USSOCOM Enterprise. Additionally, Contractors are considered employees of USSOCOM during the performance of their contract.

a. This directive provides guidance in accordance with (IAW) the DOD Privacy Program and the Privacy Act of 1974 (section 552a of title 5 U.S. Code (U.S.C)).

b. This directive does not provide guidance on:

(1) Requests for information made under the Freedom of Information Act (FOIA). They are processed IAW DOD Directive (DODD) 5400.7 DOD Freedom of Information Act Program, and 32 Code of Federal Regulations Part 286 DOD Freedom of Information Act Program.

(2) Requests for information from systems of records controlled by the Office of Personnel Management (OPM), even if maintained by a DOD component. These are processed IAW policies established by OPM.

(3) Requests for personal information from Congress. These are processed IAW DODI 5400.4, Provision of information to Congress.

3. Objectives. To balance USSOCOM's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from collection, maintenance, use, and disclosure of PII (Examples of PII are shown in Appendix E).

a. Establishes a code of fair information practices.

b. Restricts disclosure of personally identifiable records.

c. Grants individuals an increased right of access to records about them.

d. Allows individuals the right to seek amendment of records that are not accurate.

4. Responsibilities. See Appendix A.

5. Definitions. See Glossary, Section II.

6. References. See Glossary, Section III.

7. Background. The PA is governed by the Public Law and DOD Regulations. The USSOCOM Privacy Program is a supplement to the DOD Regulation to provide guidance specific to the needs of USSOCOM. This program is closely related to the Freedom of Information Act (FOIA) Program.

a. **PA.** The PA of 1974 and this directive apply to information contained in USSOCOM PA System of Records. An official system of records are authorized by law or Executive Order (E.O.) and required to carry out a USSOCOM mission or function.

b. **Relationship between PA and FOIA (5 U.S.C. Section § 552).** Both statutes require statutory disclosures. When someone requests information, the request will be considered under both statutes regardless of the Act cited; however, there is no requirement to cite either Act if the records are contained within a system of records. This is to ensure the requester(s) are given the maximum amount of information as authorized under both statutes IAW DODI 5400.11. Only if the record can be denied under both statutes may USSOCOM withhold the records from the requester.

c. **Sensitive Unit Status.** IAW the Office of the Secretary of Defense (OSD) Memorandum dated September 21, 2001, the USSOCOM Enterprise, which includes the Military Service components and Theater Special Operations Commands (TSOCs), are designated as a *Sensitive Unit*, thereby authorizing the withholding of PII regarding personnel assigned to an overseas, sensitive or routinely deployable unit and accordingly exempt from the release under the FOIA, 5 U.S.C. Section 552 (b)(3), 10 U.S.C., Section 130b. As a result, all PII will be protected IAW USSOCOM D 530-1, *Operations Security.* In brief, all names, telephone numbers and e-mail addresses will be withheld from the public. Additionally, all PII contained in either written or electronic documents/e-mails will be protected as *For Official Use Only* (FOUO) and marked IAW DOD Manual (DODM) 5200.01 Volume 4, *Controlled Unclassified Information.* Exceptions to the designation of the sensitive unit status include the Joint Special Operations University (JSOU) personnel and members of the command that routinely work with the public. See USSOCOM D 530-1 for more information.

SECTION II – POLICY

8. General. All USSOCOM Enterprise personnel have a direct, independent and individual responsibility to ensure PII is collected, maintained, used and disseminated only as authorized by law and applicable regulations. Personnel are further required to protect all PII, hard copy and/or electronic versions, from unauthorized use, access, disclosure, alteration, or destruction. PII **will not be released** outside of the Privacy Statement guidelines or to anyone who does not have a duty-related official need to know.

a. **USSOCOM Enterprise Personnel shall not:**

(1) Keep records on how a person exercises First Amendment rights. *Exceptions* are when USSOCOM has the permission of that individual or authorized by federal statute, or the information pertains to an authorized law enforcement activity.

(2) Penalize or harass an individual for exercising rights guaranteed under the PA and will give reasonable aid to individuals exercising their rights.

(3) Disclose an individual's Social Security Number (SSN) or DOD identification (ID) Number without an official need to know; this includes disclosing to personnel in USSOCOM and DOD-wide. Outside the DOD, SSN or DOD ID Number is not releasable under the DOD PA Program without the individual's consent, unless authorized under 1 of the 12 exceptions to the *No Disclosure Without Consent* Rule (DODI 5400.11).

b. **USSOCOM Enterprise Personnel shall:**

(1) Secure and safeguard PII provided by USSOCOM personnel, USSOCOM Foreign Liaison Officers (FLO) and Exchange Officer Personnel, limiting access of PII only to those with a valid need to know. PII pertaining to FLO or Exchange Officers will have limited access to their PII unless host country has authorized the release of such PII to other countries and DOD. When stored in electronic media, PII will be secured by use of username/password or common access card (CAC) enabled security measures.

(2) Label or mark any list of USSOCOM personnel, USSOCOM FLOs or National representatives created UNCLASSIFIED//FOUO at a minimum and the Releasable (REL) added as appropriate to allow access to those with an official need to know or to those with an official purpose.

(3) Keep paper and electronic records containing personal information and retrieved by name or personal identifier only in approved systems of records published in the Federal Register.

(4) Collect, maintain, and use information in such systems only to support programs authorized by law or E.O.

(5) Safeguard records included in the systems and keep them the minimum time required. See Appendix B for additional guidance on safeguarding records.

(6) Report breaches IAW procedures outlined in Appendix C. This includes reporting any potential or actual breach to the respective command's Privacy Officer as soon as it is discovered. This is followed by conducting notification procedures required to any personnel affected by the breach.

(7) Keep records timely, accurate, complete, and relevant.

(8) Amend and correct records on request.

(9) Allow individuals to review and receive copies of their own records unless an exemption for the system exists or records were created in anticipation of a civil action or proceeding.

(10) Provide a review of decisions that deny individuals access to or amendment of their records.

9. Jurisdiction. The USSOCOM Privacy Program applies to USSOCOM systems of records.

a. Most systems of records fall under the respective Military Service components (e.g., military service records, evaluations, etc.). Any requests for records in a system belonging to a Military Service component will be handled IAW their appropriate regulation.

b. All systems of records created for USSOCOM will be handled IAW this Directive.

10. Personal Notes. The PA does not apply to personal notes on individuals for use as memory aids to supervise or perform other official functions that are not shared with others.

11. Systems of Records Operated By a Contractor. Contractors who are required to operate or maintain a PA system of records by contract are considered employees of USSOCOM during the performance of the contract. The record system affected is maintained by USSOCOM and is subject to this directive. Offices that have contractors operating or maintaining such record systems must ensure the contract contains the proper PA clauses, and identify the record system number. Records maintained by the contractor for the management of contractor employees are not subject to the PA.

12. Medical Information. Military Service Component Commanders (CDRs), Sub-unified CDRs, Directors, Division Chiefs, Functional Managers, and Supervisors within USSOCOM, where appropriate, are responsible for ensuring the handling and release of Protected Healthcare Information (PHI) IAW DOD 6025.18-R, *DOD Health Information Policy Regulation* and the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

13. Access Requests by Individuals.

a. **First Party Requests for Personal Information.** USSOCOM members or their designated representatives may request a copy of their records in a system of records from the office that maintains the records or through the Command FOIA/PA/Civil Liberties Branch (SOCS-SJS-VI).

(1) Requesters do not need to state why they want access to their records. Requesters should describe the records they want, with at least a type of record or functional area if they do not have the system of records number. For *all records about me* requests, refer the requester to https://www.dpcltd.defense.gov/Privacy/SORNs-to review Systems of Records published in the Federal Register.

(2) Requesters should not use government equipment, supplies, stationery, postage, telephones, or official mail channels for making PA requests.

(3) The privacy office receiving the request will verify the identity of the requester to avoid unauthorized disclosures. The privacy office receiving the request will respond to PA requests within 10 working days of receipt, or send a letter explaining why the request cannot be responded to within 3 working days with an accompanying approximate completion date.

(4) If records exist, the office receiving the request will provide the records to the command's Privacy Office for final release determinations.

(5) The requester should be shown or given a copy of the record within 30 working days unless the system is exempt (See Appendix D for a list of exemptions). If the system is exempt, the requester will be provided any parts of the request releasable under FOIA (coordinate with the FOIA office for disclosure).

(6) Any information withheld will cite the appropriate exemptions from the PA and FOIA in addition to appeal rights (See Appendix D for PA exemptions).

(7) If the requester wants another person present during the records review, the system manager may ask for written consent to authorize discussing the record with another person present.

b. **Third Party Information.** Normally, when information in a requester's record is *about* or *pertains to* a third party, it is not considered the requester's record and should not be released. This is not considered a denial. However, if the denial of the record will result in the requester's denial of a right, privilege, or benefit, the requester must be given access to relevant portions. If the request pertains to non-judicial punishment or loss of privileges, appropriate portions shall be released (they are not exempt).

c. **Civil Action Information.** Records compiled in connection with a civil action or other proceeding, including any action where USSOCOM expects judicial or administrative adjudicatory proceedings will not be released. This exemption does not include criminal actions. Attorney work products prepared before, during, or after the action or proceeding will not be released.

d. **Denial of Individual Access.** The USSOCOM Senior Component Official for Privacy (SCOP), and when designated, the USSOCOM Privacy Program Officer (Chief, SOCS-SJS-VI), are the USSOCOM Privacy Act denial authorities for USSOCOM records.

(1) Access denials are processed within 20 working days from receipt of the request for access.

(2) The System Manager for the information requested will prepare the *Recommendation for Access Denial* package to include a copy of the request, the record requested, and applicable exemption(s) under the PA and FOIA.

(3) USSOCOM Privacy Officer will coordinate proposed denials with the command denial authority. Notification of denials to requesters will include statutory authority, reason, and pertinent appeal rights.

(4) The system of record must have an approved exemption published as a final rule in the Federal Register prior to the request to be exempted IAW DODI 5400.11; the exemption must cover each document (all parts of a system are not automatically exempt). Nonexempt portions of the request will be segregated and processed for release.

e. **Appeal Procedures.** Individuals may request a denial review within 60 calendar days after receiving a denial letter through the USSOCOM Privacy Officer.

(1) The USSOCOM Privacy Officer (Chief, SOCS-SJS-VI) will compile the appeal package to include the original appeal letter, the initial request, the initial denial, a copy of the record, any internal records or coordination actions relating to the denial, denial authority comments on the appellant's arguments, and legal reviews, if applicable, and forward to the appeal authority: Defense Privacy, Civil Liberties and Transparency Division (DPCLTD), 4800 Mark Center Drive, ATTN: DPCLTD Mailbox 24, Alexandria, VA 22350-1700.

(2) If the appeal authority DPCLTD reverses an earlier denial and grants access or amendment, the requester will be notified immediately and records will be released as directed by DPCLTD.

f. **Amendment of Records.** Individuals may ask to have their records amended to make them accurate, timely, relevant, or complete. Most requests for amendment will be processed IAW regulations of the requester's respective Military Service component because most systems of records are owned by the Military Service components.

(1) Systems managers will routinely correct a record if the requester can show that it is factually wrong.

(2) Anyone may request minor corrections orally. Requests for more significant modifications should be in writing to the office or agency responsible for maintaining the record.

(3) Requests for amendment will be acknowledged within 10 working days of receipt. An expected completion date should be given unless the change is completed within the initial 10 working days. Final decisions should be made within 30 working days. Under exceptional circumstances, it may take longer than 30 days to reach a decision on a request to amend. Any decision that takes more than 30 days to resolve requires documentation with detailed reason/circumstances for the delay in the case file.

(4) After verifying the identity of the requester, the receiving office will make the change, notify all known recipients of the record, and inform the individual.

(5) USSOCOM will not usually amend a record when the change is based on opinion, interpretation, or subjective official judgment. This type of action constitutes a denial, and requesters may appeal.

(6) If the system manager decides not to amend or partially amend the record, they will send a copy of the original request, the record, and the recommended denial reasons to their respective Military Service component Privacy Officer or the USSOCOM Privacy Officer (Chief, SOCS-SJS-VI), depending on who owns the system of record. The Privacy Officer will coordinate with the command denial authority for USSOCOM records.

(7) If the denial authority approves the request, the system manager will amend the record and notify all previous recipients of the change. Denial notification to requesters will include the statutory authority, reason, and pertinent appeal rights.

g. **Case Files.** A PA case file is required for all requests under the PA and will include requests from and replies to individuals on whether a system has records about them; requests for access or amendment; approvals, denials, appeals, and final review actions; and coordination actions and related documents. Untimely responses and the associated reasons must also be documented.

(1) The file will only be used for statistical purposes (e.g., identify trends), to process requests and as a historical file in the event of an appeal to a request. Case files will not be used to make any kind of determination about an individual.

(2) Case files will be maintained IAW the Joint Staff and Combatant Command Records Management Manual Volume II – *Disposition Schedule*, which requires PA Requests to be maintained for 7-10 years.

h. **Reproduction Fees.** Fees will only be used to recoup direct reproduction costs associated with granting access. There is not a minimum fee for duplication or any automatic fees assessed IAW DODI 5400.11.

14. Access by Other Agencies and Third Parties. Before releasing personal information to third parties, consider the consequences, check accuracy, and ensure no law or directive bans disclosure.

a. **Consent.**

(1) Personal information can be released to third parties when the person(s) identified in the request gives permission verbally or in writing. Before including personal information such as home addresses, home phones, and similar information on social rosters or directories, written consent statements must be obtained. Otherwise, the information shall not be included.

(2) Written consent must be obtained before releasing a SSN, DOD ID Number, marital status, number and sex of dependents, race, civilian educational degrees and major areas of study (unless the request for information relates to the professional qualification for federal employment), school and year of graduation, home of record, home address and phone/mobile numbers, age and date of birth, present or future assignments for overseas or for routinely deployable or sensitive units, and office and unit address and duty phone for overseas or for routinely deployable or sensitive units. ***(NOTE:** Items listed are not all inclusive.)*

b. **Third Parties.** Requests by other individuals (third parties) for the records of individuals that are contained in a system of records shall be processed under the FOIA IAW DODI 5400.11. USSOCOM is designated as a sensitive unit, which restricts the release of any PII concerning individuals assigned to the USSOCOM Enterprise. The PII of individuals in sensitive units should be marked FOUO.

c. **Official Use.** Information obtained by authorized individuals for official purposes on a need to know basis from existing systems of records in USSOCOM include:

(1) Miscellaneous personnel management actions (alert or recall rosters; wartime, mobility, emergency actions or assignments; shelter duties or assignments, etc.); off-duty employment information; and ON *A VOLUNTARY PROVIDED BASIS ONLY*, an individual's involvement in off-duty activities for rendering performance/evaluation reports.

(2) Dependent (spouse and children) information (name, age, sex, nationality, home address, home telephone number, etc.) and special needs such as availability of special education or treatment facilities. (***NOTE:*** *Dependent information used for unofficial or quasi-official use will be ON A VOLUNTARY BASIS ONLY.)*

(3) Information for social rosters (name, address, phone number, official title or position, invitations, acceptance, regrets, protocol) to include dependent information will be obtained *ON A VOLUNTARY BASIS ONLY.*

(4) Information for special events planning (biographical data including, but not limited to: Name, duty, and home address) telephone numbers; name of spouse and family members; description of position in business and community affiliations with military-oriented civic organizations; and photos will be *ON A VOLUNTARY BASIS ONLY*.

d. **Privacy Expectation.** When disclosing other information, consideration should be given to whether the subject has a reasonable expectation of privacy for the information requested, and if disclosing the information would benefit the public. USSOCOM considers information as meeting the public interest standard if it reveals anything regarding the operations or activities of the agency, or performance of its statutory duties. When deciding the release of information, the public interest must be balanced with the individual's probable loss of privacy. The requester's purpose, circumstances, or proposed use will not be considered.

e. **Non-Consensual Conditions of Disclosures.** These are exceptions to the *no disclosure without consent.* USSOCOM may release information without consent to:

(1) FOIA requests when information is releasable.

(2) Officials or employees within DOD with a need to know.

(3) Agencies outside DOD for a routine use as published in the Federal Register. The purpose of the disclosure must be compatible with the purpose of the routine use. When an Agency initially collects the information from personnel, the *Routine Uses* block in the PA Statement must name the agencies involved and the reason for collection.

(4) The Bureau of the Census to plan or carry out a census or survey under Title 13, U.S. Code., Section 8.

(5) A recipient for statistical research or reporting. The recipient must give advanced written assurance that the information is for statistical purposes only. Records will only be released in a de-identified format that makes it impossible to identify any personnel from the data provided. (***NOTE:*** *No one may use any part of the record to decide an individual's rights, benefits, or entitlements)*

(6) The Archivist of the U.S. and the National Archives and Records Administration to evaluate records for permanent retention.

(7) A federal, state, or local agency (other than DOD) for civil or criminal law enforcement. The requesting law enforcement agency must send a written request to the system manager specifying the record or part needed and the law enforcement purpose. The system manager may also disclose a record to a law enforcement agency if the agency suspects a criminal violation. This disclosure is a routine use for all DOD systems of records and is published in the Federal Register.

(8) An individual or agency that needs the information for compelling health or safety reasons. The affected individual need not be the subject of record.

(9) Congress, a congressional committee, or a subcommittee, for matters within their jurisdictions.

(10) A congressional office acting on behalf of the person of record. A published, blanket routine use permits this disclosure. If the material for release is sensitive, obtain a release statement from the individual of record prior to disclosure.

(11) The Comptroller General or an authorized representative of the General Accounting Office (GAO) for official business.

(12) A court order from a court of competent jurisdiction, signed by a judge.

(13) A consumer credit agency according to the Debt Collections Act when a published system notice lists this disclosure as a routine use.

f. **Denial of Access.** The denial and appeal procedures for third party access are the same as denial procedures for individual access. See above for more information.

15. Exemptions. A system manager who believes that a system of records needs an exemption from some or all of the requirements of the PA should send a request through SOCS-SJS-VI to the DPCLTD office. The request should detail the reasons for the exemption, the section of the Act that allows the exemption, and specific subsections of the PA from which the system is to be exempted, with justification for each subsection. Denial authorities can withhold records using these exemptions only if they were previously approved and published as an exemption for the system in the Federal Register. USSOCOM Systems of Records that are exempt are listed in the Federal Register and on the USSOCOM Portal. Exemption types include:

a. General exemptions that free a system from most parts of the PA.

b. Specific exemptions that free a system from only a few parts.

16. Publication Requirements. Systems, portals and/or databases that collect PII must be implemented IAW applicable DOD guidelines and if required, published to the Federal Register using a System of Records Notice (SORN).

a. USSOCOM must publish SORNs via DPCLTD to the Federal Register to inform the public of the systems of records USSOCOM keeps and give the public an opportunity to comment. This includes starting a new system, instituting significant changes to an existing system, sending out data collection forms or instructions, and issuing a request for proposal or invitation for bid to support a new system.

b. Program or system managers must send a proposed SORN to the SOCS-SJS-VI in the Federal Register format found in Appendix 5, DODI 5400.11 before implementing a new system of records or instituting a major change to an existing system of records.

c. Privacy Impact Assessments (PIA). Program or system managers are responsible for conducting a PIA as required by DOD Instruction (DODI) 5400.16. Generally, a PIA is required for information systems and electronic systems that collect PII about DOD personnel and contractors.

(1) DD Form 2930, **Privacy Impact Assessment (PIA)**, will be used to record all PIAs.

(2) The USSOCOM Privacy Officer will maintain a central repository of all PIAs for USSOCOM systems until the PII is no longer maintained in the system or the system is not in operation.

17. Training Requirements. All personnel within the USSOCOM Enterprise will complete PA training annually. At a minimum this training will include PA Training required by each individual's respective Military Service component. Remedial training will be conducted by those that mishandle privacy information as directed by the SCOP or Privacy Officer.

a. Additional specialized training is needed for personnel who may be expected to deal with the news media or the public, human resource specialists, finance officers, information managers, supervisors, and individuals working with medical and security records. The DOD offers training workshops, with a schedule of workshops available at: https://intelshare.intelink.gov/sites/foiaprivacytrainingworkshops/.

b. Privacy Managers designated within USSOCOM will receive additional training from the Privacy Officer.

18. Reports. The USSOCOM Privacy Officer is responsible for all reports required by the Defense Privacy Office. Any input needed from the USSOCOM Enterprise to compile reports will be tasked via the Task Management Tools (TMTs).

19. Inspections.

a. System managers will review and validate their PA SORNs annually and submit changes through their respective Privacy Officers or Managers to SOCS-SJS-VI or Military Service component for processing through the DPCLTD as required.

b. USSOCOM Privacy Officer will conduct inspections and training within the SOCOM Enterprise annually in coordination with the USSOCOM Inspector General (SOIG) inspections.

c. Inspections of the USSOCOM Portals for sensitive PII will occur on a regular basis. Non-sensitive PII (full name, rank, work phone, work e-mail, office code and assigned position) is permitted and necessary for the daily functioning of the command (See Appendix B). If unsecured sensitive PII is found on the portals, it will be locked down and action will be taken to secure it appropriately. Remedial training will be conducted with the personnel responsible for the information. CDRs/Directors may initiate an investigation or inquiry into any incident.

20. PA Violations. Any suspected violations will be reported to the local Privacy Officer. If not available, reports will be given to the next higher command's Privacy Officer. Within the USSOCOM Enterprise, the USSOCOM Privacy Officer (Chief, SOCS-SJS-VI) will be notified of any suspected Privacy Act violation by the local Privacy Officer. All violations of the PA will be handled IAW DODI 5400.11.

21. Computer Matching Program Procedures. Computer matching programs electronically compare records from two or more automated systems that may include DOD, another Federal agency, or a state or other local government. All computer matching programs will be conducted IAW DODI 5400.11.

22. Proponent. The proponent for this directive is the Special Operations Command Support Directorate (SOCS), Secretary Joint Staff (SOCS-SJS), Command Freedom of Information (FOIA)/Privacy Act (PA)/Civil Liberties Branch (SOCS-SJS-VI). Users are invited to send comments and suggested improvements directly to SOCS-SJS-VI at: NIPR: foia@socom.mil; SIPR: foia@socom.smil.mil; Comm: 813-826-3715.

(SOCS-SJS-VI)

FOR THE COMMANDER

OFFICIAL:

TONY D. BAUERNFEIND
Major General, U.S. Air Force
Chief of Staff

ROBERT M. HICKS
Lieutenant Colonel, U.S. Army
Secretary Joint Staff

DISTRIBUTION: A, B, C, D

DISTRIBUTION NOTICE: USSOCOM PUBLICATIONS SHALL NEVER BE RELEASED OUTSIDE OF THE SPECIAL OPERATIONS FORCES COMMUNITY WITHOUT PRIOR APPROVAL FROM THE FOREIGN DISCLOSURE OFFICE (FDO), THE OPERATIONS SECURITY (OPSEC) OFFICE, FOIA OFFICE, AND THE PROPONENT OF THE PUBLICATION. ANY REQUESTS FOR COMMAND PUBLICATIONS FROM AN OUTSIDE ENTITY MUST BE VETTED THROUGH THE FDO, OPSEC, FOIA, AND PROPONENT BEFORE IT CAN BE CONSIDERED FOR RELEASE.

RECORDS MANAGEMENT NOTICE: ALL RECORDS PERTAINING TO U.S. SPECIAL OPERATIONS COMMAND THAT ARE CREATED BASED ON THIS PUBLICATION MUST BE MAINTAINED AND RETAINED IAW THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL (CJCSM) 5760.01, VOLUMES I AND II; DODD 5015.2, AND USSOCOM D 25-51, *RECORDS MANAGEMENT PROGRAM.*

APPENDIX A

RESPONSIBILITIES

A-1. The Chief of Staff, USSOCOM:

a. Serves as the USSOCOM SCOP.

b. Provides oversight of the Privacy Program, including ultimate authority for denial for PA requests.

c. IAW DODI 5400.11, the USSOCOM SCOP:

(1) Oversees and provides strategic direction for USSOCOM Privacy Programs.

(2) Provides advice and information to the DOD SAOP on privacy issues and concerns within USSOCOM.

(3) Ensures employee awareness of privacy and accompanying responsibilities to protect them.

(4) IAW DODI 8510.01, *Risk Management Framework (RMF) for DOD Information Technology*, 28 July 2017 as amended, and in conjunction with the DOD Component senior information security officers and the Risk Management Framework Technical Advisory Group:

(a) Reviews and approves the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII IAW Appendix F of Committee for National Security Systems Instruction No. 1253.

(b) Designates which privacy controls will be treated as program management, common, information system-specific, or hybrid privacy controls in the Component.

(c) Uses the Privacy Overlay found in Attachment 6 of Appendix F of Committee for National Security Systems Instruction No. 1253 to select privacy and security controls for information systems containing PII. This will ensure the implementation of information security and privacy control measures at every stage in the life cycle.

(d) Reviews and approves the System Privacy Plans portion of the System Security Plan for Component information systems containing PII before authorization, reauthorization, or ongoing authorization.

(e) Identifies assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and management of privacy risks**.**

RESPONSIBILITIES (Cont.)

(f) Identifies and maintains inventory of high-value assets (HVA), as defined in the Office of Management and Budget (OMB) Memorandum M-17-09.

(g) Coordinates with authorizing officials on granting authorization to operate decisions for information systems.

(h) Ensures that the DOD SAOP is aware of information systems and Component systems of records containing PII that cannot be appropriately protected or secured, and that such systems are given a high priority for upgrade, replacement, or retirement.

(5) Implements the DOD Breach Response Plan and, as necessary, establishes Component breach management policies. Ensures adequate training and awareness is provided to employees and contractors on how to report, respond to, and mitigate breaches of PII. For breaches involving protected health information, defer to the Defense Health Agency Privacy and Civil Liberties Office for direction under Public Law 104-191, also known as the *Health Insurance Portability and Accountability Act of 1996*, and DOD 6025.18-R, *DOD Health Information Policy Regulation, 24 January 2003*.

(6) Ensures adequate procedures are in place for the management and remediation of privacy complaints and alleged violations.

(7) Reviews and approves reports as required for submission to the DPCLTD.

(8) Establishes as necessary a Component-level program to provide employee awareness of privacy as well as supervisor and senior-leader understanding of responsibilities to protect privacy. The program must include and disseminate procedures for submitting and responding to complaints of violations.

A-2. The Deputy Chief of Staff, USSOCOM. Serves as the alternate SCOP.

A-3. The Chief, SOCS-SJS-VI, USSOCOM:

a. Serves as the USSOCOM Component Privacy Program Officer.

b. Maintains the USSOCOM Privacy Program and Privacy Office consistent with the PA of 1974 and IAW the DOD Privacy Program (DODI 5400.11). This includes, but is not limited to:

(1) Manages and supervises the functions of the DOD Privacy Programs for their respective organizations.

(2) Ensures appropriate administrative, physical, and technical safeguards and procedures are established for information systems that contain PII.

RESPONSIBILITIES (Cont.)

(3) Collaborates, as necessary and appropriate with information management, information collection, information security, forms and publications management, records management, chief information officer, and attorney and legal advisor staffs.

(4) Aggregates data and submits reports to the Chief, DPCLTD, through their respective SCOPs.

(5) To the extent authorized by the PA of 1974 and using procedures outlined in Part 310 of Title 32, Code of Federal Regulations and the respective SORN: Processes requests from individuals for access to records or to information pertaining to the individual from if USSOCOM maintains the system of records.

(6) Provides a copy of such records, in whole or in part, to the individual, unless such information should be withheld pursuant to applicable exemptions.

(7) Corrects or amends such records if it has been determined by USSOCOM that the records are not accurate, relevant, timely, or complete, unless an exemption applies.

(8) Processes appeals of denials of requests to access or amend a record.

(9) Submits SORNs and exemption rules to the DPCLTD.

(10) Implements formal breach management policies, and provides adequate training and awareness for employees and contractors on how to report and respond to breaches of PII.

(11) Provides mechanisms for submitting privacy complaints or alleged violations, IAW DODI 5400.11.

(12) Ensures employee awareness of methods to address allegations of privacy violations.

(13) Reviews and coordinates with appropriate Component personnel DD Form 2930 available at http://www.esd.whs.mil/Directives/forms/, for information systems IAW DODI 5400.16. This form must be used when developing, procuring, or using IT that collects maintains, or disseminates PII, or when collecting, maintaining or disseminating PII using IT, IAW Section 208 of Public Law 107-347, also known as the *E-Government Act of 2002*.

(14) Makes the privacy impact assessments available to the public IAW OMB policy and DODI 5400.16. IAW DODI 5400.16, if section 1 of DD Form 2930 contains information that would raise security concerns or reveal classified or sensitive information, USSOCOM can restrict the publication of the assessment.

(15) Submits SSN reduction and justification memoranda to DPCLTD for final approval after the SCOP has signed them in accordance with Enclosure 3 of DODI 1000.30, *Reduction of SSN Use Within DOD,* 1 August 2012.

RESPONSIBILITIES (Cont.)

(16) Coordinates with the Defense Health Agency Privacy and Civil Liberties Office for all matters related to protected health information covered by Public Law 104-191, also known as the *Health Insurance Portability and Accountability Act of 1996*.

(17) Ensures component insider threat program officials include privacy in their training programs IAW DODD 5205.16.

(18) Provides specialized PA training for personnel managing systems of records.

(19) Coordinates with Records Managers on disposition schedules.

(20) Prepares Exemption Rules with guidance from the Special Operations Staff Judge Advocate (SOJA).

(21) Reviews SORNS for Paperwork Reduction Act considerations.

(22) Conducts reviews of the Privacy Program at regular intervals.

(23) Reviews all publications and forms for compliance with this instruction.

(24) Reviews/resolves complaints or allegations of PA violations.

(25) Reviews contracts for systems of records operated or maintained by a contractor annually.

(26) Ensures any collections from the public are approved by OMB.

A-4. SOJA, USSOCOM:

a. Reviews and advises on the use of Exception and Exemption Rules.

b. Advises as needed to ensure SORNs are in compliance with statutes.

A-5. USSOCOM HQ Directorates, Components, Sub-Unified Commands:

a. Are responsible for ensuring compliance with the PA Program.

b. Appoints a Privacy Officer or Manager to oversee the privacy programs and activities IAW this directive, respective Military Service component policies, and other relevant policies.

c. Provides copy of the Privacy Officer/Manager Appointment Memo to the Privacy Officer.

d. Ensures Privacy Officers/Managers are reasonably available for Privacy training, coordinated by the Privacy Officer.

RESPONSIBILITIES (Cont.)

A-6. Systems of Records Manager:

a. Manages the system, to include preparation of SORNs, response to PA requests, investigation of complaints or allegations of a PA violation and maintenance of case files for all PA requests.

b. Implements procedures to safeguard systems of records (paper, electronic, and IT systems).

c. Provides justification for the use of SSNs to comply with DODI 1000.30.

d. Ensures personnel with access to a system of records are aware of their responsibilities under the PA.

e. Ensures systems of records under their purview are covered by a SORN.

f. Ensures system of records have approved disposition schedules.

g. Evaluates the systems annually to ensure compliance with this directive and DODI 5400.11, including any appropriate dispositions.

h. Records promises of confidentiality to exempt from disclosure any *confidential* information under Title 5 U.S.C., 552a, Subsection (k)(2), (k)(5), or (k)(7) of the PA.

i. Collects personal information directly from the subject of the record when possible. Third parties may be asked when information must be verified, opinions or evaluations are required, the person cannot be contacted, or the person requests the information be obtained from another person.

h. Provides a Privacy Act Statement (PAS) orally or in writing to anyone from whom personal information is collected for a system of records and/or an individual's SSN or DOD ID number is requested. *(**NOTE:** Do this regardless of how answers are recorded. A sign displayed in areas where people routinely furnish this kind of information is adequate. A copy of the PAS will be provided upon request; there is no requirement for personnel to sign a PAS.)* A PAS must include the following four items:

(1) **Authority:** The legal authority is the U.S.C., or E.O. authorizing the program the system supports.

(2) **Purpose:** The reason the information is collected.

(3) **Routine Uses:** A list of where and why the information will be disclosed outside DOD.

(4) **Disclosure: Voluntary or Mandatory.** Use Mandatory only when disclosure is required by law and the individual will be penalized for not providing information. Include any consequences of nondisclosure in nonthreatening language.

APPENDIX B

SAFEGUARDING INFORMATION

B-1. Privacy Act Warning Statement. USSOCOM will include a PA Warning Statement in each USSOCOM publication that requires collecting or keeping personal information in a system of records or directs the collection of SSN or DOD ID Number from individuals. The warning statement will cite legal authority and the system of records number and title. The following is an example warning statement: *This publication requires collecting and maintaining information protected by the PA of 1974 authorized by (U.S.C., citation and or E.O. number). System of Records Notice (number and title) applies.*

B-2. Sensitivity. Information will be protected according to its sensitivity level (e.g., non-sensitive PII can be posted on USSOCOM's internal portals). All other PII should be safeguarded through encryption (***NOTE:*** The portal pages are not capable of encrypting documents). Consider the personal sensitivity of the information and the risk of loss or alteration. Most information in systems of records is FOUO. DD Form 2923, **Privacy Act Data Cover Sheet**, is used for protecting PA material such as letters, file folders, listings, etc. PA Labels must also be attached to portable electronic devices that contain material covered by the PA.

B-3. Information Systems. Any system that contains information on individuals that are retrieved by name or personal identifier are subject to the PA. These systems are required to have a PA system of records notice published in the Federal Register that covers the information collection. In addition, all information systems subject to the PA will have warning banners displayed on the first screen (at a minimum) to assist in safeguarding the information. Use the following: *PRIVACY ACT INFORMATION – The information accessed through this system is FOR OFFICIAL USE ONLY and must be protected IAW the PA and this Directive.*

a. **New Systems.** When a new system becomes operational, the system manager will establish appropriate safeguards to ensure the records are secure, confidential, and protected against any anticipated threats or hazards to their security or integrity, which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. The system manager will be responsible for data retained in the system of records, ensuring information maintained is current, and security procedures are complied with. At a minimum, this requires password protection with a log-on protocol authorized by the respective system manager.

b. **Databases.** Databases should be evaluated for requirements under the Privacy Program. Such requirements include a SORN, PIA, SSN justification memorandum and Paperwork Reduction Act submission (OMB Form 83-1). Collection of information within these databases should be limited to mission essential information and should be collected directly from the individual if feasible.

c. **Balance.** Balance additional protection against risk and cost. For example, a password may be enough protection for an automated system with a log-on protocol. Classified computer systems or those with established audit and password systems are obviously less vulnerable than unprotected files or word processors in offices that are periodically empty.

SAFEGUARDING INFORMATION (Cont.)

B-4. E-mail Communication. When utilizing USSOCOM computer systems, all personnel are responsible for and directed to encrypt all transmitted e-mails containing PII. To do this, ensure CAC certificates are loaded into the Global Access List in order to facilitate encryption of e-mails. If e-mails cannot be encrypted the information will be sent via the DOD Secure Access File Exchange (DOD SAFE) or equivalent system. When sending personal information over e-mail within USSOCOM/DOD, ensure all recipients are authorized to receive it under the PA.

a. **Subject Line.** E-mails containing PII will have the subject line begin with the FOUO marking at a minimum, followed by the subject of the e-mail.

b. **E-mail Body.** For all e-mails that contain PII, the e-mail body will begin with the following Privacy Statement: This e-mail contains FOUO information which must be protected under FOIA (5 U.S.C., 552) and/or the PA of 1974 (5 U.S.C., 552a). Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in disciplinary action, criminal and/or civil penalties. Further distribution of this message is prohibited without the approval of the author of this message unless the recipient has a need to know in the performance of official duties. If you have received this message in error, please notify the sender and delete all copies of this message.

B-5. Portal Pages. Personal information of USSOCOM personnel shall not be posted on publicly accessible DOD websites unless clearly authorized by law and/or regulation and policy. Non-sensitive PII is permitted to be posted on the home pages of the directorate portal pages on the USSOCOM Intranet for day-to-day operations of USSOCOM. Non-sensitive PII includes: full name, rank, work phone, work e-mail, office code, and assigned position. This information remains unreleasable to the public.

B-6. Records. Records must be transferred in a manner that prevents unauthorized disclosure of information contained in a system of records.

a. For hard-copy records, sealed opaque envelopes will be used to transfer PA material by mail. Sealed opaque envelopes with a PA Label will be used to transfer PA material inter-base and inter-office.

b. Records shall not be given verbally from a system of records (by telephone or otherwise) to anyone unless the disclosure is authorized under the PA and the recipient's identity and need to know are fully verified.

c. All paper record material or electronic media (floppy disks, CD-ROM disks, computer tapes, etc.) will be stored in a lockable container (filing cabinet, desk, etc.), or in a secured room at all times when not in use during working hours, and at all times during nonworking hours. Do not leave PA records unattended and exposed at any time unless the entire work area is fully secured from unauthorized persons.

d. Annotate each page of a document containing PA material with the statement, *Personal Data – Privacy Act of 1974 Applies.* (This includes correspondence containing SSNs or DOD ID Numbers).

SAFEGUARDING INFORMATION (Cont.)

e. Mark all rosters/listings, which contain personal information (home address, home telephone number, DOD ID Number or SSN) *For Official Use Only (FOUO).*

f. Within USSOCOM, destroy PA material by shredding to render material unrecognizable or beyond reconstruction. The destroyed material maybe placed in trash containers. USSOCOM will not use recycling as a method of destroying PA material. It is the system manager's responsibility to ensure this process is accomplished.

APPENDIX C

PERSONALLY IDENTIFIABLE INFORMATION (PII)

C-1. General. A breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where:

a. A person other than an authorized user accesses or potentially accesses PII or

b. An authorized user accesses or potentially accesses PII for an other than authorized purpose.

c. Examples include: Stolen/lost laptops or mobile phones, unencrypted emails/attachments containing PII, unauthorized use of another user's account, unauthorized use of system privileges and data extraction, documents containing PII posted to public sites, inappropriate disposal of PII.

d. A major incident is either:

(1) Any incident likely to result in demonstrable harm to the national security interest, foreign relations, or the economy of the U.S., or to the public confidence, or public health and safety of the American people. or:

(2) A breach involving PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the U.S., or to the public confidence, or public health and safety of the American people. Any breach that involves 100,000 or more individuals' PII automatically constitutes a major incident.

C-2. Reporting Procedures. Breaches or potential breaches of PA data will be reported utilizing USSOCOM IMT 60, **Reporting a Potential Privacy Breach**. The IMT 60 can be found on the USSOCOM Non-secure Internet Protocol Router (NIPR) and Secure Internet Protocol Router (SIPR) portals. The USSOCOM Chief of Staff (the SCOP) is responsible for breach management.

a. All USSOCOM Service Component personnel will report actual or potential breaches of PII to their respective Privacy Officer/Manager as soon as possible but not later than (NLT) one hour after the discovery of the breach or potential breach. If there is no Privacy Officer, the breach should be reported directly to the USSOCOM Privacy Officer (SOCS-SJS-VI), who in turn will notify the USSOCOM SCOP within 24 hours of discovery. ***NOTE:*** Cybersecurity incidents require faster processing, and should be followed IAW DODI 5400.11.

b. The Privacy Officer within USSOCOM Components will report the potential breach through their respective Military Service components and notify the USSOCOM FOIA Office for situational awareness. All others, including the Sub-unified Commands, will report the potential or confirmed breach to the USSOCOM Privacy Officer within one hour after notification via the SIPR at ussocom.foia@socom.smil.mil or the NIPR at foia@socom.mil.

PERSONALLY IDENTIFIABLE INFORMATION (PII) (Cont.)

c. The USSOCOM Privacy Office, at the direction of the USSOCOM SCOP, will ensure that ***ANY*** actual or potential breaches (regardless of the number of people affected) within USSOCOM are reported to DPCLTD within 48 hours IAW DODI 5400.11.

C-3. Potential Breach Investigations. An Investigating Officer will be appointed by the respective command to investigate any potential or actual breach of PII. The investigation will be conducted with assistance from the Directorate of Communications Systems (J6), Knowledge Management (SOCS-KM), USSOCOM Privacy Officer/Manager (SOCS-SJS-VI) and Legal Office (SOJA) as deemed appropriate.

C-4. Notification of Personnel Affected by PII Loss. When PII is lost, stolen or compromised, notification shall be made as soon as possible, but NLT 10 working days after the loss, theft or compromise is discovered, and the identities of the affected individuals have been ascertained. All Enterprise-associated personnel must be knowledgeable of the procedures for reporting the loss of PII.

APPENDIX D

EXEMPTIONS

D-1. No system of records with the DOD shall be considered exempted until the Head of the Component has approved the exemption and an exemption rule has been published as a final rule in the Federal Register. Provisions of the PA from which a general or specific exemption may be claimed can be found in Appendix 4, DODI 5400.11.

D-2. There are three types of exemptions IAW DODI 5400.11:

a. **An access or Special Exemption: Section 552a(d)(5) of the PA:**

(1) Exempts records compiled in reasonable anticipation of a civil action or proceeding from the access provisions of the Act.

(2) Is self-executing and does not require an implementing regulation to be effective.

b. **General Exemptions: Section 552a(j) of the PA:**

(1) Authorizes the exemption of a system of records from all but certain specifically identified provisions of the Act.

(2) (j)(1) applies only to systems of records maintained by the Central Intelligence Agency.

(3) (j)(2) applies to systems of records maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws.

(4) DOD Blanket Routine Uses can be found on the DPCLTD website at: https://dpcld.defense.gov/Privacy/SORNs/Exemption-Rules/.

c. **Specific Exemptions: Section 552(k) of the PA:**

(1) Allows a system of records to be exempted only from certain designated provisions of the Act. The seven specific exemptions in 552(k) are narrower in scope and are intended to preserve the integrity of a process.

(2) Requires the exemption to be published as a final rule to the Federal Register for the system of record or subcomponent of a system of record to be considered exempt.

(3) There are currently no specific exemptions published for USSOCOM.

(4) (k)(1) Applies to classified information compiled under an E.O. in the interest of national defense or foreign policy.

EXEMPTIONS (Cont.)

(5) (k)(2) Applies to investigatory material compiled for law enforcement purposes other than material within the scope of (j)(2). This includes information compiled by an agency whose primary activity does not pertain to the enforcement of criminal law. ***NOTE*:** Coverage is less broad where the individual has been denied a right, benefit, or privilege as a result of information sought.

(6) (k)(3) Pertains to the provision of protective services to the President of the U.S., or to other individuals (foreign heads of state), pursuant to section 3056 or Title 18.

(7) (k)(4) Applies to systems required by statute to be maintained and used solely as statistical records.

(8) (k)(5) Pertains to investigatory material compiled solely for the purpose of determining suitability for Federal employment, military service, Federal contracts, or access to classified information. It applies to the extent that the disclosure would reveal the identity of a source who furnished information to the Government under and express promise of confidentiality.

(9) (k)(6) Applies to testing or examination materials used to determine appointment or promotion in the Federal service, when disclosure would compromise the objectivity or fairness of the process.

(10)(k)(7) Pertains to evaluation material used to identify potential for promotion in the Armed Services. It applies to the extent that the disclosure would reveal the identity of a source who furnished information to the Government under an express promise of confidentiality.

D-3. Any request for an exemption of a USSOCOM system of records will be routed through the USSOCOM SOCS-SJS-VI Branch. Exemption requests will be processed IAW DODI 5400.11.

APPENDIX E

LIST OF PII

THIS LIST IS NOT ALL-INCLUSIVE

- SSN
- DOD Identification Number.
- USSOCOM Badge Number.
- Home or Quarters address (to include home web address).
- Home telephone number.
- Age and Date of birth (year).
- Place of birth.
- Race/Ethnic Origin.
- Marital status (single, divorced, widowed, separated).
- Number, name, and sex of dependent children.
- Religion.
- Citizenship.
- Types of leave used; leave balances.
- Details of health and insurance benefits.
- Promotion recommendations.
- Supervisory assessments of professional conduct and ability.
- Information provided by relatives and references.
- Names of references.
- Prior employment unrelated to civilian employee's occupation.
- Character of military discharge.
- Financial and credit data (to include checking account, and personal identification numbers).
- Medical data (to include weight, height, blood pressure; medical conditions, prognosis, prescriptions, treatments, history of disease).
- Security clearance level.
- Mother's maiden name; other names used.
- Drug test results and the fact of participation in rehabilitation programs.
- Family data.
- Performance ratings.
- Performance elements and standards (work expectations) are PII when they are so intertwined with performance appraisals that their disclosure would reveal an individual's performance appraisal.
- Photographic identifier (picture, photo image, X-ray, and video).
- Biometric identifier (fingerprint, voiceprint, DNA).
- Driver's license number.
- Certificates (birth, death, marriage).

LIST OF PII

THIS LIST IS NOT ALL-INCLUSIVE (Cont.)

- Civilian Educational Degrees and major areas of study (unless the requested information relates to the professional qualifications for Federal Employment).
- Criminal history.
- Disciplinary actions.
- Office, unit address, and duty phone for overseas or for routinely deployable or sensitive units.

NOTE:

*SSN (does not have to be associated with an individual – in any form it is considered PII).

Files may contain information of a sensitive, personal nature that, if disclosed, would be a PA violation. ***EXAMPLES:* (not inclusive) are files containing information on investigations of individuals or complaints (such as Equal Employment Opportunity) lodged by individuals.

GLOSSARY

SECTION I--ABBREVIATIONS AND ACRONYMS

CAC	Common Access Card
CJCSM	Chairman of the Joint Chiefs of Staff Manual
DOD	Department of Defense
DODD	Department of Defense Directive
DODM	Department of Defense Manual
DPCLTD	Defense Privacy, Civil Liberties and Transparency Division
E.O.	Executive Order
FLO	Foreign Liaison Officers
FOIA	Freedom of Information Act
FOUO	For Official Use Only
GAO	General Accounting Office
HIPAA	Health Insurance Portability and Accountability Act
HVA	High Value Asset
IAW	in accordance with
J6	Directorate of Communications Systems
JSOU	Joint Special Operations University
NLT	not later than
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSD	Office of the Secretary of Defense
PA	Privacy Act
PAS	Privacy Act Statement
PHI	Protected Health Information
PIA	Privacy Impact Assessment
SCOP	Senior Component Official for Privacy
SOCS-KM	Special Operations Command Support Directorate, Knowledge Management
SOCS-SJS-VI	Command FOIA/Privacy Act/Civil Liberties Branch
SOJA	Staff Judge Advocate
SORN	System of Records Notice
SSN	Social Security Number
U.S.C	U. S. Code
USSOCOM	U.S. Special Operations Command

SECTION II--DEFINITIONS

Access. Allowing individuals to review or receive copies of their records.

Agency. For the purposes of disclosing records subject to the PA among DOD Components, the DOD is considered a single agency. For all other purposes to include applications for access and amendment, denial of access or amendment, appeals from denials, and recordkeeping as regards release to non-DOD agencies, each DOD Component is considered an agency within the meaning of the PA.

Amendment. The process of adding, deleting, or changing information in a system of records to make the data accurate, relevant, timely, or complete.

Breach. The actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purpose where one or more individuals will be adversely affected.

Computer Matching. A computerized comparison of two or more automated systems of records or a system of records with non-Federal records to establish or verify eligibility for payments under Federal benefit programs or to recover delinquent debts for these programs.

Confidential Source. A person or organization who has furnished information to the Federal Government under an express promise that the person's or the organization's identity will not be disclosed or under an implied promise of such confidentiality if this implied promise was made before 27 September 1975.

Confidentiality. An expressed and recorded promise to withhold the identity of a source or the information provided by a source. The Air Force promises confidentiality only when the information goes into a system with an approved exemption for protecting the identity of confidential sources.

Denial Authority. The individuals with authority to deny requests for access or amendment of records under the PA.

Disclosure. The transfer of any personal information from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, private entity, or Government agency, other than the subject of the record, the subject's designated agent, or the subject's legal guardian.

Federal Register. Contains a list of all system of records notices that is publically available. The OSD PA Coordinator, Records Management Section, is the DOD Proponent for publishing any notices to the Federal Register. All records systems containing information covered by the PA are required to be on file in the Federal Register.

SECTION II—DEFINITIONS (Cont.)

High Value Asset. Assets, Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the U.S.' national security interests, foreign relations, economy, or to the public confidence, civil liberties or public health and safety of the American people. HVAs may contain sensitive controls, instructions, data used in critical Federal operations, or unique collections of data (by size or content), or support an agency's mission essential functions, making them of specific value to criminal, politically motivated, or state-sponsored actors for either direct exploitation or to cause a loss of confidence in the U.S. Government.

Individual. A living citizen of the U.S. or an alien lawfully admitted to the U.S. for permanent residence. The legal guardian of an individual has the same rights as the individual and may act on his or her behalf. No rights are vested in the representative of a dead person under this instruction and the term "individual" does not embrace an individual acting in an interpersonal capacity (for example, sole proprietorship or partnership).

Individual Access. To make available information pertaining to the individual by the individual or his or her designated agent or legal guardian.

Maintain. Includes collecting, safeguarding, using, accessing, amending, and disseminating personal information.

Matching Agency. The agency that performs a computer match.

Member of the Public. Any individual or party acting in a private capacity to include Federal employees or military personnel.

Minor. Anyone under the age of majority according to local state law. If there is no applicable state law, a minor is anyone under age 18. Military members and married persons are not minors, no matter what their chronological age.

Official Use. Within the context of this instruction, this term is used when employees of a DOD component have a demonstrated need for the use of any records or the information contained therein in the performance of their authorized duties.

Personal Identifier. A name, number, or symbol which is unique to an individual, usually the person's name or SSN.

Personally Identifiable Information (PII). Per DODI 5400.11, DOD Privacy Program, PII is information about an individual that identifies, links, relates, or is unique to, or describes him or her (e.g., information which can be used to distinguish or trace an individual's identity). For example, a SSN, DOD ID number, date and place of birth, mother's maiden name, age, military rank, civilian grade, marital status, race, salary, home/office phone numbers, other demographic, biometric, personal, medical, financial information, etc.

SECTION II—DEFINITIONS (Cont.)

Personal Information. Knowledge about an individual that is intimate or private to the individual, as distinguished from that related solely to the individual's official functions or public life.

Privacy Act Request. A request from an individual for notification as to the existence of, access to, or amendment of records pertaining to that individual. These records must be maintained in a system of records.

Privacy Act Statement (PAS). A statement furnished to an individual when the individual is requested to provide personal information, regardless of the medium used to collect the information, to go into a system of records. A PAS is also furnished to an individual when asking them for their SSN.

Privacy Impact Assessment (PIA). A written assessment of an information system that addresses the information to be collected, the purpose and intended use; with whom the information will be shared; notice or opportunities for consent to individuals; how the information will be secured; and whether a new system of records is being created under the PA.

Record. Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history, and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

Routine Use. The disclosure of a record outside the DOD for a use that is compatible with the purpose for which the information was collected and maintained by the DOD. The routine use must be included in the published system notice for the system of records involved. For example: *To the Veterans Administration to verify the physical disability of applicants for the purpose of authorizing monthly retirement disability payments*.

Source Agency. A federal, state, or local government agency that discloses records for the purpose of a computer match.

System Manager. The individual who initiates a system of records, operates such system, or is responsible for a segment of a decentralized part of that system and issues policies and procedures for operating and safeguarding of information in the system.

System of Records. A group of records under the control of a DOD component from which PII is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned, that is unique to the individual.

System of Records Notice. The official public notice published in the Federal Register upon the establishment and/or modification of a system of records describing the existence and character of the system. Systems of records are effective upon publication of the notice in the Federal Register. However, routine uses must be published 30 days to allow for public comment before they may be utilized.

SECTION III—REFERENCES

CJCSM 5760.01, *Joint Staff and Combatant Command Records Management Manual*, Volume I, Procedures and Volume II, *Disposition Schedule,* 13 July 2012.

DODD 5400.7, *DOD Freedom of Information Act Program*, 5 April 2019.

DOD 6025.18-R, *DOD Health Information Policy Regulation*, 24 January 2003.

DOD Instruction (DODI) 1000.30, *Reduction of Social Security Number (SSN) Use Within DOD*, 1 August 2012.
DODI 5015.02, *DOD Records Management Program,* 24 February 2015, as amended.

DODI 5230.24, *Distribution Statements on Technical Documents,* 23 August 2012, as amended.

DODI 5400.11, *DOD Privacy and Civil Liberties Programs*, 29 January 2019.

DODI 5400.16, *DOD Privacy Impact Assessment (PIA) Guidance,* change 1, 11 August 2017.

DODI 8500.01, *Cybersecurity,* 14 March 2014.

DODI 8510.01, *Risk Management Framework (RMF) for DOD Information Technology*, 28 July 2017 as amended.

DODM 5200.01, Volume 4, *DOD Information Security Program: Controlled Unclassified Information (CUI),* 24 February 2012 with Change 1, effective 9 May 2018.

DODM 5200.02, *Procedures for the DOD Personnel Security Program (PSP*), 3 April 2017.

DODM 5400.07, *DOD Freedom Of Information Act (FOIA) Program,* 25 January 2017.

DOD Memorandum, Subject: *DOD Guidance on Protecting Personally Identifiable Information (PII),* 18 August 2006.

National Institute of Standards and Technology, Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System,* August 2003.

Office of Management and Budget Memorandum M-17-09, *Management of Federal High Value Assets*, 9 December 2016.

SECTION III—REFERENCES (Cont.)

OSD Memorandum, Subject: *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* 5 June 2009.

OSD Memorandum, Subject: *Designation of USSOCOM as a Sensitive Unit,* 21 September 2001.
Public Law 100-503, *The Computer Matching and Privacy Act of 1988.*

Title 5, U.S.C., Section 552, *The Freedom of Information Act.*

Title 5, U.S.C., Section 552a, as amended, *The Privacy Act of 1974.*

Title 10, U.S.C., Section 164, *Armed Forces, Organization and General Military Powers, Combatant Commands.*

USSOCOM Manual 530-1, *Operations Security,* 5 December 2014.

32 Code of Federal Regulations 286, *DOD Freedom of Information Act*, Effective 5 January 2017