Army Regulation 25–22

Office Management

The Army Privacy and Civil Liberties Program

Headquarters
Department of the Army
Washington, DC
30 September 2022

UNCLASSIFIED

SUMMARY of CHANGE

AR 25–22
The Army Privacy and Civil Liberties Program

This administrative revision, dated 6 June 2023—

- Changes proponency from the Administrative Assistant to the Secretary of the Army to the Chief Information Officer (title page).

This expedited revision, dated 30 September 2022—

- Changes the title from The Army Privacy Program to The Army Privacy and Civil Liberties Program (cover).
- Establishes the Army Civil Liberties Program in accordance with DoDI 5400.11 (chap 1).
- Adds the Rules of Conduct in accordance with DoDI 5400.11 (chap 1).
- Updates the Fair Information Practice Principles to align with DoDI 5400.11 (chap 1).
- Modifies the applicability to contractors in accordance with Subpart 24.1 of the Federal Acquisition Regulation (chap 1).
- Clarifies that the regulation does not create any rights against the United States (para 1–1*h*).
- Updates the responsibilities of the Senior Component Official for Privacy in accordance with DoDI 5400.11 (chap 2).
- Updates the responsibilities of the Army Privacy and Civil Liberties Officer in accordance with DoDI 5400.11 (chap 2).
- Updates the elements of a System of Records Notices and Narrative Statement (para 3–2).
- Updates the relationship between Privacy and the Freedom of Information Act (chap 6).
- Removes Privacy Review Board in accordance with Army Reform Initiative #85 (chap 8).
- Updates the Breach Reporting Process to align with DoDM 5400.11, Volume 2 and Office of Management and Budget Memorandum 17–12 (chap 9).
- Removes Exemption Rules (Rules codified in 32 CFR 310).
- Removes the DoD Routine Uses (Routine Uses codified in 32 CFR 310).
- Removes figures for System of Records notices and Narrative Statement.

Headquarters
Department of the Army
Washington, DC
30 September 2022

*Army Regulation 25–22

Effective 30 September 2022

Office Management

The Army Privacy and Civil Liberties Program

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:

MARK F. AVERILL
Administrative Assistant to the Secretary of the Army

History. This publication is an administrative revision. The portions affected by this administrative revision are listed in the summary of change.

Summary. This regulation on the Army Privacy and Civil Liberties Programs has been revised. It supplements DoDI 5400.11.

Applicability. This regulation applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Proponent and exception authority. The proponent of this regulation is the Chief Information Officer. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific requirements.

Army internal control process. This regulation contains internal control provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see app C).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Administrative Assistant to the Secretary of the Army (AAHS–RDF), Fort Belvoir, VA 22060–5605.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) via email to usarmy.pentagon.hqda-cio.mbx.policy-inbox@army.mil.

Distribution. This regulation is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

*This regulation supersedes AR 25–22, dated 22 December 2016.

Chapter 1
General Information

1–1. Purpose

The purpose of this regulation is to establish and maintain a comprehensive Army Privacy and Civil Liberties Program that complies with applicable statutory, regulatory, and policy requirements. Army policy concerning the privacy and civil liberties of individuals and the Army's responsibilities for compliance with the Privacy Act (PA) are as follows:

a. Comply with all applicable guidelines—

(1) Privacy and civil liberties related laws, including requirements of the PA of 1974, while ensuring that the PA system of records notices (SORNs) are published, revised, and rescinded, as required.

(2) Privacy statutes and policies governing the disclosure or dissemination of information, and any other valid access, use, and dissemination restrictions.

(3) Executive orders (EOs), Intelligence Community directives, and other applicable guidance to DoD Components conducting intelligence activities with respect to privacy and civil liberties matters (for example, EO 12333 and DoDM 5240.01).

b. Maintain all records with personally identifiable information (PII) in accordance with AR 25–400–2 which mandates use of the Army records retention schedule according to the National Archives and Records Administration.

c. Limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII to that which is legally authorized, relevant, and reasonably deemed necessary to accomplish the Army's function.

d. Impose conditions when sharing PII with other federal and non-federal agencies or entities (including the selection and implementation of particular security and privacy controls) that govern the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of the PII, where appropriate. This will be accomplished using written agreements, including contracts, data use agreements, information exchange agreements, and memoranda of understanding.

e. Maintain adequate procedures to receive, investigate, respond to, and redress complaints from individuals who allege that the organization has violated their privacy and civil liberties.

f. Prohibit reprisals or the threat of reprisals against individuals who make complaints or disclose information that indicates a possible violation of privacy protections or civil liberties in the administration of the programs and operations of the Federal Government to the privacy or civil liberties officers as described in Subsection (a) or (b) of Section 2000ee–1, Title 42, United States Code (42 USC 2000ee–1).

g. Ensure no reprisals or threats of reprisal take place against individuals who make complaints, unless the complaint was made or the information was disclosed with the knowledge that it was false or with willful disregard for its truth or falsity.

h. This regulation does not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party against the United States, its departments, agencies, other entities, its officers, or any other persons.

1–2. References and forms

See appendix A.

1–3. Explanation of abbreviations and terms

See glossary.

1–4. Responsibilities

Responsibilities are listed in chapter 2.

1–5. Records management (recordkeeping) requirements

The records management requirement for all record numbers, associated forms and reports required by this regulation are addressed in the Army Records Retention Schedule–Army (RRS–A). Detailed information for all related record numbers, forms and reports is located in Army Records Information Management System (ARIMS), ARIMS/RRS–A at https://www.arims.army.mil/. If any record numbers, forms, and reports are not current, addressed, and/or published correctly in ARIMS/RRS–A, see DA Pam 25–403 for guidance.

1–6. Legal authority

The PA of 1974 as amended, 5 USC 552a, and 42 USC 2000ee–1 are the statutory bases for the Army Privacy and Civil Liberties Program. Within the DoD, the Privacy Act is implemented by 32 CFR 310, DoDI 5400.11, and DoD 5400.11–R. The PA assigns—

a. Overall Government-wide responsibilities for implementation to the Office of Management and Budget (OMB).

b. Specific responsibilities to the Office of Personnel Management (OPM) and the General Services Administration (GSA).

1–7. Rules of conduct

The Army is committed to protecting the privacy and civil liberties of Soldiers, DA Civilians, and individuals considered members of the public to the greatest extent possible, consistent with its mission and operational requirements regarding the collection, use and sharing of personal information.

a. Consistent with applicable law, information about an individual that is collected, used, maintained, or disseminated by Army activities will be—

(1) Legally authorized, relevant, and necessary to accomplish the Army's mission.

(2) Relevant, timely, complete, and accurate for its stated purpose.

(3) Collected directly from the individual to the greatest extent practicable. The individual will be informed of—

(a) The specific purpose or purposes for which the information is intended to be used.

(b) The authority for collection.

(c) How the PII may be used.

(d) Whether disclosing of such information is mandatory or voluntary.

(e) The consequences to the individual for not providing the information.

b. The records used in any determination about any individual will be maintained with such accuracy, relevancy, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual in the determination.

c. Army activities will establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and protect against any anticipated threats or hazards to their security or integrity that would result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

d. Army activities will make reasonable efforts to ensure records are accurate, timely, and relevant for the Army's purposes before disseminating any record about an individual to any person or to another federal or non-federal agency. This requirement does not apply if the record is being released pursuant to 5 USC 552, also known and referred to in this regulation as the Freedom of Information Act (FOIA).

e. Disclosure of records pertaining to an individual from a system of records (SOR) is prohibited in the absence of the individual's consent except as authorized by the PA of 1974 and the FOIA.

f. Pursuant to the PA of 1974, no record will be maintained on how an individual exercises rights guaranteed by the First Amendment of the United States Constitution, except when—

(1) Expressly authorized by statute, or

(2) Expressly authorized by the individual who is the subject of the record, or

(3) Pertinent to and within the scope of an authorized law enforcement, intelligence collection, or counterintelligence activity.

g. Protected health information (PHI) will be disclosed in accordance with DoDM 6025.18. Questions regarding disclosing PHI should be referred to the Defense Health Agency Privacy Office.

h. Army activities will report any unauthorized disclosures of PII and PHI from a SOR to the Senior Component Official for Privacy (SCOP) or the Army Privacy and Civil Liberties Officer (APCLO).

1–8. Applicability to Government contractors

a. In accordance with OMB M–17–12; DoDM 5400.11, Volume 2; and the Federal Acquisition Regulation, Subpart 24, when an Army activity contracts for the design, development, or operation of a SOR on individuals to accomplish a function, the organization must apply the requirements of the PA to the contractor and its employees working on the contract.

b. An agency officer or employee may be criminally liable for violations of the PA. When the contract provides for operation of a SOR on individuals, contractors and their employees are considered employees of the organization for purposes of the criminal penalties of the PA.

1–9. Fair Information Practice Principles

The Fair Information Practice Principles (FIPPs), originally developed in 1973 by the Department of Health, Education, and Welfare, formed the conceptual core for the PA of 1974. Army activities should apply these principles when handling records containing PII.

a. Access and amendment. Provide individuals with appropriate access to PII and appropriate opportunity to correct or amend their records that contain PII.

b. Accountability. Hold personnel accountable for complying with measures that implement the FIPPs and applicable privacy requirements, and appropriately monitor, audit, and document compliance. Clearly define the roles and responsibilities with respect to PII for all employees and contractors, and provide appropriate training to all employees and contractors who have access to PII.

c. Authority. Create, collect, use, process, store, maintain, disseminate, or disclose PII only with the proper authority to do so and identify this authority in the appropriate SORN.

d. Minimization. Create, collect, use, process, store, maintain, disseminate, or disclose PII only when it is directly relevant and necessary to accomplish a legally authorized purpose, and only maintain PII for as long as is necessary to accomplish the purpose.

e. Quality and integrity. Create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

f. Individual participation. Involve the individual in the process of using PII and, to the extent practicable, seek individual consent for creating, collecting, using, processing, storing, maintaining, disseminating, or disclosing PII. Establish procedures to receive and address individuals' privacy-related complaints and inquiries.

g. Purpose specification and use limitation. Provide notice of specific purpose for which PII is collected and only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

h. Security. Establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

i. Transparency. Be transparent about information policies and practices with respect to PII, and provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

1–10. General provisions

a. Consider privacy and civil liberties in the development, implementation, and review of new or existing regulations, policies, and initiatives.

b. Protect the privacy and civil liberties of Soldiers, Army civilian employees, and the public (persons and organizations not affiliated with DoD) to the greatest extent possible, consistent with DoDD 5200.27 and operational requirements.

c. Ensure that neither the Army nor any subordinate command or agency will collect, report, process, maintain, or disseminate any information on how an individual, group of individuals, or association exercises fundamental rights, specifically including the freedoms of speech, assembly, press, and religion, except when—

(1) Specifically authorized by statute; or

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

(3) Pertinent to and within the scope of an authorized law enforcement, intelligence collection, or counterintelligence activity.

d. Have adequate procedures to receive, investigate, respond to, and redress complaints from individuals who allege that the Army has violated their privacy or civil liberties.

e. Individual privacy rights policy. Although deceased individuals do not have PA rights, family members or next-of-kin may have limited privacy rights with respect to the release of information regarding the death and the funeral arrangements of the deceased individual. Family members often use the deceased individual's Social Security number (SSN) or DoD identification (ID) data number for Federal entitlements. Also, the Health Insurance Portability and Accountability Act (HIPAA) extends protection to certain medical information contained in a deceased individual's medical records. Appropriate safeguards must be implemented to protect the deceased individual's PII and PHI.

f. Reprisals or the threat of reprisals are prohibited against individuals who make complaints or disclose information that indicates a possible violation of privacy protections or civil liberties in the administration of the Army's programs and operations to privacy or civil liberties officials. Appropriate disciplinary action under law and regulation will be considered for all violations.

1–11. Special handling provisions

a. Send privacy protected data electronically via email and the world wide web according to the following guidelines:

(1) The PA requires that appropriate technical safeguards be established based on the media used to ensure the security of the records and to prevent compromise or misuse during transfer.

(2) Sensitive PII, such as SSNs, is to be transmitted via encrypted email or password protected. When sending PA protected information within the Army across encrypted or dedicated lines, ensure that—

(a) Each addressee has an official "need to know." Remove any recipient without a "need to know" from all addressee fields.

(b) Information protected by the PA is marked "Controlled Unclassified Information (CUI)" to inform the recipient of limitations on further dissemination. For example, add CUI to the beginning of an email message, along with appropriate language such as the following: "This message contains personal or privileged information which is protected under the PA of 1974, as amended. Do not further disseminate this information without the permission of the sender."

(c) For email with an attachment, include a statement similar to the following: "If you are not the intended recipient, please delete this email including any attachments, and notify the sender that you have done so."

(d) Unclassified information associated with the PA and identified as needing safeguarding is considered CUI. It requires access control; handling, marking, dissemination control; and other protective measures for safeguarding. CUI information may qualify for withholding from public release based on a specific FOIA exemption.

(e) For additional information about CUI marking and dissemination instructions, refer to DoDI 5200.48.

(3) Add appropriate privacy and security notices at major website entry points. Refer to AR 25–1 for requirements on posting privacy and security notices on public websites.

(4) Ensure Army websites are in compliance with policies regarding restrictions on persistent and third-party cookies. The Army prohibits both persistent and third-party cookies.

(5) Add a Privacy Act Advisory (PAA) on websites with host information systems soliciting PII, even when not maintained in a PA SOR. The PAA informs the individual as to why the information is being solicited and how it will be used. Post the PAA on the website where the information is being solicited, or to a well-marked hyperlink. Example wording is as follows: "Privacy Act Advisory—Please refer to the Privacy and Security Notice that describes why this information is collected and how it will be used."

b. Protect paper records containing personal identifiers such as name and SSN as follows:

(1) Only those records covered by a SORN may be arranged to permit retrieval by a personal identifier (for example, an individual's name or SSN). AR 25–400–2 requires all records thus covered to include the SOR identification number on the record label to serve as a reminder that the information contained within must be safeguarded.

(2) Use Standard Form (SF) 901 (CUI Cover Sheet) for individual records not contained in properly labeled file folders or cabinets (for example, log books or training materials).

1–12. Civil liberties

a. Civil liberties are fundamental rights and freedoms enjoyed by all individuals that cannot be restricted or deprived, without due process. Due process requires that these liberties can only be curtailed for a proper governmental objective and the affected individual must be given notice of the proposed restriction or deprivation, and an opportunity to argue before a neutral decision maker that the civil liberties should be preserved.

b. The U.S. Constitution protects civil liberties. While the U.S. Constitution explicitly identifies certain civil liberties, others can also be expressed, explicitly or implicitly, by state or federal law or judicial interpretation.

c. Civil liberties include, but are not limited to the following:

(1) Freedom of speech (First Amendment).

(2) Freedom of religion (First Amendment).

(3) Freedom to assemble (including peaceful protest) (First Amendment).

(4) Freedom of the press (First Amendment).

(5) The right to keep and bear arms (Second Amendment).

(6) Freedom from unreasonable searches and seizures (Fourth Amendment).

(7) The prohibition against deprivation of life, liberty, or property without due process of law (Fifth Amendment).

(8) The right not to answer incriminating questions (Fifth Amendment).

(9) Freedom from the deprivation of rights not included in the U.S. Constitution but retained by the people (Ninth Amendment).

Chapter 2
Responsibilities

2–1. The Secretary of the Army

In accordance with DoDI 5400–11, the Secretary of the Army will—

a. Provide adequate resources to support and maintain an effective Army Privacy and Civil Liberties Program.

b. Ensure that the SCOP and APCLO periodically review Army implementation of, and compliance with, the DoD Privacy and Civil Liberties Program.

c. Program and budget to fund, without reimbursement, the administrative and logistical support required to perform the Army's assigned Combatant Command privacy and civil liberties mission as identified in DoDD 5100.03.

2–2. Headquarters, Department of Army principal officials, Army commands, Army service component commands, and direct reporting units

HQDA principal officials, ACOMs, ASCCs, and DRUs, as listed in AR 10–87, will—

a. Implement and execute the Army Privacy and Civil Liberties Program.

b. Appoint a Privacy and Civil Liberties Officer (PCLO) for each HQDA principal official, ACOM, ASCC, and DRU in writing, and inform the APCLO. The PCLOs will—

(1) Promote privacy and civil liberties awareness throughout their respective organizations.

(2) Compile data for the Semi-annual DoD Privacy and Civil Liberties Officer's Report in accordance with 42 USC 2000ee–1.

(3) Ensure adequate procedures are in place for the management and remediation of privacy and civil liberties complaints and alleged violations.

(4) Ensure privacy and civil liberties are considered when proposing, developing, or implementing regulations, policies, procedures, or guidelines related to their mission.

(5) Implement semiannual privacy and civil liberties complaint reporting procedures.

(6) Ensure that PA records collecting and maintaining PII are properly described in a PA SOR notice published in the Federal Register (FR).

(7) Ensure no undeclared SORs are being maintained.

(8) To the extent authorized by the PA and using procedures outlined in 32 CFR 310 and the respective SORN:

(a) Process requests from individuals for access to records or to information pertaining to the individual.

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

(c) Correct or amend such records if it has been determined that the records are not accurate, relevant, timely, or complete, unless exemption applies.

(d) Review SORNs biennially to ensure that they accurately describe the SOR.

(9) Review recordkeeping practices annually to ensure compliance with privacy and civil liberties maintenance and retention guidelines, paying particular attention to the maintenance of automated records. In addition, ensure coordination with records management officials on such matters as maintenance and disposal procedures, statutory requirements, forms, and reports.

(10) Maintain narrative and statistical data for preparation of required reports (for example, Public Law (PL) 110–53 reporting for the Defense Privacy, Civil Liberties, and FOIA Directorate (DPCLFD)).

(11) Process reports of suspected PA or civil liberties violations in accordance with chapter 9 of this regulation.

(12) Review PA and civil liberties training practices annually to ensure that all personnel are familiar with the requirements of the program. Develop and provide a privacy and civil liberties training program for all personnel involved in the design, development, custody, maintenance, and use of a SOR.

(13) Review, if applicable, ongoing Computer Matching Agreements. The Defense Data Integrity Board approves Computer Matching Agreements for 18 months, with an option to renew for an additional year. The renewal review ensures that the requirements of the PA, OMB guidance, and the requirements contained in the matching agreements have been met.

(14) Collaborate, as necessary and appropriate, with information management, information collection, information security, forms and publications management, records management, Chief Information Officer (CIO), and attorney and legal advisor staffs.

c. Ensure each SOR has an Information system or electronic collection (ISEC) owner appointed . The ISEC will—

(1) In collaboration with the PCLO, review and approve the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII in accordance with Committee for National Security Systems Instruction No. 1253, Appendix F.

(2) Review the System Privacy Plans portion of the System Security Plans for information systems containing PII before authorization, reauthorization, or ongoing authorization.

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

(4) Identify and maintain an inventory of high-value assets (HVAs), as defined in OMB Memorandum M–17–09.

(5) Ensure that the SCOP, through the PCLO, is aware of information systems containing PII that cannot be appropriately protected or secured, and that such systems are given a high priority for upgrade, replacement, or retirement.

(6) When seeking information technology (IT) investment funding, coordinate with the PCLO and the CIO to ensure necessary privacy risk management efforts are accounted for in the request.

(7) Complete and coordinate with the PCLO regarding the DD Form 2930 (Privacy Impact Assessment (PIA)), for information systems in accordance with DoDI 5400.16.

(8) Prepare new, amended, or altered PA systems of records notices and submit them to the APCLO through the PCLO. The APCLO assigns a system identifier and submits the document to DPCLFD for review.

(9) Review the routine use disclosures associated with each PA SORN based on OMB guidance in order to determine if such routine use continues to be compatible with the original collection purpose.

(10) Review, biennially, contracts that provide for the maintenance of a PA SOR to accomplish an activity's mission. This requirement ensures each contract contains provisions that bind the contractor and its employees to the requirements of 5 USC 552a(m)(1).

d. Ensure that contracts requiring the operation of a SOR on behalf of the Army include provisions levying the requirements of the PA, as well as any other responsibilities concerning the protection of privacy and civil liberties.

e. Evaluate all Army legislative, regulatory or other policy proposals for consistency with the privacy and civil liberties requirements of this regulation and DoD 5400.11–R.

f. Assess the impact of technology on privacy and the protection of PII and, when feasible, adopt privacy-enhancing technology and safeguards to:

(1) Safeguard PII contained in Army PA SORs.

(2) Collect and maintain the minimum amount of PII needed to accomplish the missions and functions of the Army.

(3) Minimize the collection and use of SSNs in accordance with DoDI 1000.30.

(4) Audit compliance with the requirements of this regulation and DoD 5400.11–R.

(5) As appropriate, use de-identification and/or anonymization technology to reduce risks to collections of PII.

g. Ensure Army personnel and Army contractors, who have primary responsibility for implementing the Army Privacy and Civil Liberties Program, receive appropriate privacy and civil liberties training. Define any such roles and responsibilities in applicable contracts, including privacy and civil liberties, security, and compliance controls contained in the Federal Acquisition Regulation and Defense Federal Acquisition Regulations (DFARS).

h. For Heads of Joint Service agencies or commands for which the Army is the Executive Agent or for which the Army otherwise provides fiscal, logistical, or administrative support, adhere to the policies and procedures in this regulation.

2–3. The Assistant Secretary of the Army (Manpower and Reserve Affairs)

The ASA (M&RA) develops and oversees policies and programs for Army nonappropriated fund instrumentalities. The ASA (M&RA), the Assistant Secretary of the Army (Financial Management and Comptroller), and Deputy Chief of Staff, G–4 Logistics, in coordination with the Assistant Secretary of the Air Force, Manpower and Reserve Affairs, will ensure that the Director/Chief Executive Officer, Army and Air Force Exchange Service (AAFES)—

a. Establish and maintain a comprehensive Army Privacy and Civil Liberties Program that complies with applicable statutory, regulatory, and policy requirements; develops and evaluates privacy and civil liberties policies; and manages privacy risks (see DoDI 5400.11).

b. Ensure that AAFES personnel comply with all applicable privacy and civil liberties related laws, regulations, and policies, including this regulation.

2–4. General Counsel

The GC will—

a. Coordinate with the SCOP on policy guidance for the Army Privacy and Civil Liberties Program.

b. Determine the DA position on legal questions or procedures related to the Army Privacy and Civil Liberties Program.

2–5. Chief Information Officer

The CIO will, in accordance with DoDI 5400.11—

a. Ensure implementation of the responsibilities and procedures in this AR with respect to the security of Army information systems.

b. Provide policy, standards, and guidance in accordance with DoDD 5144.02 and applicable Army regulations and pamphlets.

c. Maintain an accurate inventory of Army information systems containing HVAs.

d. Manage the PIA Program in accordance with the DoDI 5400.16.

e. Review and assess security safeguards for Army information technology systems in relation to PII Breaches.

f. Ensure the Senior Information Security Officer (SISO) develops and maintains the Army cybersecurity program in accordance with FISMA to protect PII.

g. Review and approve the Army information technology (IT) investments budget request to ensure compliance with privacy risk management requirements.

h. Designate a representative from the CIO to serve as a member of the Defense Data Integrity Board.

i. Facilitate exchange of information necessary to evaluate privacy risk associated with an information system's implementation of privacy and security controls, and any associated residual risk between the SISO and the SCOP.

j. In coordination with the authorizing officials and SCOP, implement a risk management framework to guide and inform the categorization of Army information and information systems; the selection, implementation, and assessment of privacy controls; the authorization of information systems; and the continuous monitoring of information systems.

k. When seeking IT investment funding, coordinate with the SCOP to ensure necessary privacy risk management efforts are accounted for in the request.

2–6. Chief of Public Affairs

The CPA will—

a. Provide guidance on communicating to the media and public concerning major Army incidents involving PII, as well as other breaches that may generate public or media interest, and communicates with the media and public concerning incidents involving PII when appropriate.

b. Serve, or designate a representative to serve, as a member of the Army Breach Response Team.

2–7. Deputy Chief of Staff, G–6

The DCS, G–6 will—

a. Manage the PIA Program in accordance with the E-Government Act, Section 208.

b. Work in collaboration with the SISO, the SCOP, and the APCLO to review and assess security safeguards for information technology systems in relation to PII Breaches.

2–8. The Judge Advocate General

TJAG will—

a. Provide legal advice to Privacy and Civil Liberties Officers, commanders, and supervisors on requests for PA records under the PA and FOIA.

b. Serve (via Litigation Division) as a liaison between the Army and the Department of Justice.

2–9. Chief of Legislative Liaison

The CLL will—

a. Provide guidance when major incidents involving PII are reported to Congress and reviews and oversees the transmission of required reports to DoD.

b. Serve as the interface between Army and DoD for congressional inquiries arising from incidents involving PII.

c. Serve or designate a representative to serve, as a member of the Army Breach Response Team.

2–10. Senior Component Official for Privacy

The Executive Director, U.S. Army Enterprise Services Agency, is the Army's Senior Component Official for Privacy (SCOP). The SCOP will—

a. Oversee and provide strategic direction for the Army Privacy and Civil Liberties Program.

b. Provide advice and information to the DoD SAOP and Army senior leaders on privacy issues and civil liberties concerns within his or her respective component.

c. Ensure employee awareness of privacy and civil liberties and accompanying responsibilities to protect them.

d. In accordance with DoDI 8510.01 and in conjunction with the SISO and the Army Risk Management Advisory Group—

(1) Review and approve the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII in accordance with Committee for National Security Systems Instruction No. 1253, Appendix F.

(2) Designate which privacy controls will be treated as program management, common, information system-specific, or hybrid privacy controls in the Army.

(3) Use the Privacy Overlay found in Committee for National Security Systems Instruction No. 1253, Attachment 6 of Appendix F 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.

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

e. Identify 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.

f. Coordinate with authorizing officials on granting authorization to operate decisions for information systems.

g. Ensure that the DoD SAOP is aware of information systems and Army 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.

h. Comply with OMB Memorandum M–17–12 and DoDM 5400.11, Volume 2. Implement the Army Breach Preparedness and Response Plan and, as necessary, establish Army breach management policies. Ensure adequate training and awareness is provided to military, civilians, and contractors on how to report, respond to, and mitigate breaches of PII. For breaches involving PHI, 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 Manual 6025.18.

i. Ensure adequate procedures are in place for the management and remediation of both privacy and civil liberties complaints and alleged violations.

j. Review and approve reports as required for submission to the DPCLFD.

k. Establish as necessary an Army-level program to provide employee awareness of privacy and civil liberties as well as supervisor and senior-leader understanding of responsibilities to protect privacy and civil liberties. The program must include and disseminate procedures for submitting and responding to complaints of violations.

l. Ensure Army compliance with DoD Privacy and Civil Liberties Program reporting requirements and supplemental guidance. Ensure procedures are in accordance with all applicable federal laws, regulations, policies, and procedures.

2–11. Army Privacy and Civil Liberties Officer

The Director, Army Records Management Directorate, is the Army Privacy and Civil Liberties Officer (APCLO). The APCLO will—

a. Execute duties in coordination with the SCOP.

b. Ensure that policies, procedures, and systems for protecting the privacy and civil liberties of individuals are implemented throughout the Army in accordance with applicable laws.

c. Review legislative, regulatory, and other policy proposals with privacy and civil liberties implications.

d. Serve as a voting member on the Defense Data Integrity Board and the Defense Privacy Board.

e. Review proposed new and modified SORNs and proposed rescindment of SORNs in accordance with the PA of 1974, OMB Circular No. A–108, DoD 5400.11–R, and submit to DoD for coordination.

f. Review proposed privacy exemption rules in accordance with the PA, OMB Circular No. A–108, and DoD 5400.11–R.

g. Provide guidance, assistance, and support to the Army activities in their implementation of the Army Privacy and Civil Liberties Program to ensure that all requirements developed to maintain PII conform to DoD's Privacy and Civil Liberties Program standards.

h. Complete and submit the Federal Information Security Modernization Act of 2002 (FISMA) Annual Report and related OMB FISMA guidance.

i. Complete and submit a DD Form 2984 (Component Privacy and Civil Liberties Report) in accordance with 42 USC 2000ee–1.

j. Complete other reports, as required.

k. Develop standards and reporting guidance for Army activities for the management and reporting of alleged violations of privacy and civil liberties.

l. Ensure that the Army has adequate procedures in place to receive, investigate, respond to, and redress complaints from individuals who allege violation of their privacy or civil liberties.

m. In conjunction with the Army CIO, maintain an accurate inventory of Army's information systems containing HVAs.

n. Serve as the approval authority for SSN use and justification for all Army forms containing SSNs. Provide guidance to support DoD efforts in SSN collection, use, dissemination, and reduction in accordance with DoDI 1000.30 and Public Law 115–59, also known as the Social Security Number Fraud Prevention Act of 2017.

o. As appropriate, authorize written requests pursuant to 5 USC 552a(b)(7) for records maintained by other agencies that are necessary for an authorized law enforcement activity. This authorization may be delegated no lower than the section chief level.

Chapter 3
Systems of Records, Privacy Impact Assessments, and Computer Matching

3–1. Privacy Act system of records

a. A PA SOR is a group of records, whatever the storage media (paper or electronic), under the control of an Army activity from which personal information about an individual is retrieved by the name of the individual, or by an identifying number, symbol, or other identifying particular assigned, that is unique to the individual.

b. The PA requires agencies to publish a SORN in the FR describing the existence and character of a new or modified SOR. A SORN is comprised of the FR notice(s) that identifies the SOR, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system.

c. Notices of all Army SOR are required by the PA to be published in the FR when establishing a new SOR and when making significant changes to an existing SOR. Significant changes are those that are substantive in nature and therefore warrant a revision of the SORN in order to provide notice to the public of the modified SOR. The following are some examples of significant changes:

(1) Increases or changes in the number or types of individuals on whom records are kept so that it significantly alters the character and purpose of the SOR.

(2) Expansion of the types or categories of information maintained.

(3) Changes to the manner in which records are organized, indexed, or retrieved to change the nature or scope of those records.

(4) Changes to the purposes for which the information is used, or addition of a routine use that is not compatible with the purpose for which the system is maintained.

(5) Changes to the equipment configuration on which the system is operated, to create potential for either greater or easier access.

d. This is not an exhaustive list of significant changes that would require a revised SORN. Other changes to a SOR would require a revised SORN if the changes are substantive in nature.

3–2. Elements of a system of records notice

a. Each notice of a new or modified SOR should be drafted using the following elements:

(1) System name and number.
(2) Security classification.
(3) System location.
(4) ISEC owner(s).
(5) Authority for maintenance of the system.
(6) Purpose(s) of the system.
(7) Categories of individuals covered by the system.
(8) Categories of records in the system.
(9) Record Source categories.
(10) Routine uses of records maintained in the system, including categories of users and purposes of such uses.
(11) Policies and practices for storage of records.
(12) Policies and practices for retrieval of records.
(13) Policies and practices for retention and disposal of records.

(14) Administrative, technical, and physical safeguards.
(15) Records access procedures.
(16) Contesting record procedures.
(17) Notification procedures.
(18) Exemptions promulgated for the system.
(19) History.

b. Report of a new or altered system should include a narrative statement. The narrative statement must contain the following:

(1) System name and number.
(2) Purpose for establishing the system.
(3) Specific authority under which the SOR is maintained.
(4) Evaluation of the probable or potential effect on the privacy of individuals.
(5) Routine use compatibility.
(6) OMB public information collection requirements.

c. ISECs must send a proposed notice through their PCLO to the APCLO, at least 120 days before implementing a new or altered system. For an example of a completed SORN, a completion checklist, and a sample narrative statement, see https://www.rmda.army.mil/.

d. Supporting documentation consists of a system notice for the proposed new or altered system, PIA, SSN Justification, and a proposed exemption rule, if applicable.

e. The existence of a statute or EO mandating the maintenance of a SOR to perform an authorized activity does not remove the responsibility to ensure the information in the SOR is relevant and necessary to perform the authorized activity.

f. An OMB Control Number may be required before implementation of a SOR collecting information from the public. OMB, based on the Paperwork Reduction Act of 1995, assigns control numbers for information collection requirements that are not mandated by statute. For additional information about OMB Control Numbers, see DoDM 8910.01–V1.

3–3. Privacy Impact Assessment

The E-Government Act Section 208 requires all Federal government agencies that develop or procure IT involving the collection; maintenance, or dissemination of information in identifiable form or that make substantial changes to existing IT that manages information in identifiable form complete a PIA. See DoDI 5400.16 and AR 25–1 for additional information on PIAs.

3–4. Computer matching

a. The Computer Matching and Privacy Protection Act of 1988 amends the PA to establish procedural safeguards affecting agencies use of PA records in performing certain types of computerized programs.

b. Computer matching covers the use of records from Federal personnel or payroll systems and Federal benefit programs where matching meets the following criteria:

(1) To determine eligibility for federal benefit;
(2) Determine compliance with benefit program requirements; or
(3) Recover improper payments or delinquent debts from current or former beneficiaries.

c. The comparison of records must be computerized; manual comparisons do not apply. In all cases, Computer Matching Agreements are processed by the DPCLFD as specified in DoD 5400.11–R and approved by the Defense Data Integrity Board. The Director, Army Records Management Directorate (ARMD) is a member of the Defense Data Integrity Board. Agreements are conducted in accordance with the requirements of 5 USC 552a and OMB Circular A–130. For additional information regarding the computer matching publication and review requirements, see DoD 5400.11–R.

Chapter 4
Exemptions

4–1. Exempting systems of records

The Secretary of the Army or authorized designee may exempt Army SORs from certain requirements of the PA under the following provisions:

a. General exemption. Relieves SORs from most requirements of the PA. Only Army activities actually engaged in the enforcement of criminal laws as their primary function may claim exemption 5 USC 552a(j)(2).

b. Specific exemptions 5 USC 552a(k)(1)–(k)(7). Relieves SORs from a few selected provisions of the PA.

c. Access exemption. Relieves SORs from the access provision of the PA. This exemption applies to information compiled in reasonable anticipation of a civil action or proceeding. See 5 USC 552a*(d)(5).*

4–2. General exemption

Only Army activities actually engaged in the enforcement of criminal laws as their principal function may claim the general exemption. To qualify for this exemption, a SOR must consist of the following:

a. Information compiled to identify individual criminals and alleged criminals, which consists only of identifying data and arrest records; type and disposition of charges; sentencing, confinement, and release records; and parole and probation status.

b. Information compiled for the purpose of a criminal investigation, including efforts to prevent, reduce, or control crime, and reports of informants and investigators associated with an identifiable individual.

c. Reports identifiable to an individual, compiled at any stage of the process of enforcement of the criminal laws, from arrest or indictment through release from supervision.

4–3. Specific exemptions

a. Classified information. This exemption has been construed to permit the withholding of classified records from an agency employee with a security clearance who seeks only private access to records about himself or herself. Before denying an individual access to classified information, the Denial Authority must make sure that it was properly classified under the standards of EO 11652 or 12356 and that it must remain classified in the interest of National defense or foreign policy (see 5 USC 552a(k)(1)).

b. Investigatory data for law enforcement purposes (other than that claimed under the general exemption). Investigatory material compiled for law enforcement purposes, other than material within the scope of 5 USC 552a(j)(2). Provided, however, that if any individual is denied any right, right, privilege, or benefit to which the individual is entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material will be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section (September 27, 1975), under an implied promise that the identity of the source would be held in confidence (see 5 USC 552a(k)(2)).

c. Protective services. Records maintained in connection with providing protective services to the President of the United States or other individuals protected based on 18 USC 3056 (see 5 USC 552a(k)(3)).

d. Statistical data. Statistical data required by statute and used only for statistical, research, or program evaluation purposes, and not to make decisions on the rights, benefits, or entitlements of individuals, except for census records that may be disclosed under 13 USC 8 (see 5 USC 552a(k)(4)).

e. Investigatory material. Data compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section (September 27, 1975), under an implied promise that the identity of the source would be held in confidence (see 5 USC 552a(k)(5)).

f. Testing or examination material. Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process (see 5 USC 552a(k)(6)).

g. Evaluation material. Evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section (September 25, 1975), under an implied promise that the identity of the source would be held in confidence (see 5 USC 552a(k)(7)).

4–4. Army systems of records notices citing exemptions

a. When an ISEC owner seeks an exemption for a SOR, the following information should be furnished to the APCLO:

(1) Applicable system notice.

(2) Exemption(s) sought.

(3) Justification.

b. After appropriate staffing and approval by the Secretary of the Army, or authorized designee, the rule is forwarded to DPCLFD for publication in the FR (see DoDI 5400.11). No exemption may be invoked until these steps have been completed. Army SORNs citing exemptions are codified in 32 CFR 310. For the most current listing of Army SORNs, see the ARMD website at https://www.rmda.army.mil/privacy/sorns/armypublishedsorn.html.

Chapter 5
Handling and Safeguarding Personally Identifiable Information

5–1. Collecting personally identifiable information

a. When collecting PII, Army administrators and other users of PII must observe the provisions and guidelines described in this section. This section applies to Army military, civilians, and contractors.

b. General provisions for collecting PII are as follows:

(1) The Army collects PII directly from the subject of the record whenever possible. This is especially important when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs.

(2) When an Army activity asks an individual for his or her PII that will be maintained in a SOR, the activity must provide the individual with a Privacy Act Statement (PAS). A PAS notifies individuals of the authority, purpose, and use of the collection, whether the information is mandatory or voluntary, and the effects of not providing all or any part of the requested information. See paragraph 5–3 of this regulation when soliciting SSNs for any purpose.

c. A PAS must be prepared and administered based on the following guidelines:

(1) The Federal statute or EO that authorizes collection of the requested information.

(2) The principal purpose or purposes for which the information is to be used.

(3) The routine uses that will be made of the information.

(4) Whether providing the information is voluntary or mandatory.

(5) The PAS includes language that is explicit, easily understood, and concise.

(6) A sign is displayed in areas where people routinely furnish this kind of information, and a copy of the PAS is made available upon request by the individual.

(7) The individual reads but does not sign the PAS.

(8) A PAS must include the following items:

(a) Authority. Cite the specific statute or EO, including a brief title or subject that authorizes the DA to collect the PII requested.

(b) Principal purpose(s). Cite the principal purposes for which the information will be used.

(c) Routine use(s). Cite the routine uses for which the information may be used. The routine use should be specific and must align with the routine use included in the applicable SORN. If none, the language to be used is: ''Routine Use: None." However, the "Blanket Routine Uses" set forth at the beginning of the Army's compilation of systems of records notices may apply.

(d) Disclosure: Voluntary or Mandatory. Include in the PAS specifically whether furnishing the requested PII is voluntary or mandatory. A requirement to furnish PII is mandatory only when a Federal statute, EO, or other law specifically imposes a duty on the individual to provide the information sought, and when the individual is subject to a penalty if he or she fails to provide the requested information. If providing the information is only a condition of or prerequisite to granting a benefit or privilege and the individual has the option of requesting that benefit, then the collection is voluntary. However, the loss or denial of the privilege, benefit, or entitlement sought must be listed as a consequence of not furnishing the requested information.

d. Some acceptable means of administering the PAS are as follows, in the order of preference:

(1) Below the title of the media used to collect the PII (positioning the PAS so the individual will observe the PAS before providing the requested information).

(2) Within the body with a notation of its location below the title.

(3) On the reverse side with a notation of its location below the title.

(4) Attached as a tear-off sheet.

(5) Issued as a separate supplement.

e. The usage and elements of a PAS are described in appendix B.

f. Include a PAS on a website if the site requires information directly from an individual and the information is retrieved by his or her name or personal identifier.

g. When collecting PII from third parties, it may not be practical to collect personal information directly from the individual in all cases. Some examples of when third-party collection may be necessary include—

(1) To verify information.
(2) To solicit opinions or evaluations.
(3) To use another source when the subject cannot be contacted.
(4) At the request of the subject individual.

h. When asking third parties to provide information about other individuals, advise them of—

(1) The purpose of the request.
(2) Their rights to confidentiality as defined by the PA.

Note. Consult with your servicing Staff Judge Advocate for potential limitations to the confidentiality that may be offered.

i. Promises of confidentiality must be prominently annotated in the record to protect from disclosing any information provided in confidence based on 5 USC 552a(k)(2), 5 USC 552a(k)(5), or 5 USC 552a (k)(7).

5–2. Safeguarding personally identifiable information

a. The PA requires establishment of proper administrative, technical, and physical safeguards to—

(1) Ensure the security and confidentiality of records (for example, to periodically verify that only personnel with a current and valid need to know have access to shared drives and document management systems).

(2) Protect against any threats or hazards to the subject's security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness.

b. Ordinarily, PII must be afforded at least the protection required for information designated "Controlled Unclassified Information." PA data will be afforded reasonable safeguards to prevent inadvertent or unauthorized disclosure of record content during processing, storage, transmission, and disposal.

c. With the growing use of websites, the proliferation of social media, and the increasing risks of and cases of identity theft, the dimensions for the safeguarding of data have expanded exponentially in recent decades. Webmasters and web maintainers must apply appropriate privacy and security policies to respect user privacy. As specified in AR 25–1, organizations must screen their websites and display a privacy and security notice in a prominent location on at least the first page of all major sections of each website. Each website must clearly and concisely inform visitors to the site about any information the activity collects, why it is collected, and how it will be used.

d. Each privacy and security notice must clearly and concisely inform visitors to the site what information the activity collects about individuals, why it is collected, and how it will be used. If PII is requested in the notification and record access procedures, but not collected or listed in the categories of records, the reason for requesting the PII must be explained.

e. If the SSN is used for verification purposes, the custodian of the record must state "SSN required for verification purposes only."

f. The DA recognizes the importance of safeguarding PII in all forms of electronic media in addition to paper media. For information on approved Army use of social media, see website: https://www.army.mil/mobile/socialmedia.html.

5–3. Protecting Social Security numbers

a. When soliciting or using SSNs, Army administrators and other users of SSNs observe the provisions and guidelines described in this section and DoDI 1000.30. It is unlawful for any Federal, State, or local Government agency to deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to give their SSN unless the law requires disclosure, or a law or regulation adopted prior to January 1, 1975, required the SSN or if DA uses the SSN to verify a person's identity in a SOR established and in use before that date. EO 9397 (issued prior to January 1, 1975 and amended by EO 13478) authorizes the Army to solicit and use the SSN as a numerical identifier for individuals in most federal systems. However, the SSN should only be collected as needed to perform official duties. EO 9397 does not mandate the solicitation of SSNs from Army personnel as a means of identification.

b. Upon entrance into military service or civilian employment with DA, individuals are asked to provide their SSN. The SSN becomes the service or employment number for the individual and is used to establish personnel, financial medical, and other official records. After an individual has provided his or her SSN for the purpose of establishing a records, the PAS is not required if the individual is only requested to furnish or verify the SSN for identification purposes in connection with the normal use of his or her records. If the SSN is to be used for a purpose other than identification, the individual must be informed whether disclosure of the SSN is mandatory or voluntary; by what statutory authority the SSN is solicited; and what uses will be made of the SSN. This notification is required even if the SSN is not to be maintained in a PA SOR.

c. The current use of the DoD ID number is gradually replacing use of the SSN. Increased use of the DoD ID helps to minimize use of the SSN and assists with the safeguarding process. (See DoDI 1000.30 for additional information regarding acceptable uses of the SSN).

d. Army activities will continually review their use of the SSN to determine whether such use can be eliminated, restricted, or concealed in business processes, systems, and paper and electronic forms. While use of the SSN may be essential for program integrity and national security when information about an individual is disclosed outside the DoD, it may not be as critical when the information is being used for internal Departmental purposes.

e. The use of SSNs requires a SSN justification memorandum and an elimination plan signed by Senior Executive Service or general officer.

Chapter 6
Individual Access to Records and Denials

6–1. Individual access applicability

The PA's access provision permits an individual to gain access to "his or her record or to any information pertaining to him or her" that is contained in a SOR indexed and retrieved by their name or personal identifier (see 5 USC 552a(d)(1)).

a. Upon a written request, an individual will be granted access to information pertaining to him or her that is maintained in a PA SOR, except in the following conditions:

(1) The information is subject to an exemption, and the program manager has invoked the exemption.

(2) The information is compiled in reasonable anticipation of a civil action or proceeding.

b. Legal guardians or parents acting on behalf of a minor child have the rights of access under the PA, unless the records were created or maintained during circumstances where the interests of the minor child were adverse to the interests of the legal guardian or parent.

c. These provisions should allow for the maximum release of information consistent with Army and DoD statutory responsibilities.

Note. PA requests can be made only by requesters asking for information within a SOR concerning themselves, their minor children, and persons for whom legal guardianship has been established. (A minor is an individual under 18 years of age, who is not a member of the U.S. Army, or married. Minors of interest to this regulation are usually children or legal dependents of U.S. Army members; dependents are not necessarily minors.)

6–2. Individual requests for access

Individuals must submit requests for access to records in a PA SOR to the program manager or the custodian of the record designated in DA SORNs. For the most current listing of Army SORNs, see the ARMD website at https://www.rmda.army.mil/privacy/sorns/armypublishedsorn.html.

a. Individual requests for record access must be submitted in writing.

b. Individuals do not have to state a reason or justify the need to gain access to records under the PA. However, requesters should reasonably describe the records they are requesting.

c. Before granting access to personal data, an individual must provide verification of identity (for example, submission of a notarized signature). An alternative method for verifying identity is an un-sworn declaration in accordance with 28 USC 1746 in the following format:

(1) If executed within the United States, its territories, possessions, or commonwealths: "I declare under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

(2) If executed outside of the United States: "I declare under perjury or penalty under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

d. If an individual seeks access in person or electronically, identification will be verified by a Government-issued identification card. For example, driver's license, passport, permit, military ID, or government pass normally used for identification purposes.

e. If an individual wishes to have their records released directly to a third party or to be accompanied by a third party when seeking access to their records, reasonable proof of authorization must be obtained. A signed access authorization with a notarized signature is sufficient for granting the third party access.

6–3. Individual access to Army medical records

See AR 40–66 for information pertaining to Army medical records.

6–4. Personal notes

a. The PA does not apply to personal notes of individuals used as memory aids. These documents are not considered PA records. The five conditions for documents to be considered as personal notes of individuals used as memory aids are as follows:

(1) Maintained and discarded solely at the discretion of the author;

(2) Created only for the author's personal convenience and restricted to that of memory aids;

(3) Not the result of official direction or encouragement, whether oral or written;

(4) Not shown to others for any reason; and

(5) Not filed in agency files.

b. Any disclosure from personal notes, either intentional or unintentional, removes the information from the category of memory aids and the personal notes then become subject to provisions of the PA.

6–5. Relationship between Privacy Act and Freedom of Information Act

Not all requesters are knowledgeable of the appropriate statutory authority to cite when requesting records. In some instances, they may cite neither the PA nor the FOIA, but will imply one or both Acts. The guidelines below are provided to ensure that requesters are given the maximum amount of information as authorized under both statutes.

a. PA requests only compel disclosure of records from a SOR to the individuals to whom they pertain, or the legal guardian of an individual, or parents of a minor . Unlike FOIA, the PA applies only to U.S. citizens and aliens admitted into the U.S. for permanent residence.

b. Requesters seeking records about themselves contained only in a PA SOR will have their requests processed pursuant to the PA.

(1) If the PA SOR is exempt from the access provisions of Section (d)(1) of the PA, and if the records or any portion thereof are exempt pursuant to FOIA, the Army Activity will advise of the appropriate PA and FOIA exemption(s) in its response. Appeals will be processed in accordance with both the FOIA and PA.

(2) If the PA SOR is not exempt from the access provisions of Section (d)(1) of the PA, Army activities cannot claim a FOIA exemption on the information and must release all information to the first-party requester. However, the Department of the Army may withhold from such requester privacy-related information about another individual within the requester's PA file. When this is the case, the Army Activity will advise the first-party requester that information was withheld because "a portion of the record you requested contains privacy-related information about a party other than yourself."

c. Requester seeking records about themselves not in a PA SOR who cite or imply the PA will have their requests processed pursuant to the FOIA, since the PA does not apply to these records.

d. Requester seeking records about themselves in a PA SOR and outside a PA SOR will have their requests processed pursuant to both the PA and the FOIA.

e. Army activities will advise first-party requesters in the final response letter which PA and FOIA statutory authorities were used, inclusive of appeal rights.

6–6. Denial authorities

a. The only officials authorized to deny a request for records or a request to amend records in a PA SOR are the appropriate denial authorities, their designees, or the Secretary of the Army, acting through the GC.

b. Denial authorities are authorized to deny requests, either in whole or in part, for access and amendment of PA records contained in their respective areas of responsibility. The following denial procedures must be followed:

(1) The initial denial authority (IDA) may delegate all or part of their authority to an office chief or subordinate commander. All delegations must be in writing.

(2) The denial authority will send the names, office names, and telephone numbers of their delegates to the APCLO.

(3) If a denial authority delegate denies access or amendment, the delegate must clearly state that he or she is acting on behalf of the denial authority, who must be identified by name and position in the written response to the requester. Denial authority designation will not delay processing privacy requests/actions.

(4) The official denial authorities are for records under their authority. The individuals designated as denial authorities under this regulation are often the same individuals designated as IDAs under AR 25–55.

(5) The custodian of the record will acknowledge requests for access made under the provisions of the PA within 10 working days of receipt.

(6) The custodian will forward requests for information recommended for denial to the appropriate denial authority, along with a copy of the request, disputed records, and justification for withholding the information.

(7) Within 30 working days, the denial authority will provide the following notification to the requester in writing if the decision is to deny the requester access to the information:

(a) Denying official's name, position title, and business address.

(b) Date of the denial.

(c) Reasons for the denial, including citation of the appropriate subsections of the PA and this regulation.

(d) The individual's right to administratively appeal the denial within 60 calendar days of the mailing date of the notice, through the denial authority, to the Office of the General Counsel, Secretary of the Army, 104 Army Pentagon, Washington, DC 20310–0104.

(8) The appeal must be in writing and the requester should provide a copy of the denial letter and a statement of reasons for seeking review. For denials made by the DA when the record is maintained in a Government-wide SOR, an individual's request for further review must be addressed to each of the appropriate Government PA Act offices listed in the PA SOR notices. For a current listing of Government-wide PA SOR notices see the DPCLFD website at https://dpcld.defense.gov/privacy/sornsindex/governmentwidenotices.aspx.

(9) Denial is appropriate only if the record meets either of the following conditions:

(a) Was compiled in reasonable anticipation of a civil action or proceeding.

(b) Is exempted by the Secretary of the Army from the disclosure provisions of the PA, a legitimate governmental purpose for invoking the exemption exists, and the record is not required to be disclosed under the FOIA.

c. Once the GC issues a determination, the requester has the right to contest the decision within the U.S. District Court of the appropriate jurisdiction. The case is then forwarded to the Litigation Division, Office of the Judge Advocate General.

6–7. Fees

Requesters will be charged only for reproduction of requested documents. Normally, there will be no charge for the first copy of a record provided to an individual to whom the record pertains. Thereafter, fees will be computed as set forth in AR 25–55.

6–8. Use of contractors in Privacy Act and Freedom of Information Act administration

Pursuant to DoDI 1100.22, OMB Circular No. A–76, and Office of Federal Procurement Policy Letter 11–01, DoD Components may not use contract support for certain functions known as "inherently governmental activities" (such as, "governmental FOIA, Privacy and Civil Liberties functions").

a. Inherently governmental FOIA and PA functions include:

(1) Formulating or approving FOIA and Privacy policies and procedures.

(2) Making final determinations regarding whether to treat an incoming correspondence as a FOIA or PA request.

(3) Making denial or release determinations of information requested pursuant to the FOIA or PA.

(4) Deciding any issues regarding the scope or interpretation of a FOIA or PA request.

(5) Determining the appropriateness of claimed exemptions.

(6) Approving the approach taken in negotiations or discussions with a requester.

(7) Deciding administrative appeals.

(8) Conducting a final review of all outgoing final determination correspondence, memoranda, and release packages.

(9) Making final determinations on requests for expedited processing, fee category, and fee waivers.

(10) Executing documents for filing in litigation pursuant to the FOIA if the documents assert an official position of the DoD, any DoD Components, or any other federal agencies. Contractors may prepare and execute documents describing their own actions while processing requests.

b. Office of Federal Procurement Policy Letter 11–01 identifies the preparation of responses to requests as a function closely associated with inherently governmental functions. Examples of FOIA or PA functions and duties that contractors may perform in the preparation of responses to FOIA requests include, but are not limited to:

(1) Making redactions to documents under the direction of an IDA.

(2) Preparing correspondence for signature by a U.S. Government official.

(3) Communicating with a requester concerning the status of their request.

(4) Recommending information to be denied.

(5) Entering relevant information into the Army's FOIA tracking system.

Chapter 7
Disclosure of Personal Records to other Agencies and Third Parties

7–1. Disclosure to third parties

The PA limits the Army from disclosing a record from a SOR without obtaining the prior written consent of the individual, except when disclosure is—

a. Made to officers and employees of DoD who have a need for the record in the performance of their duties. For the purpose of disclosures and accounting of disclosures, DoD is considered a single agency, therefore, disclosures within Army activities and other DoD components are not considered third party requests, and the requirements for consent for disclosure and disclosure accounting do not apply.

b. Required under the Freedom of Information Act. The FOIA requires that records be made available to the public unless withholding is authorized pursuant to one of nine exemptions or one of three law enforcement exclusions under the Act. (See AR 25–55 for additional information.)

(1) Army activities must be in receipt of a FOIA request and a determination made that the records are not withholdable pursuant to a FOIA exemption or exclusion before records may be disclosed.

(2) Records that have traditionally been held to be in the public domain or which are required to be disclosed to the public, such as press releases, may be disclosed independent of a FOIA request.

c. Protected by Freedom of Information Act provisions. Personal privacy interests are protected by two provisions of the FOIA, exemptions 6 and 7(C). FOIA exemption 6 applies to most personal records, such as personnel, medical, and similar records. Exemption 7(C) applies to personal records compiled for law enforcement purposes, including personnel security investigation records. Both exemptions apply when disclosure of information would constitute a clearly unwarranted invasion of personal privacy.

(1) Disclosures of personal information regarding military and civilian employees should be made in accordance with the following considerations:

(a) Lists or compilations of unit or office address or telephone numbers are not released where the requester's primary purpose in seeking the information is to use it for commercial solicitation.

(b) Listings of personnel currently or recently assigned, details, or employed with the Army are not releasable if the disclosure of such a list would pose a privacy or security threat.

(c) Information regarding military or civilian personnel assigned, detailed, or employed by the National Security Agency, the Defense Intelligence Agency, the National Reconnaissance Office, or the National Geospatial Intelligence Agency, may only be disclosed as authorized by Public Law 86–36 (1959) and 10 USC 424. Personally identifying information regarding a member of the armed forces, and a civilian employee of the DoD or Coast Guard assigned, detailed, or employed by an overseas unit, a sensitive unit, or a routinely deployable unit can be withheld from disclosure under 10 USC 130b.

(2) Military personnel information that may be disclosed under the FOIA includes—

(a) Name.

(b) Rank.

(c) Date of rank.

(d) Gross salary.

(e) Past and present duty assignments.

(f) Future officially established assignments to units within the United States that are not sensitive or routinely deployable as defined in 10 USC 130b(c). (See also the glossary of this regulation. AR 25–22 glossary merely republishes the definitions that are codified in 10 USC 130b).

(g) Office/unit name, duty address, and telephone number.

(h) Source of commission, promotion sequence number, military awards and decorations, and military and civilian education.

(i) Duty status, at any given time.

(j) Separation or retirement dates.

(k) Biographies and photos of key personnel.

(3) Civilian employee information that may be disclosed under the FOIA includes—

(a) Name.

(b) Past and present position titles, occupational series, and grade.

(c) Past and present annual salary rates (including performance awards or bonuses, incentive awards, merit pay amount, Meritorious or Distinguished Executive Ranks, and allowances and differentials).

(d) Past and present duty stations.

(e) Office or duty telephone number.

(4) In addition to the disclosure of information regarding civilian employees, the following information may be made available to a prospective employer of a current or former Army employee:

(a) Tenure of employment.

(b) Civil service status.

(c) Length of service in the Army and the Government.

(d) Date and reason for separation shown on SF 50 (Notification of Personnel Action).

(5) Disclosure of personal information regarding Army civilian personnel must be made in accordance with OPM policies.

(6) Non appropriated funds employee personal information that may be disclosed under the FOIA includes—

(a) Name.

(b) Grade, date, or position.

(c) Gross salary.

(d) Past and present duty assignments.

(e) Future assignments, if officially established.

(7) Information permitted by a routine use that has been published in the FR:

(a) Made to the Bureau of the Census for planning or carrying out a census or survey, or to a related activity pursuant to 13 USC.

(b) Made to a recipient who has provided the Army with advance written assurance that the records will be—

1. Used solely as a statistical research or reporting record.

2. Transferred in a form that is not individually identifiable.

(c) Made to the National Archives of the United States as a record that has sufficient historical or other value to warrant its continued preservation by the U.S. Government, or for determination of such value by the GSA, or designee. (Records sent to Federal Records Centers for storage remain under Army control. These transfers are not disclosures and do not therefore need an accounting.)

(d) Made to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if—

1. The activity is authorized by law.

2. The head of the agency or instrumentality has made a written request to the Army element that maintains the record. The request must specify the particular portion desired and the law enforcement activity for which the record is sought.

(e) Made to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual. Upon such disclosure notification will be transmitted to the last known address of such individual.

(f) Made to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress, or subcommittee of any such joint committee.

(g) Made to the Comptroller General, or authorized representatives, in the course of the performance of the duties of the General Accountability Office.

(h) Pursuant to the order signed by a judge of a court of competent jurisdiction. (Reasonable efforts must be made to notify the subject individual if the legal process is a matter of public record.)

(i) Made to a consumer reporting agency under Section 3(d) of the Federal Claims Collection Act of 1966 (implemented by 49 CFR 89). The name, address, SSN, and other information identifying the individual; amount, status, and history of the claim; and the agency or program under which the case arose may be disclosed in this instance.

7–2. Disclosure accounting

a. An accounting of disclosure is required whenever a record from an Army SOR is disclosed to someone other than the subject individual, except when records are—

(1) Disclosed to DoD officials who have a ''need to know'' the information to perform official Government duties.

(2) Required to be disclosed under the FOIA.

b. Since the characteristics of records maintained within DA vary widely, no uniform method for keeping the disclosure accounting is prescribed.

c. Essential elements to include in each disclosure accounting report are—

(1) The name, position title, and address of the person making the disclosure.

(2) Description of the record disclosed.

(3) The date, method, and purpose of the disclosure.

(4) The name, position title, and address of the person or agency to which the disclosure was made.

d. The purpose for the accounting of disclosure is to—

(1) Enable an individual to ascertain those persons or agencies that have received information about them.

(2) Enable the DA to notify past recipients of subsequent amendments or ''Statements of Dispute'' concerning the record.

(3) Provide a record of DA compliance with the PA, if necessary.

e. When an individual requests such an accounting, the program manager or designee will respond within 20 workdays and inform the individual of the items above.

f. The only basis for not furnishing the subject individual an accounting of disclosures is if disclosure was made for law enforcement purposes under 5 USC 552a(b)(7), or the disclosure was from a SOR for which an exemption from 5 USC 552a(c)(3) has been claimed.

g. There are no approved filing procedures for the accounting of disclosure of records; however, ISEC owners must be able to retrieve them upon request. With this said, disclosure accountings should be kept in accordance with disposition instructions in ARIMS.

Chapter 8
Amending Records

8–1. Periodic review and amendment of records

a. Individuals are encouraged to periodically review the information maintained about them in PA SORs and to familiarize themselves with the amendment procedures established by this regulation.

b. An individual may request to amend records that are retrieved by his or her name or personal identifier from a SOR unless the system has been exempted from the amendment provisions of the Act. The standard for amendment is that the records are inaccurate as a matter of fact rather than judgment, irrelevant, untimely, or incomplete. The burden of proof is on the requester.

c. The program manager must review PA records for accuracy, relevance, timeliness, and completeness.

d. Amendment procedures are not intended to permit individuals to challenge events in records that have actually occurred. Amendment procedures only allow individuals to amend those items that are factually inaccurate and not matters of official judgment (for example, performance ratings, promotion potential, and job performance appraisals). In addition, an individual is not permitted to amend records for events that have been the subject of judicial or quasi-judicial actions and/or proceedings.

e. An amendment does not allow an individual to challenge the merits of an adverse action. However, if the record contains a misspelled name or an incorrect date of birth or SSN, the amendment procedures may be used to request correction of the record.

f. The U.S. Army Criminal Investigation Division (USACID) law enforcement reports have been exempted from the amendment provisions of the PA. Requests to amend these reports will be considered under AR 195–2 by the Director, USACID. Actions by the Director of USACID will constitute final action on behalf of the Secretary of the Army under that regulation.

g. Inspector General investigative files and action, request, and/or complaint files (records in system notice A0021–1 SAIG, Inspector General Records) have been exempted from the amendment provisions of the PA. Requests to amend these reports will be considered under AR 20–1 by the Inspector General (TIG). Action by TIG will constitute final action on behalf of the Secretary of the Army under that regulation.

h. Records placed in the National Archives are exempt from the PA provision allowing individuals to request amendment of records. Most provisions of the PA apply only to those SORs that are under the legal control of the originating agency; for example, an agency's current operating files or records stored at a Federal Records Center.

8–2. Amendment of records

Amendment procedures are as follows:

a. Requests to amend records should be addressed to the program manager of the records. The request must reasonably describe the records to be amended and the changes sought (for example, deletion, addition, or amendment). The burden of proof is on the requester.

b. The program manager or records custodian will provide the individual with a written acknowledgment of the request within 10 working days and will make a final response within 30 working days of the date the request was received. The acknowledgment must clearly identify the request and inform the individual that final action will be forthcoming within 30 working days.

c. Records for which amendment is sought must be reviewed by the proper program manager or custodian for accuracy, relevance, timeliness, and completeness to ensure fairness to the individual in any determination made about that individual on the basis of that record.

d. If the amendment is appropriate, the program manager or custodian will physically amend the records accordingly. The requester will be notified of such action.

e. If the amendment is not warranted, the request and all relevant documents, including reasons for not amending, will be forwarded to the proper denial authority within 10 working days to ensure that the 30-day time limit for the final response is met. In addition, the requester will be notified of the referral.

f. Based on the documentation provided, the denial authority will either amend the records and notify the requester and the custodian of the records of all actions taken, or deny the request. If the records are amended, those who have received the records in the past will receive notice of the amendment.

g. If the denial authority determines that the amendment is not warranted, he or she will provide the requester and the custodian of the records reason(s) for not amending. In addition, the denial authority will send the requester an explanation regarding his or her right to appeal the decision and the right to file a concise "Statement of Disagreement" to append to the individual's records.

h. Appeals of denial to amend a record received by an Army denial authority must be forwarded through the denial authority to the OGC. On receipt of an appeal, the denial authority will—

(1) Send the appeal to the OGC with a copy of the documents that are the subject of the appeal, the initial denial letter; and any other relevant material.

(2) Assist the GC as requested during his or her consideration of the appeal.

Chapter 9
Breach Reporting, Risk Assessment, Notification, and Mitigation

9–1. Breach reporting process

For the purpose of safeguarding against and responding to the breach of PII, the term "breach", the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for other than an authorized purpose (as defined by OMB Memorandum M–17–12). A breach occurs when it is suspected or confirmed. The SCOP is responsible for managing breaches for the Department of the Army with support from the APCLO. HQDA Principal Officials, ACOMs, ASCCs, and DRUs are responsible for reporting any actual or suspected compromises of PII within their activity. Army activities should report all incidents involving PII in physical or electronic form and should not distinguish between suspected and confirmed breaches. Reporting requirements are—

a. Report the details on suspected and actual PII breaches to the APCLO within 24 hours of breach discovery. This includes a breach in any medium or form, including paper, oral, and electronic by entering data into the Privacy Act Tracking System (PATS). PATS populates DD Form 2959 (Breach of Personally Identifiable Information (PII) Report) for processing.

b. When a breach warrants a report to law enforcement, the activities should ensure that the report occurs promptly, even if the breach is unconfirmed or the circumstances are unclear.

c. When a breach involves Government-authorized credit cards, the credit card holder must notify the issuing bank immediately upon discovering the breach.

d. The APCLO reports IT-related breaches to the Army's Security Operations Center, U.S. Army Cyber Command (ARCYBER). Headquarters, ARCYBER reports breaches to the U.S. Cyber Command, which in turn reports to U.S.-Computer Emergency Readiness Team and the OMB Office of the Federal CIO, as appropriate. The APCLO will continue to submit actual or suspected breaches and the appropriate details to the DPCLFD via the Compliance and Reporting Tool within 48 hours of discovery.

e. In accordance with Public Law 115–132, DoD will notify Congress of any significant loss of PII involving 250 or more civilian or uniformed members of the armed forces.

f. PHI, a subset of PII, is defined by the Health Insurance Portability and Accountability Act of 1996 and in DODM 6025.18. Additional guidance on breach reporting involving PHI is available at website https://www.hhs.gov/ocr/privacy/. When the breach includes an actual or suspected compromise of PHI, the APCLO will also report the incident to the Defense Health Agency Privacy and Civil Liberties Office within 24 hours of discovery.

g. Activities may have additional requirements for reporting breaches. Consult with your PCLO and follow your activity's guidance for reporting PII breaches.

h. Submit updates to the APCLO and the appropriate individual within your activity as additional information becomes available.

9–2. Risk assessment and notification determination

In order to properly escalate and tailor breach response activities, the SCOP, in coordination with the APCLO, will review all risk assessments. The Army activity reporting the breach must conduct and document a written assessment of the risk of harm to individuals potentially affected by a breach, including the factors the activity will consider when assessing the risk. When the breach involves a major incident or multiple DoD components, the SCOP and APCLO will engage in consultation with the SAOP and the Breach Response Team, as appropriate. When conducting an assessment, the Army activity should weigh the following determination factors to assess the breach.

a. Risk of harm to individuals. When assessing the risk of harm to individuals potentially affected by a breach, consider the potential harms that could result from the loss or compromise of PII. Such harms may include:

(1) Breach of confidentiality or fiduciary responsibility;

(2) Potential for blackmail;

(3) Disclosure of private facts;

(4) Mental pain and emotional distress;

(5) Financial harm;

(6) Disclosure of contact information for victims of abuse;

(7) Potential for secondary uses of the information that could result in fear or uncertainty; or

(8) Unwarranted exposure leading to humiliation or loss of self-esteem.

b. Risk of harm to the Government. Consider any and all risks relevant to the breach, which may include risks to the DoD, DoD information systems, DoD programs and operations, the Federal Government, or national security.

c. When conducting an assessment, Army activities should weigh the following determination factors to assess the likely risk of harm:

(1) *Nature and sensitivity of the personally identifiable information potentially compromised by the breach.* Include the actual and potential harms that an individual experiences or may experience from the compromise of the particular type of PII.

(2) *Likelihood of access to and use of personally identifiable information.* Include whether the PII was properly encrypted or rendered partially or completely inaccessible by other means.

(3) *Type of breach.* Include the circumstances of the breach, as well as the actors involved and their intent.

d. Nature and sensitivity of personally identifiable information. At a minimum, consider the following factors when assessing the nature and sensitivity of PII potentially compromised by a breach:

(1) *Data elements.* Analyze the sensitivity of each individual data element, as well as the sensitivity of all the data elements together.

(a) Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual because of their greater potential for misuse and harm to the individual. These data elements include, but are not limited to:

1. SSNs.
2. Passport numbers.
3. Driver's license numbers.
4. State identification numbers.
5. Bank account numbers.
6. Biometric identifiers.
7. Passwords.

(b) In addition to evaluating the sensitivity of each data element, be aware that the compromise of multiple data elements together may present an increased risk of harm to the individual when combined. For example, date of birth, place of birth, address, and gender may not be particularly sensitive alone, but when combined would pose a greater risk of harm to the individual.

(c) Also consider data that has been potentially compromised in previous breaches, as well as any other available information, public or agency-specific, that may increase the risk of harm to the individuals involved.

(2) *Context.*

(a) When assessing the nature and sensitivity of PII potentially compromised by a breach, consider the context. The context includes the purpose for which the PII was collected, maintained, and used.

(b) This assessment is critical because the same information in different contexts can reveal additional information about the impacted individuals. For example, a list of personnel and their associated office phone numbers may not be particularly sensitive. However, the same list of personnel and their associated office phone numbers on a list of personnel who hold sensitive positions within a DoD law enforcement agency or a group of routinely deployed DoD personnel is sensitive information. Similarly, the same list of names and associated phone numbers on a list of individuals along with information about a medical condition is also sensitive.

(3) *Private information.* Include the extent to which the PII, in a given context, may reveal particularly private information about an individual. Evaluate the extent to which the PII constitutes information an individual would generally keep private. Such private information may not present a risk of identity theft or other criminal conduct, but may pose a risk of harm such as embarrassment, blackmail, or emotional distress. Examples of private information include:

(a) Derogatory personnel or criminal information.

(b) Personal debt and finances.

(c) Medical conditions.

(d) Treatment for mental health.

(e) Pregnancy related information, including pregnancy termination.

(f) Sexual history or sexual orientation.

(g) Adoption or surrogacy information.

(h) Password.

(i) Immigration status.

(4) *Vulnerable populations.* Include the extent to which the PII identifies or disproportionately impacts a particularly vulnerable population. Consider whether the potentially affected individuals are from a particularly vulnerable population that may be at greater risk of harm than the general population. Potentially vulnerable populations include, but are not limited to:

(a) Children.

(b) Active duty military.

(c) Government officials in sensitive positions.

(d) Senior citizens.

(e) Individuals with disabilities.

(f) Confidential informants.

(g) Witnesses.

(h) Certain populations of immigrants.

(i) Non-English speakers.

(j) Victims of certain crimes such as sexual assault, identity theft, child abuse, trafficking, domestic violence, or stalking.

(5) *Permanence.* Include the continued relevance and utility of the PII over time and whether it is easily replaced or substituted. Consider the permanence of the PII. This includes an assessment of the relevancy and utility of the information over time and whether the information will permanently identify an individual. Some information loses its relevancy or utility as it ages.

(a) For example, an individual's health insurance identification number can be replaced. However, information about an individual's health, such as Family health history or chronic illness, may remain relevant for an individual's entire life, as well as for the lives of his or her Family.

(b) Special consideration is warranted when a breach involves biometric information including fingerprints, hand geometry, retina or iris scans, and deoxyribonucleic acid or other genetic information. When considering the nature and sensitivity of biometric information, factor in the known current uses of the information and consider that, with future advancements in science and technology, biometric information could have many additional uses not yet contemplated.

e. Likelihood of access to and use of personal identifiable information. Consider the following when assessing the likelihood of access to and use of PII potentially compromised by a breach.

(1) *Security safeguards.* Include whether the PII was properly encrypted or rendered partially or completely inaccessible by other means. When assessing the likelihood of access to and use of PII potentially compromised by a breach, the Army CIO will evaluate the implementation and effectiveness of security safeguards protecting the information. Security safeguards may significantly reduce the risk of harm to potentially affected individuals, even when the PII is particularly sensitive. The Army CIO will consider each of the employed security safeguards on a case-by-case basis and take into account whether the type, value, or sensitivity of the information might motivate a malicious actor to put time and resources towards overcoming those safeguards. For more information on security safeguards, see DoDM 5400.11, Volume 2, Section 8-2c(1).

(2) *Format and media.* The SCOP, in coordination with the Army CIO, will evaluate whether the format or media of the PII may make its use difficult, resource-intensive, and time consuming.

(a) The format of the PII or the media on which it is maintained may make the PII more susceptible to a crime of opportunity. For example, a spreadsheet on a portable universal serial bus flash drive does not require special skills or knowledge to access and an unauthorized user could quickly search for specific data fields. Conversely, magnetic tape

cartridge used for backing up servers that is 1 of a set of 30 and contains large amount of unstructured PII would require special expertise and equipment to access and use the information.

(b) The SCOP will also consider the type, value, or sensitivity of the PII. If the PII is particularly valuable, it may increase the likelihood of access and use regardless of its format or media. The value of information may outweigh the difficulty and resources needed to access the information for misuse.

(3) *Duration of exposure.* When assessing the likelihood of access and use of PII potentially compromised by a breach, consider the amount of time that the PII was exposed. PII that was exposed for an extended period of time is more likely to have been accessed or used by unauthorized persons.

(4) *Evidence of misuse.* When assessing the likelihood of access and use of PII potentially compromised by a breach, determine whether there is evidence of misuse. In some situations, it may be determined with a high degree of certainty that PII has been or is being misused. Evidence may indicate that identity theft has already occurred as a result of a specific breach or that PII is appearing in unauthorized external contexts. For example, law enforcement may confirm that PII is appearing on a website dedicated to the sale of stolen PII and may determine that there is strong evidence of misuse. Conversely, a forensic analysis of a recovered device may reveal that PII was not accessed.

f. Type of breach. Consider the following when determining the type of breach:

(1) *Intent.* When assessing the risk of harm to individuals potentially affected by a breach, consider whether the breach was intentional, unintentional, or whether the intent is unknown.

(a) If the breach was intentional, determine whether the information was the target, or whether the target was the device itself, like a mobile phone or laptop, and whether the compromise of the information was incidental. Examples of an intentional breach include theft of a device storing PII from a car or office, the unauthorized intrusion into a government network that maintains PII, or an employee looking up a celebrity's file in a Army database out of curiosity. While the risk of harm to individuals may often be lower when the information was not the target, the potential for a significant risk of harm to individuals may still exist.

(b) The risk of harm to individuals may be lower when a breach is unintentional, either by user error or sometimes by failure to follow Army policy. However, that is not always the case, and the SCOP must conduct a case-by-case assessment to determine the risk of harm. Examples of an unintentional breach include an employee accidentally emailing another individual's PII to the wrong email address or storing personnel files in a shared folder that was believed to be access-controlled but actually was not.

(c) In many circumstances, it may not be clear whether a breach was intentional or unintentional. For example, if an employee realizes their mobile device is missing, it may be that it was stolen intentionally or lost accidentally. Similarly, a shipment of files containing PII that never arrives at its destination may have been unintentionally lost or may have been targeted by a malicious actor and intercepted.

(2) *Recipient.* When assessing the risk of harm to individuals potentially affected by a breach, consider whether the PII was disclosed to a known or unknown recipient, and the trustworthiness of a known recipient. In some cases, the Army may know who received the compromised PII. This information, when available, may help the SCOP assess the likely risk of harm to individuals. For example, a breach is often reported by a recipient who receives information they should not have. This may be an indication of a low risk of harm to individuals, particularly when the recipient is another Army employee.

(a) One common type of low-risk breach is when an employee sends an individual's PII via email to another employee within the Army activity who does not have a need to know that PII for their duties. In many such cases it may be reasonable to conclude that there is negligible risk of harm. Even where PII is inadvertently sent to an individual outside the Army, the risk of harm may be minimal if it is confirmed that the individual is known to the Army, acknowledged receipt of the PII, did not forward or otherwise use the PII, and the PII was properly, completely, and permanently deleted by the recipient. This is a breach that must be reported and appropriately responded to, but the risk of harm is low enough that the response often does not necessitate that the Army activity notify or provide services to the individual whose PII was compromised.

(b) Conversely, if analysis reveals that the PII is under control of a group or person who is either untrustworthy or known to exploit compromised information, the risk of harm to the individual is considerably higher.

(c) In many cases there will be no information indicating that the compromised or lost PII was ever received or acquired by anyone. In such circumstances, the SCOP will rely upon other factors in this volume.

g. After evaluating each of these factors, activities should reassess the level of impact already assigned to the information using the impact levels defined by National Institute of Standards and Technology. The impact levels of low, moderate, and high describe the (worst case) potential impact on an organization or individual if a breach of security occurs. The levels of potential impact are—

(1) Low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example,

the loss of confidentiality, integrity, or availability might cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; result in minor damage to organizational assets; result in minor financial loss; or result in minor harm to individuals.

(2) Moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; result in significant damage to organizational assets; result in significant financial loss; or significant harm to individuals that does not involve loss of life or serious life threatening injuries.

(3) High if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; result in major damage to organizational assets; major financial loss; or result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

h. The impact levels will help determine if notification is warranted and how it should be provided. Where there is a range of risk levels attributed to the factors, the decision to provide notification should give greater weight to the likelihood the information is accessible and usable and whether the breach may lead to harm. The decision to notify should not be based on one factor alone. A final decision regarding whether to make notification cannot be made until all applicable harm and potential impact have been assessed.

i. Army activities should carefully evaluate the benefit of notifying the affected individual(s) of low or moderate impact breaches. Leaders should always remain cognizant of the effect that unnecessary notification may have on individuals. Notification, when there is little or no risk of harm, might create unnecessary concern and confusion.

9–3. Risk mitigation

a. General. Once the SCOP assesses the risk of harm to individuals potentially affected by a breach, he or she will consider, in coordination with the APCLO, how best to mitigate the identified risks. The SCOP will advise the Army's senior leadership on whether to take countermeasures, offer guidance, or provide services to individuals potentially affected by a breach. When the breach involves a major incident or involves multiple components, the SCOP and APCLO will engage in appropriate consultation with the SAOP and the DoD Breach Response Team, as appropriate.

b. Countermeasures, guidance, and services. Because each breach is fact-specific, the decision of whether to take countermeasures, offer guidance, or provide services to potentially affected individuals will depend on the circumstances of the breach.

(1) The SCOP will decide, in coordination with APCLO, whether to take countermeasures, offer guidance, or provide services to individuals potentially affected by a breach.

(2) The SCOP will determine and document the actions that the Army will take to mitigate the risk of harm to individuals potentially affected by a breach. These actions can include:

(a) Countermeasures. Countermeasures may not always prevent harm to potentially affected individuals, but may limit or reduce the risk of harm. For example, if credit card information is potentially compromised, the Army may proactively notify appropriate banks so they can monitor the associated accounts or reissue of the lines of credit using new accounts. Other countermeasures may also include expiring potentially compromised passwords or placing an alert in a database containing potentially compromised PII.

(b) Guidance. The type of guidance provided to mitigate the risk of harm to individuals will necessarily depend on the potentially compromised information. Use the information available at https://www.identitytheft.gov/info-lost-or-stolen as a baseline when drafting guidance.

1. There are several steps individuals can take to mitigate their own risk of harm resulting from a breach. These include:

a) Setting up fraud alerts or credit freezes.

b) Changing or closing accounts.

c) Taking advantage of services made available by the Federal Trade Commission (FTC).

2. The FTC provides specific guidance for when a breach involves SSNs, payment credit information, bank accounts, driver's licenses, children's information, and account credentials.

3. The Army may advise individuals to change passwords and encourage the use of multi-factor authentication for account access. When choosing guidance to mitigate the risk of harm, the SCOP should consider the guidance options included in OMB Memorandum M–17–12, Appendix II.

(c) Services. The SCOP will determine, in coordination with the APCLO, if there are services that are appropriate to provide to potentially affected individuals. Many of the services currently available in today's marketplace only mitigate risks of financial identity theft, and even the most comprehensive services are unable to eliminate the potential harms resulting from the evolving threat and risk landscape. The SCOP will identify those services that best mitigate the specific risk of harm resulting from the particular breach when selecting services.

1. If the SCOP determines, in coordination with the APCLO, that no service currently available appropriately mitigates a specific risk of harm, he or she may choose not to provide services to potentially affected individuals. Choosing not to provide services is a decision separate from the decision to provide notification and there may be circumstances where potentially affected individuals are notified but not provided services.

2. When choosing identity monitoring, credit monitoring, and other related services to mitigate the risk of harm to individuals potentially affected by a breach, the SCOP will take advantage of GSA blank purchase agreements (BPAs) in accordance with OMB Memorandum M–16–14. For details on the Identity Protection Services BPA (Identity Protection Services Special Item Number on the Multiple Awards Schedule), including task order instructions, offered services, authorized users, order dollar value limitation, the inclusion of DoD-specific terms, and ordering periods, visit https://www.gsa.gov/.

9–4. Notification

The SCOP is responsible, in coordination with APCLO, for advising Army senior leadership on whether and when to notify individuals potentially affected by a breach. The decision of whether to notify individuals depends on the specific circumstances of the breach and the assessed risk of harm conducted. The PCLOs should send a copy of the overall risk-of-harm findings and impact determination to the APCLO for review and consultation with the SCOP.

a. For breaches not determined to be major incidents, the SCOP is responsible, in conjunction with the APCLO, for making a decision regarding whether to provide notification.

b. When a breach constitutes a major incident, the SCOP will ensure that appropriate consultation with the SAOP and the Army Breach Response Team occurs in accordance with DoD Manual 5400.11, Volume 2. The SCOP may consider a delay in notifying individuals potentially affected by a breach if the notification would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions in accordance with OMB Memorandum M–17–12. Any recommendation to delay notification will be sent to the SAOP.

c. When the determination has been made that it is necessary to notify individuals potentially affected by a breach, the SCOP, in coordination with APCLO, will need to determine the source, timeliness, contents, and methods of notification. See DoD Manual 5400.11, Volume 2, Section 8.4 for details regarding notification.

9–5. Army Breach Response Team

The SCOP will designate an Army Breach Response Team ("Team") at the department level, to review, assess, and respond to breach of PII. The Team will meet annually for a Tabletop exercise and will convene as determined by the SCOP to assess whether a breach constitutes a major incident. In that regard, it will adhere to the following guidelines:

a. A breach constitutes a major incident when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. 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. Note: Unauthorized exfiltration is defined as the act or process of obtaining, without authorization or in excess of authorized access, information from an information system without modifying or deleting it.

b. Membership. The Team will include the SCOP, the SISO, APCLO, and representatives of the following offices: the Office of General Counsel, the Office of the Chief of Liaison, the Office of the Chief of Public Affairs, and TJAG. Other personnel, to include a representative from Army Inspector General and PCLOs, may be added to the Team as appropriate.

c. The SCOP will—

(1) Assess, in conjunction with the SISO, OGC and APCLO, whether a major incident breach has occurred. The assessment will be done in consultation with the Army activity where the incident occurred.

(2) Inform DoD of the agency's assessment as to a major incident.

(3) Ensure that the Office of the Provost Marshal General and office of TIG and OGC receive timely notification when notification is appropriate.

9–6. Completion of Privacy Act Tracking System submission

Submissions must be input according to the above-mentioned timelines and must include the following reportable information (see para 9–1):

a. Date of breach and date discovered.

b. Component Internal Tracking Number (if applicable).

c. Component and office name.

d. Point of contact information including name, duty phone, and office mailing address.

e. Narrative description of breach including—

(1) The parties involved in the breach.

(2) The media used such as email, info-sharing, paper records, or equipment.

(3) Type of breach: loss, theft, or compromise.

(4) Immediate steps taken to contain the breach.

f. Mitigating actions taken including—

(1) Whether the breach was intentional or inadvertent.

(2) Any lessons learned.

g. Number of individuals affected (including numbers of Soldiers, civilians, and contractors involved).

h. Type of PII compromised such as SSN, PHI, and financial information.

i. Any additional information as indicated on DD Form 2959.

j. Once DD Form 2959 is completed, the breach reporting individual should submit it as indicated above.

Chapter 10
Complaints and Judicial Sanctions

10–1. Privacy and civil liberties complaints process

a. Anyone may file a complaint alleging that some action by the Department of the Army or one of its members infringed on his or her privacy or civil liberties. Individuals may bring a complaint to the attention of the local Office of TIG, the local Office of the Staff Judge Advocate or supporting legal advisor, the local chaplain, or their command or supervisory chain, among others.

b. An assertion or complaint alleging a violation of privacy or civil liberties by the Army or an agent of the Army requires prompt attention. Personnel or organizations receiving a complaint will bring it to the attention of the command or supervisory chain and to the organization's privacy and civil liberties officer. If an Office of TIG receives a complaint, it will initiate an action pursuant to its prescribed policies and procedures. Commanders will initiate a preliminary inquiry upon receipt of information that a member of the command is accused or suspected of committing a privacy or civil liberties violation.

c. The PCLO assists complainants alleging civil liberties violations by referring them to an appropriate authority for assistance. For complainants alleging privacy violations, PCLOs will review allegations and evidence presented by the complainant. The PCLO will make an initial assessment as to the validity of the complaint and take appropriate corrective or mitigating action. The PCLO will coordinate with the Staff Judge Advocate to determine whether a more substantive investigation, such as a Commander's Inquiry or a 15–6 investigation's is appropriate.

d. Commanders and supervisors will report to the PCLO whether the inquiry or investigation of an allegation of a privacy or civil rights violation is pending or complete. For completed inquiries or investigations, commanders and supervisors will report whether the allegations were founded or unfounded; and, if founded, whether responsive action was taken. Except as authorized or required by law, commanders and supervisors will not release any PII that can be used on its own or when combined with other information to identify any individual named, consulted, or involved in the inquiry or investigation.

e. The decision at the local level may be appealed to the next higher command level PCLO. A legal review from the next higher level command PCLO's servicing Staff Judge Advocate is required prior to action on the appeal..

f. In accordance with 42 USC 2000ee–1, commanders and supervisors will prohibit reprisals or threats of reprisal against individuals who make complaints to DoD Privacy and Civil Liberties Program officials or the Privacy and Civil Liberties Oversight Board indicating a possible violation of privacy protections or civil liberties in the administration of Federal Government programs relating to efforts to protect the Nation from terrorism, unless the complaint was made or the information was disclosed with knowledge that it was false or with willful disregard for its truth or falsity. (See DoDI 5400.11).

g. The PCLO will submit a semi-annual summary of privacy and civil liberties complaints to the APCLO.

10–2. Violations of civil liberties

a. Improper government interference with the exercise of fundamental rights and freedoms violates the U.S. Constitution.

b. The Army has a compelling government interest in achieving its mission. For Soldiers and civilian employees, individual rights are balanced against applicable government interests. Some examples of situations where the government's interest may outweigh individual rights are:

(1) Prohibiting participation by Soldiers in formal or informal organizations or events that advocate violence as a legitimate means to overthrow the government or respond to regularly constituted government authority.

(2) Certain speech that violates the Uniform Code of Military Justice (UCMJ), such as verbal disrespect by a Soldier to a superior commissioned or noncommissioned officer(s), (UCMJ Art. 89 and Art. 91); and certain public speech by Soldiers that criticizes the President, the Vice President, Congress, the Secretary of Defense, the Secretary of a military department, the Secretary of Homeland Security, or the Governor or legislature of any State, Commonwealth, or possession (see UCMJ, Art. 88).

c. Individuals who believe their civil liberties have been violated should consult their civil liberties official for further guidance.

10–3. Judicial sanctions for privacy act and civil liberties violations

Violations of the provisions of the PA and of an individual's civil liberties have both civil remedies and criminal penalties.

a. Civil remedies. An individual may file a civil suit against DA if Army personnel fail to comply with the PA. In addition to specific remedial actions, 5 USC 552a(g) may provide for the payment of damages, court costs, and attorney's fees.

b. Criminal penalties. A member or employee of the Army may be found guilty of a misdemeanor and fined not more than $5,000 for—

(1) Willfully maintaining a SOR without first meeting the public notice requirements of publishing in the FR;

(2) Willfully disclosing information from a SOR, knowing that the disclosure is prohibited to one not entitled to receive it; or

(3) Knowingly and willfully requesting or obtaining any record concerning an individual from an agency under false pretenses.

Chapter 11
Training Requirements and Resources

11–1. Training requirements

The PA of 1974 5 USC 552a(e)(9), requires the Army to establish rules of conduct for all personnel involved in the design, development, operation, and maintenance of any PA SOR and to train the appropriate personnel with respect to the privacy rules, including the penalties for noncompliance. (See 5 USC 552a(e)(9)). All military, civilians, and contractors must complete Privacy and Civil Liberties training as identified below.

a. Annual. This course fulfills both the initial and annual privacy and civil liberties training requirements for military, civilians, and contractors. It provides a basic understanding of the Privacy Act, civil liberties, and this regulation as they apply to the individual's job performance and is a prerequisite to specialized training.

b. Specialized. This course is geared towards the application of this regulation to specialized areas of job performance for military, civilians and contractors. The list of personnel to whom this training applies includes but is not limited to personnel working in the following occupational series: human resources management; accounting and budget; medical, hospital, dental and public health; legal; information technology management; inspection, investigation, enforcement, and compliance; and anyone responsible for implementing or carrying out functions under this regulation. Specialized training is required within the first 90 days of assuming duties in a specialized area. Contact the PCLO for additional information.

11–2. Training records

a. The PCLOs will have access to Privacy and Civil Liberties training completion records in an electronic training system or training accountability tool (for example, sign-in rosters, spreadsheets). For Army contractors, the training record of completion will be retained by the appropriate office supported by the contract. Each trainee should retain a copy of privacy training completion documentation for their records.

b. The training record, demonstrating Privacy and Civil Liberties training completion, may be subject to inspection during reviews by the APCLO, the TIG of the DoD, or TIG. Additionally, each PCLO should be able to demonstrate training completion rates for each category of personnel.

c. Each Army activity should examine their training, and, if necessary, expand their training materials and program to include specific privacy and security awareness segments.

11–3. Training materials

The APCLO provides training materials on the ARMD website at https://www.rmda.army.mil/index.html. The materials include an online Privacy and Civil Liberties Initial/Annual Course and a Specialized Training Course, (Army Learning Management System), access to external related educational opportunities, and a link to the DPCLFD website at https://dpcld.defense.gov/privacy, which includes an assortment of privacy-related resources and publications.

Appendix A

References

Section I

Required Publications

Unless otherwise stated, all publications are available at https://armypubs.army.mil/. Department of Defense regulations are available at https://www.esd.whs.mil/. Public Laws, United States Codes, and Code of Federal Regulations are available at https://www.govinfo.gov/.

AR 10–87
Army Commands, Army Service Component Commands, and Direct Reporting Units (Cited in para 2–2.)

AR 20–1
Inspector General Activities and Procedures (Cited in para 8–1*g*.)

AR 25–1
Army Information Technology (Cited in para 1–11*a*(3).)

AR 25–2
Army Cybersecurity (Cited in terms.)

AR 25–55
The Department of the Army Freedom of Information Act Program (Cited in para 6–6*b*(4).)

AR 25–400–2
The Army Records Information Management System (ARIMS) (Cited in para 1–1*b*.)

AR 40–66
Medical Record Administration and Healthcare Documentation (Cited in para 6–3.)

AR 195–2
Criminal Investigation Activities (Cited in para 8–1*f*.)

DoD 5400.11–R
DoD Privacy Program (Cited in para 2–2*f*.)

DoDD 5200.27
Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense (Cited in para 1–10*b*.)

DoDI 1000.30
Reduction of Social Security Number (SSN) Use Within DoD (Cited in para 2–2*g*(3).)

DoDI 5400.11
DoD Privacy and Civil Liberties Programs (Cited in the title page.)

DoDI 5400.16
DoD Privacy Impact Assessment (PIA) Guidance (Cited in para 2–2*c*(7).)

DoDM 5400.11, Volume 2
DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan (Cited in para 1–8*a*.)

DoDM 6025.18
Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Program (Cited in para 1–7*g*.)

EO 13478
Amendments To Executive Order 9397 Relating To Federal Agency Use of Social Security Numbers (Cited in para 5–3*a*.)

FAR, Subpart 24.1
Acquisition of Utility Services (Cited in para 1–7*a*.)

OMB Circular A–108
Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act (Cited in para 2–1*c*.)

OMB Memorandum M–16–14
Category Management Policy 16–2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response (Cited in para 9–3*b*(2)(*c*)2.)

OMB Memorandum M–17–09
Management of Federal High Value Assets (Cited in para 2–2*c*(4).)

OMB Memorandum M–21–02
Fiscal Year 2020–2021 Guidance on Information Security and Privacy Management Requirements (Cited in para 9–5*a*.)

10 USC 130b
Personnel in overseas, sensitive, or routinely deployable units: nondisclosure of personally identifiable information (Cited in para 7–1*c*(1)(*c*).)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read the publication to understand this regulation. The FAR is available at https://www.acquisition.gov/far/. EOs are available at https://www.archives.gov/federal-register/executive-orders/disposition.html/. OMB guidance is available at https://www.whitehouse.gov/. Public Laws, United States Codes, and Code of Federal Regulations are available at https://www.gpo.gov/fdsys/search/home.action. UCMJ is available at https://jsc.defense.gov/.

AR 11–2
Managers' Internal Control Program

AR 15–6
Procedures for Administrative Investigations and Boards of Officers

AR 25–30
Army Publishing Program

AR 27–10
Military Justice

AR 27–40
Litigation

AR 36–2
Audit Services in the Department of the Army

AR 190–45
Law Enforcement Reporting

AR 215–8/AFI 34–211(I)
Army and Air Force Exchange Service Operations

AR 380–5
Army Information Security Program

AR 600–37
Unfavorable Information

AR 630–10
Absence Without Leave, Desertion, and Administration of Personnel Involved in Civilian Court Proceedings

AR 633–30
Military Sentences to Confinement

DA Pam 25–403
Guide to Recordkeeping in the Army

DoDD 5105.53
Director of Administration and Management (DA&M)

DoDD 5400.07
DoD Freedom of Information Act (FOIA) Program

DoDI 1332.28
Discharge Review Board (DRB) Procedures and Standards

DoDI 5200.48
Controlled Unclassified Information (CUI)

DoDI 5400.04
Provision of Information to Congress

DoDI 7650.01
Government Accountability Office (GAO) and Comptroller General Requests for Access to Records

DoDI 8170.01
Online Information Management and Electronic Messaging

DoDI 8500.01
Cybersecurity

DoDI 8910.01
Information Collection and Reporting

DoDM 5200.01–V1
DoD Information Security Program: Overview, Classification, and Declassification

DoDM 5400.07
DoD Freedom of Information Act (FOIA) Program

DoDM 7750.08
DoD Forms Management Program Procedures

EO 9397
Numbering System for Federal Accounts Relating to Individual Persons

EO 11652
Classification and Declassification of National Security Information and Material

EO 12333
United States Intelligence Activities

EO 12356
National Security Information

EO 13388
Further Strengthening the Sharing of Terrorism Information to Protect Americans

EO 13402
Strengthening Federal Efforts to Protect Against Identity Theft

Federal Register, Volume 40
Office of Management and Budget, Privacy Act Implementation (Available at https://www.federalregister.gov/.)

Federal Register, Volume 54
Final Guidance Interpreting the Provisions of Public Law 100–503, the Computer Matching and Privacy Protection Act of 1988 (Cited in para

FIPS Publication 199
Standards for Security Categorization of Federal Information and Information Systems (Available at https://csrc.nist.gov/.)

OMB Circular A–19
Legislative Coordination and Clearance

OMB Circular A–130
Transmittal Memorandum No. 4: Managing Information as a Strategic Resource

OMB Memorandum 10–23
Guidance for Agency Use of Third-Party Websites and Applications

OMB Memorandum M–05–08
Designation of Senior Agency Officials for Privacy

OMB Memorandum M–17–12
Preparing for and Responding to a Breach of Personally Identifiable Information

OMB Memorandum M–19–03
Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program

PL 100–503
Computer Matching and Privacy Protection Act of 1988

PL 105–318
Identity Theft and Assumption Deterrence Act of 1998

PL 107–347, Section 208
E-Government Act of 2002, Privacy Provisions

PL 108–458, As Amended Through PL 113–293
Intelligence Reform and Terrorism Prevention Act of 2004

PL 110–53
Implementing Recommendations of the 9/11 Commission Act of 2007

PL 115–232
John S. McCain National Defense Authorization Act for Fiscal Year 2019

Treasury Fiscal Requirements Manual, Bulletin No. 76–07
Department of the Treasury Fiscal Requirements Manual (Available at https://tfm.fiscal.treasury.gov/)

UCMJ, Art. 88
Contempt toward officials

UCMJ, Art. 89
Disrespect toward superior commissioned officer; assault of superior commissioned office

UCMJ, Art. 91
Insubordinate conduct toward warrant officer, noncommissioned officer, or petty officer

UCMJ, Art. 92
Failure to obey order or regulation

5 CFR 293
Personnel Records

5 CFR 294
Availability of Official Information

5 CFR 297
Privacy Procedures for Personnel Records

5 CFR 310
Employment of Relatives

16 CFR Part 681
Identify Theft Rules

32 CFR 310
Protection of Privacy and Access to Amendment of Individual Records under the Privacy Act of 1974

48 CFR 24
Protection of Privacy and Freedom of Information

49 CFR 89
Implementation of the Federal Claims Collection Act

5 USC 552
Public information; agency rules, opinions, orders, records, and proceedings

5 USC 552a
Records maintained on individuals

5 USC 1205
Transmittal of information to Congress

5 USC 1206
Annual report

5 USC 2302
Prohibited personnel practices

6 USC 482
Facilitating homeland security information sharing procedures

6 USC 485
Information sharing

10 USC 424
Disclosure of organizational and personnel information: exemption for specified intelligence agencies

10 USC 1034
Protected communications; prohibition of retaliatory personnel actions

10 USC 1553
Review of discharge or dismissal

10 USC 1587
Employees of nonappropriated fund instrumentalities: reprisals

10 USC 7013
Secretary of the Army

13 USC
Census Bureau

13 USC 8
Authenticated transcripts or copies of certain returns; other data; restriction on use; disposition of fees received

18 USC 3056
Powers, authorities, and duties of United States Secret Service

28 USC 1746
Unsworn declarations under penalty of perjury

42 USC
The Public Health and Welfare

42 USC 2000ee–1
Privacy and civil liberties officers

44 USC Chapter 33
Disposal of Records

44 USC 3102
Establishment of program of management

44 USC 3506
Federal agency responsibilities

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website https://armypubs.army.mil; DD forms are available on the DoD website https://www.edsd.whs.mil/directives/forms/, and https://www.gsa.gov. Standard Forms are available on the U.S. Office of Personnel Management website https://www.opm.gov/forms/standard-forms/.

DA Form 11–2
Internal Control Evaluation Certification

DA Form 2028
Recommended Changes to Publications and Blank Forms

DD Form 2930
Privacy Impact Assessment (PIA)

DD Form 2959
Breach of Personally Identifiable Information (PII) Report

DD Form 2984
Component Privacy and Civil Liberties Report (42 USC 2000ee-1)

SF 901
CUI Cover Sheet

Appendix B

Privacy Act Statement

B–1. Usage

Provide a PAS to individuals when information is collected that will be maintained in a PA SOR, regardless of the medium used to collect the information (for example, forms, personal interviews, telephonic interviews, and other methods). Also provide a PAS when individuals are asked to confirm that their data is current and correct.

B–2. Elements

The elements of a PAS include AUTHORITY, PRINCIPAL PURPOSE, ROUTINE USES, and DISCLOSURE. Figure B–1 describes each element.

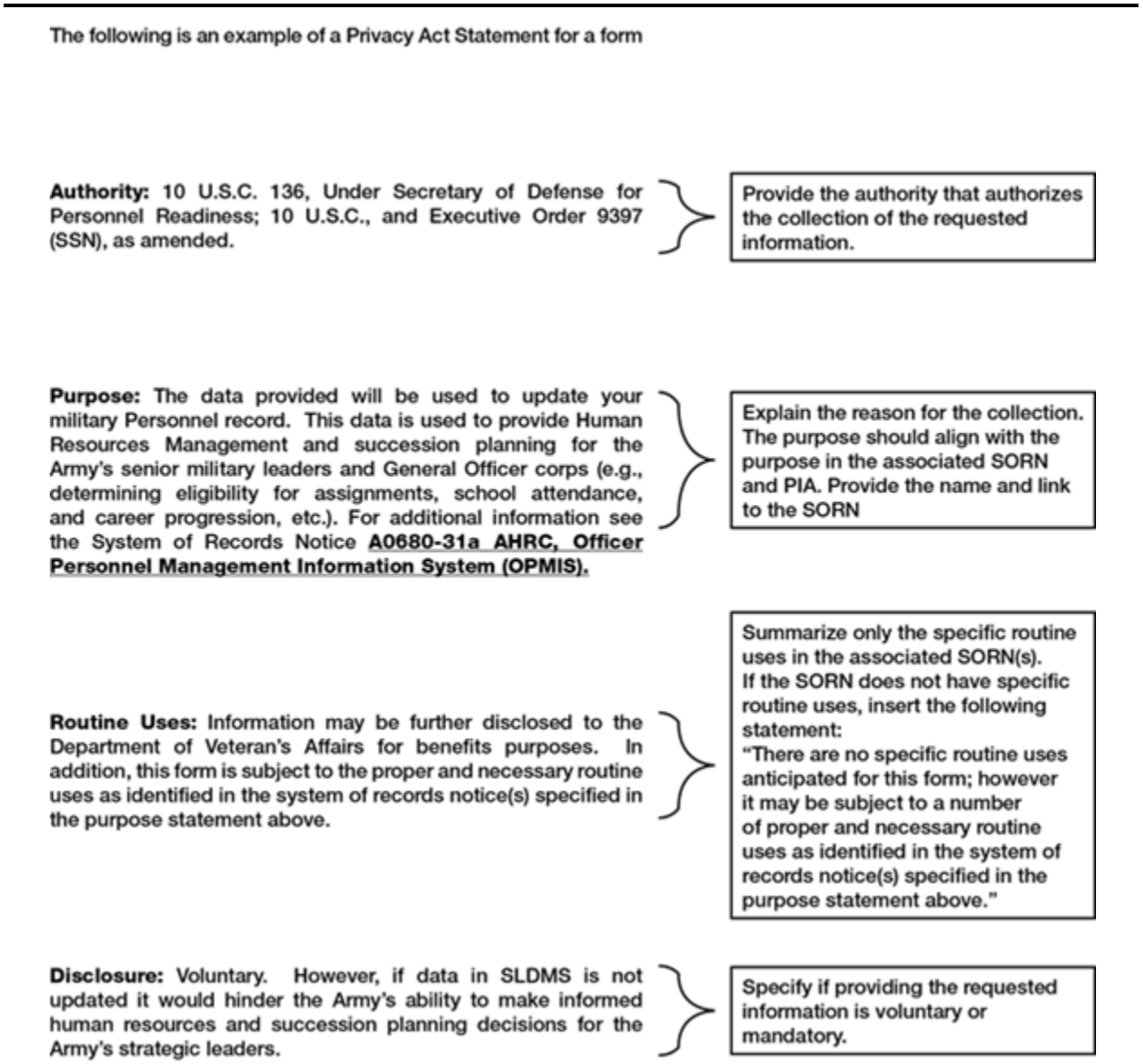

Figure B–1. Privacy Act Statement Structure

Appendix C

Internal Control Evaluation

C–1. Function
The function covered by this evaluation is the Army Privacy and Civil Liberties Program.

C–2. Purpose
The purpose of this evaluation is to assist users of AR 25–22 in evaluating the key internal controls listed. It is not intended to cover all controls.

C–3. Instructions
Answers must be based on the actual testing of key internal controls (for example, document analysis, direct observation, sampling, and simulation). Answers that indicate deficiencies must be explained and the corrective action identified in supporting documentation. These internal controls must be evaluated at least once every five years. Certification that the evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification).

C–4. Test questions
a. Is a Privacy and Civil Liberties Program established and implemented in your organization?
b. Is an individual(s) appointed to implement the privacy and civil liberties requirements?
c. Are appointed privacy and civil liberties officers providing annual privacy and civil liberties training tailored to their organization requirement?

C–5. Supersession
This evaluation replaces the previously published evaluation, dated 22 December 2016.

C–6. Comments
Help make this a better tool for evaluating internal controls. Submit comments to the Army Privacy and Civil Liberties Officer via the email address specified at usarmy.belvoir.hqda-oaa-ahs.mbx.rmda-foia-privacy-alert@mail.mil or via U.S. Mail to the Army Records Management Directorate, 9301 Chapek Rd, Building 1458, Fort Belvoir, VA 22060–5605.

Glossary

Section I

Abbreviations

AAFES
Army and Air Force Exchange Service

AASA
Administrative Assistant to the Secretary of the Army

ACOM
Army command

AFI
Air Force Instruction

APCLO
Army Privacy and Civil Liberties Officer

ARCYBER
U.S. Army Cyber Command

ARIMS
Army Records Information Management System

ARMD
Army Records Management Directorate

ASA (M&RA)
Assistant to the Secretary of the Army (Manpower and Reserve Affairs)

ASCC
Army service component command

BPA
blanket purchase agreement

CFR
Code of Federal Regulations

CIO
Chief Information Officer

CLL
Chief Legislative Liaison

CPA
Chief of Public Affairs

CUI
controlled unclassified information

DA
Department of the Army

DCS, G–6
Deputy Chief of Staff, G–6

DFAR
Defense Federal Acquisition Regulation

DoDD
Defense of Defense Directive

DoDI
Department of Defense Instruction

DoDM
Department of Defense Manual

DPCLFD
Defense Privacy, Civil Liberties, and FOIA Directorate

DRU
direct reporting unit

EO
Executive Order

FAR
Federal Acquisition Regulation

FIPP
fair information practice principle

FISMA
Federal Information Security Management Act

FOIA
Freedom of Information Act

FR
Federal Register

FTC
Federal Trade Commission

GC
General Counsel

GSA
General Services Administration

HIPAA
Health Insurance Portability and Accountability Act

HQDA
Headquarters, Department of the Army

HVAs
high-value assets

ID
identification

IDA
initial denial authority

ISEC
Information system or electronic collection

IT
Information Technology

OGC
Office of the General Counsel

OMB
Office of Management and Budget

OPM
Office of Personnel Management

PA
Privacy Act

PAA
Privacy Act Advisory

PAS
Privacy Act Statement

PATS
Privacy Act Tracking System

PCLO
Privacy and Civil Liberties Officer

PHI
protected health information

PIA
privacy impact assessment

PII
personally identifiable information

RRS–A
records retention schedule–Army

SAOP
Senior Agency Official for Privacy

SCOP
Senior Component Official for Privacy

SF
Standard Form

SISO
Senior Information Security Officer

SOR
system of records

SORN
system of record notice

SSN
Social Security number

TIG
The Inspector General

TJAG
The Judge Advocate General

UCMJ
Uniform Code of Military Justice

USACID
U.S. Army Criminal Investigation Division

USC
United States Code

Section II

Terms

Access
A transfer of a record, a copy of a record, or the information in a record to the subject individual, or the review of a record by the subject individual.

Agency
Any executive department, military department, Government corporation, Government-controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.

Amendment
For the purposes of Army personnel records only, amendment means the correction, addition, deletion, or destruction of a records or specific portions of a record (see 5 CFR 297.102).

Army Records Information Management System
A system for identifying, arranging, and retrieving Army records for reference and disposition according to the directive, usually an AR or DA Pam, which prescribes their creation, maintenance, and use.

Breach
The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other-than-authorized purpose.

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

Computer matching agreement
A written agreement between a recipient agency and a source agency (or a non-Federal agency) that is required by the PA for parties engaging in a matching program.

Cookie
A cookie is a mechanism that allows the server to store its own information about a user on the user's own computer. Cookies are embedded in the hypertext markup language information flowing back and forth between the user's computer and the servers. They allow user-side customization of web information. Cookies normally expire after a single session.

Copy
A reproduction or duplication of an original record. Copies identified by their function include action copy, comeback copy, file or record copy, information or reference copy, official copy, and stayback copy. Copies identified by method of creation include carbon, ribbon, electronic, electrostatic, mimeograph, offset, press, diazo, and vesicular.

Defense Data Integrity Board
Composed of full-time or permanent part-time government employees or military Servicemembers and includes the Military Department SCOPs. The board reviews, approves, and maintains all written agreements for receiving or disclosing DoD records for matching programs to ensure compliance with the PA of 1974, as amended, and all relevant statutes, regulations, and guidelines (see DoDI 5400.11).

Department of Defense contractor
Any person or other legal entity that directly or indirectly (for example, through an affiliate) is awarded a government contract. This may include a contract for carriage under government or commercial bills of lading, or a subcontract under a government contract. A DoD contractor includes a contractor who conducts business with the Federal Government as an agent or representative of another contractor.

Disclosure
The information sharing or transfer of any PII from a SOR by any means of communication (such as oral, written, electronic, or other) to any person, entity, or forum, other than the subject of the record, the subject's designated agent, or the subject's legal guardian.

Identifiable form
Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Identity theft
A fraud committed or attempted using the identifying information of another person without authority (see 16 CFR Part 681).

Incident
An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Individual
A citizen of the United States or an alien lawfully admitted for permanent residence.

Maintain
For the purpose of the PA of 1974, the term "maintain" includes maintain, collect, use, or disseminate.

Major incident
A major incident is either: an incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people; or, a breach that involves 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 United States, or to the public confidence, civil liberties, or public health and safety of the American people. A major incident determination is required for any unauthorized modification of, unauthorized deletion of, or unauthorized access to the PII of 100,000 or more people.

Minor children
Unmarried children under 18 years of age who are not on active duty with the Armed Forces.

Personally identifiable information
Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Privacy Act Statement
A document that explains why the Army is collecting personal information, the purpose of the collection, and the consequences of not providing the requested information. A PAS is required when the collected personal information (name, date of birth, SSN, and so forth) will be entered into an Army SOR. This applies to all collection methods including forms, as well as personal and telephonic interviews.

Privacy impact assessment
An analysis of how personal information is handled to: (a) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (b) determine the risks and effects of collecting, maintaining, and disclosing personal information; and (c) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. The PIA process provides a way to ensure compliance with laws and regulations governing privacy.

Protected health information
Individually identifiable health information (as defined by the HIPAA Privacy Rule) that, except as provided by DoDI 6025.18, is transmitted or maintained by electronic or any other form or medium. PHI excludes individually identifiable health information in employment records held by a covered DoD entity in its role as employer. Information that has been de-identified in accordance with the HIPAA Privacy Rule is not PHI.

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

Records management
The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and economical management of agency operations.

Reprisal
The taking of (or threatening to take) an unfavorable personnel action or the withholding (or threatening to withhold) a favorable personnel action because the member made (or was thought to have made) a protected communication.

Risk assessment
The process to identify, assess, and control risks and make decisions that balance risk with mission benefits.

Routine use
Disclosure of a record for a use that is compatible with the purpose for which the record was collected.

Routinely deployable unit
A unit that normally deploys from its permanent home station on a periodic or rotating basis to meet peacetime operational requirements that, or to participate in scheduled training exercises that, routinely require deployments outside the United States and its territories. Such term includes a unit that is alerted for deployment outside the United States and its territories during an actual execution of a contingency plan or in support of a crisis operation (see 10 USC 130b).

Sensitive unit
A unit that is primarily involved in training for the conduct of, or conducting, special activities or classified missions, including a unit involved in collecting, handling, disposing of, or storing if classified information and materials; a unit engaged in training special operations units, security group commands weapons stations, and any other unit that is designated as a sensitive unit by the Secretary of Defense or, in the case of the Coast Guard when it is not operating as a service in the Navy, by the Secretary of Homeland Security (see 10 USC 130b).

Statistical record
A record in a SOR maintained for statistical research or reporting purposes only and not used in whole or in part in making determinations about an identifiable individual.

System manager
A system manager is responsible for development, production, and sustainment of a capability that meets user operational needs, and functions as the focal point for the integration of cybersecurity into and throughout the system life cycle (see AR 25–2).

System of records
A group of any records under the control of the DA from which information is retrieved by the name of the individual or by an identifying number, symbol, or other identifying particular assigned to the individual.

System of records notice
The notice published by the Army in the FR upon establishment and/or modification of a systems of records describing the existence and character of the system. A SORN identifies the SOR, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained, the routine uses to which the records are subject (see OMB Circular No. A–108).

Website
A location on the Internet; specifically it refers to the point of presence location in which it resides. All websites are referenced using a special addressing scheme called a uniform resource locator. A website can mean a single hypertext markup language file or hundreds of files placed on the Internet by an enterprise.