UNITED STATES SPACE COMMAND INSTRUCTION (SPI)

OPR: J006

SPI 2803.01A
17 June 2021

PRIVACY ACT AND CIVIL LIBERTIES PROGRAMS

Reference(s): Enclosure C

1. Purpose. The purpose of this Space Instruction (SPI) is to implement the Privacy Act (PA) and Civil Liberties (CL) programs within the United States Space Command (USSPACECOM) per Department of Defense Instruction (DoDI) 5400.11, DoD Privacy and Civil Liberties Programs; and Department of Defense (DoD) 5400.11-R, Department of Defense Privacy Program; and to supplement instructions in Air Force Instruction (AFI) 33-332, The Air Force Privacy and Civil Liberties Program. The United States Air Force is USSPACECOM's executive agency for privacy; however, the Defense Privacy, Civil Liberties and Transparency Division (DPCLTD) is the Combatant Command's advocate for PA and CL matters as directed by the DoD PA and CL programs.

2. Superseded/Cancellation. This is the initial publication of this format.

3. Applicability. This SPI applies to USSPACECOM and its Command Components.

4. Procedures. See Enclosures A through C.

5. Summary of Changes. According to DoD Senior Agency Official for Privacy (SAOP) memorandum, Designation of Senior Component Officials for Privacy and Establishment of Roles and Responsibilities, dated 28 August 2017, the Commander, USSPACECOM designates the Senior Component Official for Privacy (SCOP) position and responsibilities to the positions of the USSPACECOM Chief of Staff and the Deputy Chief of Staff. By this designation, SCOP related duties are added to the USPACECOM Privacy Civil Liberties Officer (PCLO) responsibilities when the primary and alternate SCOPs are unavailable. Creation of Command forms collecting personally identifiable information (PII) guidance is included. Privacy Impact Assessments (PIA) responsibilities are further defined.

6. Releasability. This directive is approved for public release; distribution is unlimited on NIPRNET. This SPI is approved for release to USSPACECOM, all of its Components, and additional outside agencies. Department of Defense (DoD) Components (to include the Combatant Commands), other Federal agencies, and the public, may obtain copies of this directive through the Internet via the USSPACECOM SharePoint Publications Electronic Library.

7. Effective Date. This instruction is effective upon receipt.

LEONARD.BROOK.J.1026246748 Digitally signed by LEONARD.BROOK.J.1026246748 Date: 2021.06.17 14:36:18 -06'00'

BROOK J. LEONARD
Major General, USAF
Chief of Staff

Enclosures
A — Privacy Act: Policy, Processes, and Responsibilities
B — Civil Liberties: Policy, Processes, and Responsibilities
C — References
GL — Glossary of Terms and Abbreviations

ENCLOSURE A

PRIVACY ACT: POLICY, PROCESSES, AND RESPONSIBILITIES

1. Policy.

a. USSPACECOM personnel will protect personal privacy as required by the Privacy Act of 1974 (section 552(a) of Title 5, U.S.C.), as amended. There are both criminal and civil penalties, as well as potential Uniform Code of Military Justice (UCMJ) sanctions, for violations of the PA. The PA and this SPI apply only to information in records on living U.S. citizens and aliens admitted as permanent residents of the U.S. that are maintained in an approved System of Record (SOR).

b. The U.S. Government (USG) is authorized to collect, maintain, use, and disseminate PII about individuals for the purpose of discharging its statutory responsibilities. However, all DoD personnel and USG contractors have an affirmative obligation to take reasonable steps to protect PII in order to reduce the risk of harm to individuals, whether that harm is embarrassment, harassment, or much worse—identity theft or physical injury.

c. PII is information about an individual that identifies, links, relates to, is unique to, or describes him or her. For ease of understanding, PII can be broken down into the following two categories: High risk of harm and low/no risk of harm.

(1) High Risk of Harm: Social Security Number (SSN); date of birth (DOB); mother's maiden name; home of record; age; marital status; number, name, and sex of dependents/children; civilian education level, school, and year of graduation; race/ethnic origin; personal telephone numbers; personal electronic mail (e-mail) addresses; home mailing address; financial, medical, and biometric information.

(2) Low/No Risk of Harm: Name; rank or civilian grade; Electronic Data Interchange Personal Identifier (EDIPI), also known as the DoD ID number; date of rank; service entry date; federal pay; pay date; position title; unit address; duty phone number; duty status of active, retired, or reserve; date of retirement/separation.

d. To comply with the requirements of the PA, and protect PII from unauthorized disclosure, USSPACECOM personnel will:

(1) Collect, maintain, and use such information only to support programs authorized by law or an Executive Order (E.O.).

(2) Ensure records in approved SOR are timely, accurate, complete, and relevant. Amend, on request, any record not meeting these requirements, and provide a review of decisions that deny individuals access to, or amendment of, their records.

(3) Safeguard records in SOR, and keep records the minimum time required to protect the rights and provide for the needs of the individual and the USG.

(4) Protect records from unauthorized use, disclosure, alterations, access, or destruction. Tailor the level of protection to the sensitivity of the information. Specifically:

(a) Do not use records for other than their intended, published purposes; e.g., do not create a listing to send happy birthday messages; do not use membership lists to determine non-members; do not use contributor lists to determine non-contributors, etc.

(b) Do not discuss derogatory or sensitive PII in a group setting (staff meetings, conferences, etc.) or in open work areas (to include cubicles) unless everyone in attendance has a need-to-know and is aware the information requires further PA mandated protection.

(c) Do not disclose third-party PII to anyone outside the DoD unless specifically authorized by law or E.O. Always apply discretion when disclosing your own PII to anyone outside the DoD.

(d) Do not use or move PII beyond USSPACECOM or its Component's premises or control (e.g., Temporary Duty (TDY), telework, etc.), without specific written authorization from a Division Chief or higher authority. Encrypt all e-mails containing PII. Under no circumstances will PII be sent unencrypted via e-mail to a commercial/private e-mail account.

(e) Mark all documents containing PII as CONTROLLED UNCLASSIFIED INFORMATION (CUI) in accordance with DoDI 5200.48, *Controlled Unclassified Information*.

(f) Do not use an individual's SSN or other PII unnecessarily. The SSN will not be collected if another means of identification is permissible/available. If a SOR requires the collection of an individual's PII, ensure anyone granted access to the SOR has a definite need-to-know. Otherwise, if more than a name is needed to positively identify an individual, the EDIPI should first be used to verify identity. In the event the SOR requiring access requires the use of the SSN, use only the number of digits required by the SOR. Development of a new SOR requiring collection of the SSN must comply with the requirements mandated by DoDI 1000.30, *Reduction of Social Security Number (SSN) Use Within DoD*. The PCLO must be contacted prior to development of a new SOR, regardless of the type of PII anticipated to be collected.

(g) Group Orders. Sanitize orders to ensure the SSN, EDIPI, and other PII (home address, home/cell phone, etc.) are not released to a third-party (e.g., fellow travelers) if the other travelers do not have an official need-to-know.

(h) Databases, Rosters, or Lists. Limit distribution or access to databases, rosters, or lists containing names of individuals, SSNs, EDIPI, or other PII to those with a need-to-know in the performance of their official duties. Sanitize lists to ensure the SSN, EDIPI, and/or other PII is not released to, or accessible by, a third-party (e.g., other personnel on the lists) without an official need-to-know, and ensure no further distribution is made without the express approval of the Office of Primary Responsibility (OPR). This is very important in the case of Recall Rosters and Communication-Out Rosters. Only the minimum identifying information necessary should be contained on these rosters (no SSNs, EDIPI, dates of birth, spouse names, identification of children, or physical addresses in the case of Recall Rosters). Only personnel in leadership positions should have access to Communication-Out Rosters, or any like roster containing physical addresses of personnel.

(i) Command Forms. Command forms containing PII must be reviewed by the PCLO prior to being used in order to determine whether or not a Privacy Act Statement (PAS) or a Privacy Act Advisory (PAA) is required to be inserted on the form. As a general rule, any Command form containing a named individual and an additional identifier, such as: rank, office phone number; SSN; date of birth; etc., requires a PAS or PAA to be included on the form, preferably on the first page, at the top or bottom. The PCLO will provide guidance for developing the PAS or PAA and will determine which type will be applied. A PAA is primarily used when the requested PII will be destroyed/deleted once positive identification is made or uploaded to a database.

(j) Do not process or store PII on mobile computing devices or removable electronic media.

(k) Do not send PII to distribution lists or group e-mail addresses unless each recipient has an official need-to-know. When in doubt, send only to individual accounts. Before forwarding e-mails containing PII, verify the intended recipients are authorized to receive the information under the PA. Remember, if an individual or an organization e-mail box cannot receive an encrypted e-mail, do not hit send.

(l) Report unauthorized disclosure (breach) of PII immediately/upon discovery to the PCLO.

2. Processes.

a. USSPACECOM systems managers will advise individuals on procedures to review or obtain copies of their own records in a SOR unless there is an approved exemption identified in the System of Record Notice (SORN), or the records were created in anticipation of civil action or proceedings.

b. Amending Records: Anyone may request minor corrections to their records orally. However, written requests are required for more serious modifications, or if any oral request is denied.

c. Approving or Denying a Record Amendment: USSPACECOM does not usually amend a record when the change is based on opinion, interpretation, or subjective official judgment. This action constitutes a denial, and requesters may appeal. If the system manager decides not to amend or partially amend the record, send a copy of the request, the record, and the recommended denial reasons to the IDA through the PCLO.

d. Reporting Alleged PA Violations and Complaints: Initially, refer alleged PA violations/complaints to the SOR manager or PCLO. However, individuals may register alleged PA violations/complaints with any existing reporting/complaint systems such as the IG's complaint system. If the violation/complaint is registered with any agency other than those in the PA system, that agency must coordinate action with the PCLO to ensure any required breach reporting is accomplished.

e. Processing PA Violations and Complaints: Process allegations of PA violations or complaints through the responsible SOR manager. The PCLO provides guidance to the SOR manager, providing he/she is not an involved party to the violation or the subject of the complaint. If the local SOR manager is not involved in the violation or complaint, he/she will: investigate complaints, or allegations of PA violations; establish and review the facts when possible; obtain legal guidance through USSPACECOM/J006; interview individuals as needed; determine validity of the complaint or violation; take appropriate corrective action(s); and ensure a response is sent to the complainant through the PCLO, within 10 days, unless an extension is granted by the appointing authority. However, some complaints or violations may be best investigated using Service-specific processes: e.g.; U.S. Air Force *Commander Directed Investigation (CDI) Guide*; Army Regulation (AR) 15-6, *Investigation Guide for Informal Investigations*; or *Manual of the Judge Advocate General of the Navy* (JAGMAN). Process and send component unique privacy complaints, which cannot be resolved within USSPACECOM, through the PCLO to the respective component PA officer.

f. PA Protective Markings and Caveats: There are no mandatory PA markings other than “CUI.” However, the following or similar caveats may be used in e-mails and/or in written correspondence:

(1) CUI – Contains information protected by the Privacy Act. Do not release without written authorization from the individual (Privacy Act of 1974, as Amended applies).

(2) CUI – Contains information protected by the Privacy Act. Do not reproduce or distribute further without written authorization from the Office of Primary Responsibility.

(3) CUI – Do not use PII from this document for any reason other than its intended, published purposes.

g. Establishing and Maintaining a Privacy Act SOR.

(1) USSPACECOM may keep paper and electronic records containing PII, retrieved by name or personal identifier, only in an approved SOR published in the *Federal Register*.

(2) The three most common methods of storing (maintaining) information in a SOR are:

(a) "automated" with material maintained on magnetic tapes or disks;

(b) "manual" with material maintained in paper files, microfilm, etc.; and

(c) "hybrid" with material maintained in combination of hard copy and automated form.

(3) Once established, the method of storage may not be changed until a notice of alteration is published in the *Federal Register*.

(4) In the absence of an existing SOR, a new system must be proposed. The organization desiring to establish a new SOR, or making major modifications to an existing SOR, must appoint a system manager. The proposed SOR must be reported to Congress and the Office of Management and Budget (OMB), through DPCLTD. The SOR must be approved and published in the *Federal Register*, and the public must be given an opportunity to comment before the SOR may be used. Normally, it takes a minimum of 180 days after the proposal leaves USSPACECOM before the SOR can be implemented.

(5) For new or major modifications to an existing SOR, the system manager must contact the PCLO for guidance.

h. As necessary, process unique or specific PA matters through the individual's military component only when that component's policy conflicts with AFI 33-332 or this instruction.

i. Privacy Act Routine Uses Required For PII Breach Response.

(1) To facilitate DoD's response to a breach of its own records, USSPACECOM and its Components will include a routine use into each SORN, as shown in Figure 1, below:

Figure 1. Routine Use for Breach of DoD Records

"To appropriate agencies, entities, and persons when (1) DoD suspects or has confirmed that there has been a breach of the system of records; (2) DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, 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 DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm."

(2) To ensure that DoD is able to disclose records in its system of records that may reasonably be needed by another agency in responding to a breach, USSPACECOM and its Components will incorporate a routine use into each SORN, as shown in Figure 2, below:

Figure 2. Routine Use for Assisting Another Federal Agency with Breach Responses

"To another federal agency or federal entity, when 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."

3. Responsibilities.

a. Initial Denial Authority (IDA). The Commander, USSPACECOM and Deputy Commander, USSPACECOM are authorized to deny individuals access to their official personal records or to amend official personal records in possession of USSPACECOM activities. Except for Inspector General (IG) records, IDA is delegated to the USSPACECOM Chief of Staff (J0CS). No other personnel are authorized to deny individuals access to their official personal records or to amend official records in possession of USSPACECOM organizations or activities.

b. Senior Component Official for Privacy (SCOP): Commander, USSPACECOM has designated the position of the USSPACECOM Chief of Staff and Deputy Chief of Staff as the Command's SCOP. The major SCOP responsibilities are:

(1) Oversee and provide strategic direction for the Command's PA program.

(2) Provide advice and information to the DoD SOAP on PA issues and concerns within USSPACECOM, and when applicable, external USSPACECOM components.

(3) Review all information technology investment funding agreements involving PII, including data hosting agreements, to ensure all necessary privacy risk management efforts are accounted for in accordance with DoDI 5400.11.

(4) In conjunction with USSPACECOM/J6, and the DoD Chief Information Officer's (CIO) Technical Advisory Group:

(a) Review and approve, according to the *National Institute of Standards and Technology* (NIST) *Federal Information Processing Standards* (FIPS) Publication 199, and NIST Special Publication 800-60, the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.

(b) Designate which PA controls will be treated as program management, common, information system-specific, or hybrid PA controls within the Command.

(c) Develop and deploy a process to select and implement PA controls for information systems and programs that satisfies applicable PA requirements as stated in OMB guidance.

(d) Review and approve the PA plans portion of the System Security Plan for Command information systems before authorization, reauthorization, or ongoing authorization.

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

(6) Identify and maintain inventory of high value assets as defined in OMB Memorandum M-17-09, *Management of Federal High Value Assets*.

(7) Coordinate with authorizing officials on granting Authority to Operate decisions for Command information systems.

(8) Ensure the DoD SAOP is made aware of information systems and components that cannot be appropriately protected or secured, and that the Command ensures such systems are given a high priority for upgrade, replacement, or retirement.

(9) Implement the DoD Breach Preparedness and Response Plan and, as necessary, establish Command breach management policies, and ensure adequate training and awareness is provided to employees and contractors on how to report and respond to breaches of PII. For further guidance, see Department of Defense Manual (DoDM) 5400.11, Vol 2, *DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan*, 6 May 2021; Memorandum, Deputy Secretary of Defense, SUBJECT: *Reporting Breaches of Personally Identifiable Information in Accordance with the Department of Defense Breach Response Plan*, 30 November 2018; and OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information,* 3 January 2017.

(a) Ensure the Chief, DPCLTD, and the Commander, USCYBERCOM, are informed of all breaches within 48 hours of being notified that a breach has occurred to ensure a seamless flow of information throughout the DoD.

(b) Determine, in consultation with the PCLO, if a major incident breach involving PII has occurred.

(c) Ensure a written assessment is completed concerning whether a major incident involving PII has occurred.

(i) An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII constitutes a major incident as defined in OMB Memorandum M-21-02, *Fiscal Year 2020-21 Guidance on Federal Information Security and Privacy Management Requirements*.

(ii) Unauthorized exfiltration is the act or process of obtaining, without authorization or in excess of authorized access, information from an information system without modifying or deleting it.

(d) Conduct and document an assessment of the risk of harm to individuals potentially affected by a breach.

(e) Determine how to best mitigate the harm to individuals affected by the breach.

(f) Determine whether to notify individuals potentially affected by the breach. The SCOP will consider the source, timeliness, content, method, and any special considerations necessary when notifying individuals. Affected individuals will not typically be notified if a low to no risk of harm has been determined.

(g) Determine appropriate actions in response to a breach, to include countermeasures, additional staff resources when appropriate, and guidance or services to individual(s) potentially affected; and

(h) Ensure law enforcement, J005, and J006 receive timely notification as appropriate.

(10) Review and approve required reports for submission to the DPCLTD.

(11) Establish the Command's program to provide employee awareness of PA issues as well as supervisor and senior leader understanding of responsibilities to protect privacy; ensuring the program includes procedures for submitting and responding to complaints or violations.

c. The PCLO manages the PA program and:

(1) Trains PA system managers.

(2) Reviews the program at regular intervals.

(3) Submits required reports.

(4) Reviews publications and forms for compliance with applicable regulatory guidance.

(5) Assists system managers regarding complaint investigations.

(6) Performs breach reporting and identifies responsible SOR owner for conducting breach inquiry.

(a) Per the DoD Breach Preparedness and Response Plan, the PCLO will report the details of suspected and/or actual breach incidents to the SCOP within 24 hours of breach discovery and report suspected and/or confirmed computer breach incidents to US-CERT within 1 hour, if the breach involves a confirmed cybersecurity incident.

(b) Upon being notified of a PII breach, the PCLO will:

(i) Provide the SCOP with the SORNs, PIA, and privacy notices applicable to the potentially compromised information;

(ii) Document all breaches and actions taken in response to a breach using the DD Form 2959, and submit it to DPCLTD via the Compliance and Reporting Tool (CART);

(iii) Notify DPCLTD within 48 hours of discovery of a breach incident;

(iv) Update initial reports in CART as information becomes available and/or as pertinent decisions are made. This includes documenting whether affected individuals are being notified and, if so, the form of notification and the number of affected individuals notified; and

(v) Close breach reports in CART when all actions are complete.

(7) Reviews and forwards denial recommendations to the component OPR, when applicable.

(8) Assists/advises Command Chief Information Officer (CIO) and SCOP in reviewing PIAs.

(9) Creates basic and advanced PA training for all Command personnel, to include USG contractors.

(10) Acts on behalf of the SCOP when both Chief of Staff and Deputy Chief of Staff are unavailable.

(11) Assists the SCOP with all matters related to SCOP duties.

(12) Notifies DPCLTD when SCOPs rotate in and out of the Command.

d. Directors, Chiefs of Command Support Staff Offices within USSPACECOM, and Commanders of Subordinate USSPACECOM Organizations, within their area of jurisdiction, implement instructions in DoDI 5400.11, DoD 5400.11-R, AFI 33-332 and this SPI and also act as the authorizing official for requests from units within their jurisdiction to remove PII from DoD facilities when an official need has been determined.

e. System Managers. A system manager is the person responsible for management of the SOR(s) they create or control. Local system managers have authority to release records, to an appropriate requestor, within an SOR under their jurisdiction. They also have authority to amend records, as requested, to make them accurate, timely, relevant, or complete. The system manager will:

(1) Decide the need for, and content of systems.

(2) Manage and safeguard the SOR. Protect PII in the SOR from unauthorized alterations, use, or removal, and take immediate corrective action upon discovery.

(3) Immediately report violations/breaches to the PCLO.

(4) Ensure personnel do not load or transfer PII protected by the PA onto personal computers or computer systems, removable magnetic media etc., not under control of the DoD.

(5) Ensure personnel obtain approval to move PII protected by the PA beyond DoD premises or control (e.g., TDY, telework, etc.) from a Division Chief or higher authority. Retain documentation per SOR requirements and CJCSM 5760.01A, Volumes I and II.

(6) Train personnel on the PA requirements of their specific SOR.

(7) Coordinate the preparation of SORN, PAS, PIA, and any required PA related reports with the PCLO.

(8) Coordinate the answering of PA requests with the PCLO.

(9) Ensure PIAs are initiated when required, and are coordinated through the Command CIO, SCOP, and PCLO.

(10) Keep records of disclosure.

(11) Evaluate SOR annually. Prepare and submit required changes or SOR termination notices to the Command CIO, SCOP, and PCLO.

(12) Ensure SORs are accounted for in the *DoD Information Technology Portfolio Repository* (DITPR).

ENCLOSURE B

CIVIL LIBERTIES: POLICY, PROCESSES, AND RESPONSIBILITIES

1. Policy. Civil Liberties (CL) encompass the fundamental freedoms of a citizen to exercise customary rights protected by the *United States Constitution*.

a. DoDI 5400.11 establishes policy and provides responsibilities, administrative policies, and procedures for the implementation of USSPACECOM's CL Program.

b. All USSPACECOM Directorates/staff offices, Components, and associated units under the support or control of USSPACECOM are required to protect the CL of military and civilian personnel to the greatest extent possible consistent with its operational requirements.

c. No information will be gathered or maintained on how an individual exercises rights protected by the *First Amendment* to the *United States Constitution*, including the freedoms of speech, right to assemble, and religion, except when:

(1) Specifically authorized by Federal Statute;

(2) Expressly authorized by the individual, group of individuals, or association on whom the record is maintained; or

(3) The record is pertinent to and within the scope of an authorized law enforcement, intelligence collection, or counter intelligence activity.

d. USSPACECOM will have adequate procedures to receive, investigate, respond to, and redress complaints from individuals who allege USSPACECOM or one of its Components has violated their CL.

e. No USSPACECOM service member, employee, or contractor shall take any action constituting a reprisal, or threat of reprisal, in response to a CL complaint or a disclosure of information to the PCLO. However, disciplinary action may be taken if the CL complaint or disclosure:

(1) Was made with the knowledge that the complaint or disclosure was false; or

(2) Was made with a willful disregard for its truth or falsity.

2. Process for Handling CL Complaints.

a. USSPACECOM/IG and Staff Judge Advocate (SJA), including the Peterson-Schriever Garrison EO, will refer and report complaints that may be CL related to the PCLO for review/resolution. The PCLO will determine whether a complaint is valid and, if so, refer it to the appropriate office for investigation.

b. Written complaints will be addressed to: USSPACECOM/J006, ATTN: Privacy Civil Liberties Officer, 1670 North Newport Road, Colorado Springs, CO, 80916 or by e-mail at usspacecom.j006.privacy.cl.foia@usspacecom.mil.

c. Upon receiving a CL complaint, the PCLO will log the complaint into the CL Office database and acknowledge it in writing to the complainant within 5 working days of receipt.

d. The PCLO will review the complaint to determine its validity. A valid CL complaint will provide sufficient detail to adequately describe an infringement of a fundamental right or freedom protected by the United States Constitution. At minimum, a complaint must contain the following information:

(1) What CL was violated;

(2) A brief description, with reasonable specificity, explaining how the violation occurred, including:

(a) When and where the violation occurred;

(b) Whether the violation is ongoing;

(c) Who or what caused the violation, identifying the person, program, policy, or procedure responsible for the violation;

(d) Whether the violation was reported to any other authorities; and,

(e) What, if any, steps have been taken to resolve the violation.

e. If the PCLO determines the complaint to be valid, he or she will:

(1) Coordinate with the SCOP, IG, SJA, and the Peterson-Schriever EO Office to determine the appropriate investigating office and procedures.

(2) Make an initial resolution determination within 20 working days of receiving a CL complaint. If a resolution cannot be determined within 20 working days, the PCLO will send interim updates to the complainant and the SCOP as warranted by the investigation.

(3) Because complaints of this type can often be resolved through full, fair, and respectful communication, the PCLO will make reasonable efforts to mediate and resolve the complaint in a manner agreeable to the complainant and all relevant parties. The PCLO will document the efforts made to resolve the complaint.

(4) Valid CL complaints that cannot be mediated will be resolved through objective investigation, to include consideration of findings and recommendations provided by an impartial investigating official. The authority who appointed the investigating official will take appropriate action to resolve or adjudicate the CL complaint based on the results of the investigation, consultation with a legal advisor, and the appointing authority's best judgment.

f. If the PCLO determines that a CL complaint is invalid (i.e., fails to adequately describe or articulate a CL violation), he or she will notify the complainant and the SCOP in writing, briefly explaining why the complaint was found invalid. The complainant may challenge the PCLO's determination within 5 working days of receiving it by submitting a written appeal to the SCOP.

(1) Upon receipt of a timely written appeal, the SCOP will review and consider the original complaint, the rationale set forth in the PCLO's validity determination, and the complainant's appeal. The SCOP may also consider any other information he or she deems relevant and appropriate to making a fair decision on the appeal.

(2) If the SCOP determines that the appeal is without merit, he or she will deny it: notifying the complainant and the PCLO in writing that the appeal has been denied.

(3) If the SCOP determines that the appeal has merit, he or she will grant relief. The relief granted will be to return the appeal and complaint to the PCLO, with instructions to have the complaint investigated. Within 3 working days of receiving notice of the SCOP's decision to grant appellate relief, the PCLO will notify the complaint that his appeal was granted and that the complaint will be investigated.

3. Responsibilities.

a. Senior Component Official for Privacy (SCOP): Commander, USSPACECOM has designated the position of the USSPACECOM Chief of Staff and Deputy Chief of Staff as the Command's SCOP. The SCOP is responsible for overseeing and providing strategic direction for the Command's CL program. In that role, the SCOP will:

(1) Establish the Command's program to provide employee awareness of CL issues as well as supervisor and senior leader understanding of responsibilities to protect CL; ensuring the program includes procedures for submitting and responding to complaints or violations.

(2) Ensure all USSPACECOM personnel are trained regarding the protection of CL.

(3) Consider CL when proposing, developing, or implementing laws, regulations, policies, procedures, or guidelines related to USSPACECOM's mission.

(4) Ensure employee awareness of CL as well as supervisor and senior leader understanding of the responsibility to protect CL within the scope of their authority.

(5) Ensure adequate procedures are in place for management and remediation of CL complaints.

(6) Periodically review USSPACECOM actions, procedures, guidelines, and related laws to their implementation to ensure USSPACECOM is considering appropriate CL.

b. The PCLO manages the CL program and ensures the following:

(1) CL Program information will be made available on the J006 webpage.

(2) Establish procedures for the investigation of complaints from individuals who allege USSPACECOM or one of its Components violated their CL.

(3) Coordinate CL activities with USSPACECOM/IG office and the Peterson-Schriever Equal Opportunity (EO) office to avoid duplication of effort.

(4) Submit reports as directed by the DPCLTD: Semiannually from first half: 1 October to 31 March; second half: 1 April to 30 September.

ENCLOSURE C

REFERENCES

a. AFI 33-332, *Air Force Privacy and Civil Liberties Program*, 10 March 2020

b. AR 15-6, *Investigation Guide for Informal Investigations*, 1 April 2016

c. CJCSM 5760.01A, *Joint Staff and Combatant Command Records Management Manual: Volume I--Procedures,* 7 February 2008, incorporating Change 2, 13 July 2009

d. CJSCM 5760.01A, Vol II, *Joint Staff and Combatant Command Records Management Manual: Volume II - Disposition Schedule*, 13 July 2012

e. *Commander Directed Investigation (CDI) Guide,* 18 Feb 2016.

f. DoD 5400.11-R, *Department of Defense Privacy Program*, 14 May 2007

g. DoDI 1000.30, *Reduction of Social Security Number (SSN) Use Within DoD*, 1 August 2012. Incorporating Change I, 15 April 2020

h. DoDI 5200.48, *Controlled Unclassified Information,* 6 March 2020

i. DoDI 5400.11, *DoD Privacy and Civil Liberties Programs*, 29 January 2019, incorporating Change I, 8 December 2020

j. DoDM 5400.11, Vol 2, *DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan*, 6 May 2021

k. Federal Information Processing Standards Publication (FIPS) PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004

l. JAGINST 5800.7G, *Manual of the Judge Advocate General of the Navy (JAGMAN)*, 15 January 2021

m. Memorandum, Deputy Secretary of Defense, SUBJECT: *Reporting Breaches of personally identifiable information in Accordance with the Department of Defense Breach Response Plan*, 30 November 2018

n. Memorandum, DoD Senior Agency Official for Privacy, SUBJECT: *Designation of Senior Component Officials for Privacy and Establishment of Roles and Responsibilities*, 28 August 2017

o. National Institute of Standards and Technology (NIST) Special Publication 800-60, *Volume I: Guide for Mapping Types of Information and Information Systems*, 31 August 2008

p. OMB M-17-09, *Management of Federal High Value Assets*, 9 December 2016

q. OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, 3 January 2017 (including US-CERT Federal Incident Notification Guidelines cited therein at footnote 44)

r. OMB M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*, 9 November 2020

ENCLOSURE GL

GLOSSARY OF TERMS AND ABBREVIATIONS

PART I—ACRONYMS AND ABBREVIATIONS

CIO	Chief Information Officer
CL	Civil Liberties
CUI	Controlled Unclassified Information
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDM	Department of Defense Manual
DPCLTD	Defense Privacy, Civil Liberties, and Transparency Division
EDIPI	Electronic Data Interchange Personal Identifier
E.O.	Executive Order
E-MAIL	Electronic Mail
FIPS	Federal Information Processing Standards
IDA	Initial Denial Authority
IG	Inspector General
J006	USSPACECOM Staff Judge Advocate
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OPR	Office of Primary Responsibility
PA	Privacy Act
PAA	Privacy Act Advisory
PAS	Privacy Act Statement
PCLO	Privacy and Civil Liberties Officer
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
SAOP	Senior Agency Official for Privacy
SCOP	Senior Component Official for Privacy
SOR	System of Record
SORN	System of Record Notice
SSN	Social Security Number
TDY	Temporary Duty
USSPACECOM	United States Space Command

PART II-- DEFINITIONS

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

Amendment—The process of adding, deleting, or changing information in an SOR to make the data accurate, relevant, timely, or complete.

Civil Liberties—Fundamental rights and freedoms protected by the United States Constitution.

Controlled Unclassified Information (CUI)—Types of information that require application of controls and protective measures for a variety of reasons.

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

Disclosure—Giving information from an SOR, by any means, to anyone other than the record subject.

Individual—A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. The parent of a minor of the legal guardian of any individual also may act on behalf of an individual. Members of the United States Armed Forces are "individuals." Corporations, partnerships, sole proprietorships, professional groups, business, whether incorporated or unincorporated, and other commercial entities are not "individuals." Reference DoDD 5400.11.

Individual Identifier—Information associated with a single individual and used to distinguish him or her from other individuals, e.g., name, SSN or other identifying number, symbol, or other identifying particular such as a finger or voice print or photograph.

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

Personal Information—Information about an individual other than items of public record.

Personally Identifiable Information (PII)—Any information about an individual maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, SSN, date and place of birth, mother's maiden name, biometric records, etc., including any PII which is linked or linkable to an individual.

Privacy Act Request—An oral or written request by an individual about his or her records in a system of records.

Privacy Act Advisory (PAA)—A statement required when soliciting PII by an Air Force web site and the information is not maintained in a SOR. The PAA informs the individual why the information is being solicited and how it will be used.

Privacy Act Complaint—An allegation that the Agency did not comply with specific provisions of the Privacy Act, with respect to the maintenance, amendment, or dissemination of SOR.

Privacy Act Statement—A statement required when soliciting personally identifiable information that is maintained in a SOR (known as Personal Information). The Privacy Act Statement informs the individual why the information is being solicited and how it will be used.

Record—Any information about an individual.

Routine Use—A disclosure of records to individuals or agencies outside DoD for a use compatible with the purpose for which the Air Force created the records.

System Manager—The official who is responsible for managing an SOR, including policies and procedures to operate and safeguard it. Local system managers operate record systems or are responsible for part of a decentralized system.

System of Record Notice—The official public notice published in the *Federal Register* of the existence and content of the SOR.

System of Records—A group of records retrieved by the individual's name, personal identifier, or individual identifier through a cross-reference system.

Violation of Civil Liberties—Undue interference with the exercise of civil liberties.