DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

JUN 10 2013

DISA INSTRUCTION 210-225-2*

INFORMATION SERVICES

Privacy Program

1. **Purpose**. This Instruction prescribes policy, assigns responsibilities, and provides procedures for the Privacy Program for DISA. It also includes guidance on individual access to Privacy Act information, protection of personally identifiable information (PII), and safeguarding against and responding to the breach of PII.

2. **Applicability.** This Instruction applies to all DISA activities.

3. **Scope**. This Instruction applies to information and records (including all media formats) accessed and created by DISA civilian, military, and contractor personnel.

4. **Authority.** This Instruction is published in accordance with the authority contained in DoD Directive 5400.11, Department of Defense Privacy Program, 8 May 2007; DoD Regulation 5400.11-R, Department of Defense Privacy Program, 14 May 2007; DoD Instruction 5400.16, DoD Privacy Impact Assessment (PIA) Guidance, 12 February 2009; and Office of the Secretary of Defense (OSD) Office of Administration and Management (OA&M) Department of Defense (DoD) Senior Privacy Official Memorandum, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII), 5 June 2009.

5. **Definitions.** Definitions are provided in enclosure 1.

6. **Policy.** To comply with 5 U.S.C. §552a, Privacy Act of 1974, as amended, DISA will:

6.1 Preserve the personal privacy of individuals and maintain within its records system only information about an individual which is relevant and necessary to comply with a Federal statute; Executive Order of the President; or other applicable

Directives, Regulations, and/or Instructions. Ensure the information is relevant, timely, complete, and accurate for its intended use.

6.2 Collect information about an individual, to the greatest extent practicable, directly from the individual, when the information may result in adverse determinations about the individual's rights, benefits, or privileges. Inform the individual why the information is being collected, the authority for the collection, what uses will be made of the information, whether disclosure is mandatory or voluntary, and the consequences of not providing that information.

6.3 Ensure records are not maintained that describe how individuals exercise their rights guaranteed by the First Amendment to the Constitution of the United States, unless expressly authorized by statute, or by the individual about whom the record is maintained, and unless pertinent to, and within the scope of, an authorized law enforcement activity.

6.4 Ensure records contained in a system of record are not disclosed to anyone other than those who require the records for official purposes, in conformance with the routine uses for such records, as published in the Federal Register in a system of records notice (SORN).

6.5 Allow individuals to know what existing Agency records pertain to them, with the exception of those identified in paragraph 8. Provide access to or copies of all or any portions of such records to individuals, upon request, to make corrections or amendments. (Guidance on individual access to Privacy Act information is provided in enclosure 2.)

6.6 Protect from unauthorized disclosure any personal information contained in any system of records. (Appendix 3, DoD Blanket Routine Uses, to DoD 5400.11-R [authority document], applies to all DISA systems of records, unless specifically excluded in a SORN.)

6.7 Ensure a SORN has been published in the Federal Register before maintaining files and listings that contain information about individuals. Verify the applicable SORN is retrievable by name or other personal identifier.

6.8 Report any unauthorized disclosures of personal information from a system of records or the maintenance of any system of records to the appropriate Privacy Official.

6.9 Ensure computer matching programs and Privacy Protection Act data shared among the Federal Government agencies will benefit one of the agencies by disclosing an individual has received benefits in excess of those they may be entitled to obtain, as required of section 552a of 5 U.S.C., Privacy Act of 1974, as amended; Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Requirements; and DoD 5400.11-R (authority document).

6.10 Ensure all e-mail that contains PII is digitally signed and encrypted. (The body of the e-mail, including any e-mail attachments containing PII, must be properly marked (e.g., "FOR OFFICIAL USE ONLY (FOUO)." Any misuse or unauthorized disclosure may result in both civil and criminal penalties. The e-mail must only be sent to those recipients that have an official need-to-know.)

6.11 Ensure all PII stored on the DoD Enterprise Portal Services (DEPS) (hereafter referred to as the "enterprise portal" is safeguarded with proper security mechanisms to protect from unauthorized access, alteration, or disclosure and that confidentiality is preserved and protected. (PII shall be nondiscoverable to unauthorized users, and access to PII shall be based on appropriate need-to-know and data-owner approval.)

7. **Privacy Standards of Conduct.** Standards of conduct to be observed whenever using or having access to information of a personal nature or pertaining to a particular individual or individuals are as follows:

7.1 Personal information about any individual whether in a system of records or not is to be safeguarded and protected so that the security and confidentiality of the information is preserved and limited to official uses.

7.2 Disclosure of personal information contained in any system of records is to be prevented, except as authorized by Section 32 CFR part 310 (DoD Privacy Program) or other applicable law or regulation. (Personnel willfully making such a disclosure knowing the disclosure is prohibited are subject to possible criminal penalties and/or administrative sanctions.)

7.3 Unauthorized disclosure of personal information from a system of records or the maintenance of any system of records that is not authorized by this Instruction is to be reported to the DISA Privacy Officer.

8. **Exemptions Applying to Certain Privacy Act Records.**

8.1 Individual access to record content is to be denied in the following circumstances:

8.1.1 Properly classified national security information under section (k)(1) of 5 U.S.C. §552a to the extent that the system contains any information properly classified under E.O. 13526.

8.1.2 Information compiled or maintained in reasonable anticipation of civil actions or proceedings under 5 U.S.C. §552a (d)(5). (Requests for pending investigations will be denied and the requester instructed to forward another request allowing adequate time for the investigation to be completed.)

8.1.3 Information compiled for investigation of criminal offenses per 5 U.S.C. §552a (j)(2) and (k)(2). (Other exemptions relating to background checks and employment suitability are also found in 5 U.S.C. §552a (k).)

8.2 The types of information that shall be exempt from disclosure are those which would compromise the identity of confidential sources; alert subjects of an investigation of an actual or potential criminal or civil violation to the investigation; endanger the physical safety of witnesses, informants, and law enforcement personnel; violate the privacy of third parties; and those which would otherwise impede effective law enforcement. Information exempt from disclosure will be redacted from the requested documents and the balance made available, whenever possible.

9. **Remedies That May Be Invoked by an Individual Claiming Violation of Privacy Act Rights.** Provisions of the Privacy Act that may be invoked to effect relief when an individual claims the Agency or its employees have violated his or her privacy rights are when an individual is permitted to seek relief through appropriate administrative channels or when an individual may file a civil suit. (See 5 U.S.C. §552a (g)). In addition to specific remedial actions, the Privacy Act provides for the payment of damages, court costs, and attorney fees in some cases.

10. **Criminal Penalties.** The Privacy Act of 1974 also provides for criminal penalties. (See 5 U.S.C. §552a (i)(1).)

10.1 Any official or employee who by virtue of his or her employment or official position has possession of, or access to,

an agency system of records which contains individually identifiable information, knowing that dissemination is prohibited, willfully provides data from a Privacy Act protected record to anyone not entitled to receive the information, may be found guilty of a misdemeanor and fined not more than $5,000.

10.1.2 Any official or employee who willfully maintains a system of records without publishing the required public notices in the Federal Register may be found guilty of a misdemeanor and fined not more than $5,000.

10.1.3 Any individual who knowingly and willfully requests or obtains any record concerning another individual under false pretenses may be found guilty of a misdemeanor and fined up to $5,000.

11. **Responsibilities.**

11.1 **Chief Information Officer (CIO).** The CIO will:

11.1.1 Direct and administer the DISA Privacy Program.

11.1.2 Serve as the Agency principal point of contact for administrative Privacy Act matters.

11.1.3 Ensure an internal Agency Privacy Program is maintained and all echelons effectively comply with this Instruction.

11.1.4 Coordinate with Agency senior management in response to a breach of PII.

11.1.5 Publish, as necessary, internal Privacy Act procedures that are consistent with DoD Directive 5400.11, Department of Defense Privacy Program, and DoD 5400.11-R, Department of Defense Privacy Program (authority documents).

11.1.6 Provide policy guidance to system managers for processing internal Privacy Act requests.

11.1.7 Prepare Privacy Act reports for DoD and other authorities, as required.

11.1.8 Prepare required Privacy Act SORNs and amendments for submission to the Federal Register. (Subparagraph 14.1 provides additional details.)

11.1.9 Assign a trained individual as the Privacy Officer to carry out the administrative management responsibility of the Privacy Program on behalf of the CIO.

11.2 **Chief of Staff (COS).** The COS, as the Privacy Act Appeal Authority, will dictate internal appeal procedures.

11.3 **General Counsel (GC).** The GC will:

11.3.1 Serve as the DISA principal point of contact for legal and litigation matters related to the Privacy Act.

11.3.2 Be the final authority within DISA on all legal opinions regarding the Privacy Act or its implementation.

11.3.3 Render legal opinions to the CIO, the Privacy Act Appeal Authority, and other DISA elements, as appropriate.

11.3.4 Provide legal support and guidance in responding to a suspected or actual breach.

11.3.5 Review all Privacy Act request denials to ensure uniformity and consistency in legal positions and interpretations rendered.

11.3.6 Review all Privacy Act notices and amendments prior to submission to the Defense Privacy Office for publication in the Federal Register.

11.3.7 Approve all Privacy Act statements prior to their reproduction and distribution.

11.3.8 Approve all Privacy Impact Assessments (PIAs) prior to submittal to OSD.

11.3.9 Notify the Privacy Officer, who will, in turn, notify Defense Privacy Office, when a complaint citing the Privacy Act of 1974 is filed in a U.S. District Court against DISA.

11.4 **Inspector General (IG).** The IG will conduct criminal investigations related to a breach or disclosure of PII, if circumstances warrant such an investigation.

11.5 **Director for Strategic Planning and Information (SPI).** The Director, SPI, will determine the most effective means to notify the public in cases of a breach of PII, in accordance with the OSD OA&M DoD Senior Privacy Official 5 June 2009 memorandum (authority document).

11.6 **Principal Directors, Directors, Commanders, and Chiefs of Major Organizational Elements.** These individuals will designate a Privacy Coordinator to be responsible for Privacy Act matters in their directorates. (The name of the Privacy Coordinator and an alternate is to be provided to the DISA Privacy Officer annually or when the designation changes.)

12. **System Manager Duties.** A system manager will:

12.1 Properly establish and maintain records that can be retrieved by a name or other personal identifier and handle documents as specified in the associated Privacy Act SORN.

12.1.2 Establish appropriate administrative, technical, and physical safeguards to ensure the records in each system of records are protected from unauthorized access, alteration, or disclosure and that their confidentiality is preserved and protected.

12.1.3 Ensure all personnel who handle records containing personal information are Privacy Act trained and know the proper procedures for protecting and safeguarding personal information.

12.1.4 Process Privacy Act requests forwarded by the Privacy Officer.

12.1.5 Maintain a disclosure accounting record for each Privacy Act system of records. (Subparagraph 14.2 provides additional details.)

12.1.6 Ensure all personnel who have access to information from a system of records or who are engaged in developing procedures for processing such information are aware of the provisions of the DoD Privacy Program policies and procedures.

12.1.7 Promptly notify the Privacy Officer of any required new, amended, or altered SORNs, whenever a new requirement for using personal information or an existing requirement or method of file storage changes.

12.1.8 Notify an individual, as soon as possible, but no later than 10 working days after discovery of the loss, theft, or compromise of protected PII. Advise the individual as to what specific data was involved and the circumstances surrounding the loss, theft, or compromise. Apprise the individual of protective actions that the individual can take.

12.1.9 Ensure all information systems and electronic collections that collect, maintain, use, or disseminate PII about members of the public, Federal personnel, contractors, or foreign nationals employed at U.S. military facilities internationally have a Privacy Impact Assessment (PIA) completed by the office responsible for the information system or electronic collection.

12.1.10 Ensure that whenever an agency's use of a third-party Web site or application makes PII available to the agency, an Adapted Privacy Impact Assessment (Adp-PIA) is completed by the office responsible for the information system or electronic collection. (Each adapted PIA should be tailored to address the specific functions of the Web site or application.)

12.1.11 Ensure that if any system is established, in whole or in part, and maintained by a contractor, that the Federal Acquisition Regulation (FAR) clauses 52.224-1, Privacy Act Notification, and 52.224-2, Privacy Act Solicitation Provision and Contract Clauses, are included in the contract.

12.1.12 Ensure mitigation effort for a compromised system is implemented to the greatest extent possible, provide necessary support to the breach reporting team for assessing the circumstances, and support the determining factors of mitigating and providing notification for the breach.

13. **Privacy Officer and Privacy Coordinator Duties.**

13.1 **Privacy Officer (PO).** The PO will:

13.1.1 Maintain liaison with the Defense Privacy and Civil Liberties Office.

13.1.2 Serve as the point of contact on administrative matters relating to the Privacy Act of 1974.

13.1.3 Direct the day-to-day activities of the DISA Privacy Program.

13.1.4 Develop and implement response procedures to be followed in the event of a breach of PII. (Procedures for reporting a breach are detailed in paragraph 18.)

13.1.5 Coordinate privacy-related activities and responses to breaches of PII with Agency managers, as appropriate.

13.1.6 Review PIAs, as required by the E-Government Act.

13.1.7 Submit SORNs for publication in the Federal Register.

13.1.8 Review and approve forms that collect PII prior to number issuance.

13.1.9 Provide guidance and assistance to the Privacy Coordinator in their implementation and execution of the Agency Privacy Program.

13.1.10 Develop and implement annual mandatory Privacy Act training.

13.1.11 Advise and train system managers and other Agency personnel on privacy requirements.

13.1.12 Direct and manage safeguard efforts on the enterprise portal to protect all PII within any content stores.

13.2 **Privacy Coordinator (PC) and Alternate Privacy Coordinator (APC).** A PC and an APC will:

13.2.1 Ensure organizations receive annual mandatory Privacy Act training.

13.2.2 Maintain an inventory of internal SORNs under the organization's sponsorship.

13.2.3 Serve as organization's liaison between the program managers that sponsor such system of records containing privacy information and the DISA Privacy Officer.

13.2.4 Conduct internal organizational reviews to ensure Privacy Act information is properly managed and protected.

13.2.5 Understand how to prepare a Privacy Act statement on a form and narrative statement for a new or altered SORN.

13.2.6 Advise the Agency Privacy Officer when systems containing Privacy Act information are no longer active.

13.2.7 Work closely with the respective repository site manager and content manager to ensure PII is protected from unauthorized disclosure and misuse.

13.2.8 Provide oversight for PII located in their organizational content stores on the enterprise portal.

13.2.9 Perform routine spot checks and searches in their organizational content stores on the enterprise portal to ensure PII is protected with the appropriate permissions.

13.2.10 Report all incidents involving the security, loss, misuse, or unauthorized disclosure of PII regardless of form or format immediately to the DISA Privacy Officer. (Procedures for reporting a breach are detailed on paragraph 18.)

14. **Recordkeeping and Reporting.** Privacy records and reports required to comply with provisions of the Privacy Act and applicable regulations are as follows:

14.1 A Privacy Act system of records notice (SORN) published in the Federal Register whenever a system of records is implemented or changed to include changing from a manual to an electronic system. (The format for a SORN is contained in Appendix 5 of DoD 5400.11-R [authority document].)

14.2 A disclosure accounting record containing the dates the record was disclosed; description of the information released; purpose of the disclosure; and name and address of the person or agency to whom the disclosure was made. The disclosure accounting record is maintained 5 years. (An individual requesting a record may also request the associated disclosure accounting record and is entitled to receive this record unless a published exemption to the Privacy Act SORN would prohibit such release.).

14.3 A litigation status sheet used by the system manager to keep the Privacy Officer apprised of legal developments concerning complaints lodged against the Agency under the Privacy Act of 1974. (The format is found in the Appendix 8 of DoD 5400.11-R.). A revised litigation status sheet is provided at each stage of the litigation. When a court renders a formal opinion or judgment, copies of the opinion or judgment are to be provided to the Defense Privacy Office via the Privacy Program

Office and office of the General Counsel (GC) with the latest litigation status sheet, which includes the report of that opinion of judgment.

14.4 A Privacy Impact Assessment (PIA) prepared when PII is collected, maintained, used, or disseminated in electronic form regarding members of the public, federal personnel, contractors, or foreign nationals employed at U.S. military facilities internationally.

14.1.5 An Adapted Privacy Impact Assessment (Adp-PIA) that is required whenever an agency's use of a third-party Web site or application makes PII available to the agency. Each adapted PIA should be tailored to address the specific functions of the Web site or application, but adapted PIAs need not be more elaborate than the agency's other PIAs. Each PIA is to be posted on the DISA Privacy Web site.

15. **Submission of a Privacy Act Request.**

15.1 **Internal Privacy Act Request.**

15.1.1 A request to obtain records from a system of records or to inspect a list of previous disclosures of records must be in writing. The request is submitted directly to the system manager in the office holding the record.

15.1.2 An individual's written request for access to or copies of records about himself or herself will be processed as a Privacy Act request unless it is otherwise specified as a Freedom of Information Act (FOIA) request.

15.2 **External Privacy Act Request.**

15.2.1 A request for access to records in a system of records must be in writing and directed to the CIO. In the case of a request received by mail, a notarized statement or unsworn declaration, in accordance with 28 U.S.C. 1746, proving the personal identity of the requester, is required.

15.2.2 A request from contractor personnel seeking explanation as to why they were not cleared for access and which does not mention either the Privacy Act or the FOIA will be referred to the Manpower, Personnel, and Security Directorate (MPS) Security Division (MPS6) for reply.

15.2.3 A request from applicants seeking an explanation as to why they were not hired and does not mention either the Privacy Act or the FOIA is referred to the MPS Civilian Personnel Division (MPS1) for reply.

16. **Appeal of Denial of Access to Privacy Act Information.** Any individual denied access to records may appeal the initial decision to the Privacy Act Appeal Authority within 60 calendar days of the date of the denial of access notification. A written determination will be issued to the appellant within 30 working days of the date of appeal or when all necessary information has been provided by the requester.

16.1 If the Appeal Authority cannot make a fair and equitable review within 30 days, the appellant will be notified, in writing, of the decision to extend the period of review, the reasons for the delay, and as to when the appellant may expect an answer. If the appeal is granted, the appellant will be notified, in writing, and granted access to the denied material.

16.2 If the Appeal Authority decides that the request for access should be denied, the recommendation of the Appeal Authority will be forwarded to the Vice Director who makes a final determination and, through the office of the GC, notifies the appellant, in writing, of the decision. The office of the GC ensures the notification complies with the appeals provisions contained in DoD 5400.11-R (authority document).

17. **Amendment of Records in a Privacy Act System of Records.** Minor factual errors (e.g. misspelled names, age, incorrect addresses, etc.) in an individual's personal records may be corrected routinely upon request without resort to the Privacy Act or to the provisions of this Instruction, provided the requester and the record holder agree to the procedure and the requester receives a copy of the corrected record whenever possible. Requests for deletions, removal of records, and amendment of substantive factual information will be processed in accordance with the following provisions:

17.1 A request submitted under the Privacy Act for amendment of a record containing substantial factual error because the information is incorrect or incomplete must be in writing and acknowledged within 10 working days of receipt of the request by the system manager of the record containing the information to be amended. The request is reviewed, and the requester advised of the result of the review within 10 working days.

If additional time is needed, there will be an extension of no more than 30 working days, and the requester will be advised of the extension.

17.1.2 If the system manager agrees with the request, the system manager notifies the requester and promptly amends the record and then notifies all holders and recipients of the record that the correction was made. The amendment procedure is not intended to replace other procedures; such as, those for registering grievances or appealing performance appraisal ratings.

17.1.3 If the system manager refuses to amend any part of a record, the system manager promptly notifies the requester of the refusal and states the reason(s). The system manager informs the requester of the procedures for requesting a review of the decision by the Privacy Act Appeal Authority.

17.1.4 Upon receipt of an appeal of a denial to amend a record, the Appeal Authority renders a decision within 30 working days, except when circumstances require an extension. If an extension is necessary, the requester will be informed, in writing, of the reasons for the delay and of the appropriate date on which the review is expected to be completed.

17.1.5 If the Appeal Authority denies the request for amendment, in whole or in part, the requestor promptly forwards the recommendation to the Vice Director who makes a final determination and, through the office of the GC, notifies the requester, in writing, of the decision. The office of the GC ensures the notification complies with the appeals procedure contained in DoD 5400.11-R (authority document). A copy of the memorandum sent to the requester will be provided to the DISA Privacy Officer.

18. **Breach Reporting.**

18.1 All DISA civilian employees and military personnel, as well as contractors, who discover a suspected or actual breach of personally identifiable information (PII) will immediately report the discovery to their supervisor and directorate Privacy Coordinator.

18.2 The directorate designated official and directorate Privacy Coordinator will submit a Preliminary PII Incident Report. (The format for the report, provided by the Defense Privacy Office, is located on DISA Privacy Web site at http://www.disa.mil/About/Legal-and-Regulatory/Privacy-Office.)

18.3 The Preliminary PII Incident Report will be electronically forwarded to the DISA Privacy Office, DISA Command Center (DCC), and the General Counsel (GC).

18.4 Within 1 hour of discovery of the PII breach, the reporting directorate will ensure the United States Computer Emergency Readiness Team (USCERT) has been notified, in accordance with the requirements and guidance at https://forms.us-cert.gov/report.

18.5 Within 24 hours of discovery of the PII breach, the Privacy Office, DCC, and GC will review the investigatory findings, analyze of the likelihood of risk to the affected individual and to DISA, and make the final decision as to whether a breach as occurred.

18.6 Within 48 hours of discovery of the PII breach, the Privacy Officer will notify the DISA Senior Privacy Official who will, in turn, notify the Chief Information Officer (CIO) and Director, DISA, that a breach, has occurred.

18.7 The DISA Privacy Officer will forward the completed Breach Report to the Defense Privacy and Civil Liberty Privacy Office (DPCLO).

19. **Privacy Act Training Requirements.** To meet Privacy Act training requirements for individuals that have differing functions in DISA, three levels of Privacy Act training are provided as follows:

19.1 Orientation training that provides basic understanding of this Instruction as it applies to the individual's job performance. This training is provided to personnel, as appropriate, and is a prerequisite to all other levels of training.

19.2 Specialized training that provides information as to the application of specific provisions of this Instruction to specialized areas of job performance. Personnel of particular concern include, but are not limited to, personnel specialists, finance officers, DISA personnel who may be expected to deal with the news media or the Public Affairs personnel, special

investigators, and other specialists (reports, forms, records, and related functions), computer systems administrators personnel, computer systems operations personnel, statisticians dealing with personal data and program evaluations, and individuals responsible for implementing or carrying out personnel-related functions. Specialized training is provided on a periodic basis.

19.3 Management training that is designed to identify for managers (such as senior system managers) considerations they should take into account when making management decisions regarding the DISA Privacy Program.

FOR THE DIRECTOR:

2 Enclosures a/s

FREDERICK A. HENRY
Brigadier General, USA
Chief of Staff

SUMMARY OF SIGNIFICANT CHANGES: This revision includes DoD Instruction 5400.16, DoD Privacy Impact Assessment (PIA) Guidance, as an authority document. DoDI 5400.16 states that all information systems and electronic collections that collect, maintain, use, or disseminate personally identifiable information (PII) must complete a Privacy Impact Assessment (PIA). Guidance on breach reporting when PII is lost, stolen, or compromised has been added. Definitions for PIA and PII are now included.

---

*This Instruction cancels DISAI 210-225-2, 16 February 2007.
OPR: CIO
DISTRIBUTION: P

Enclosure 1: DISAI 210-225-2

DEFINITIONS

Access. Permission for an individual to review a record, copy of a record, or parts thereof in a systems of records.

Agency. For the purpose of disclosing records subject to the Privacy Act among DoD Components, the Department of Defense is considered a single agency. However, for all other purposes involving the Privacy Act, the DoD Components are considered independent agencies. Other purposes include requests by individuals for access and amendment to records pertaining to them, denial of access or amendment to such records, appeals from denials, and the recordkeeping documenting access actions by system managers and Privacy Act Officials employed by each DoD independent agency.

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

Computer Match Program. The computerized comparison of two or more automated systems of records or a system of records with nonfederal records. Manual comparisons of systems of records or systems of records with nonfederal records are not covered.

Confidential Source. A person or organization who has furnished information to the Federal Government under an express promise that the person's or the organization's identity will be held in confidence or under an implied promise of such confidentiality if this implied promise was made before 27 September 1975.

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

Electronic Collection. Any collection of information enabled by information technology.

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

Law Enforcement Activity. Any activity engaged in the enforcement of criminal laws, including efforts to prevent, control, or reduce crime or to apprehend criminals and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities.

Lost, Stolen, or Compromised Information. Actual or possible unauthorized disclosure or personal information either to known or unknown persons whether or not a potential exists that the information may be used for unlawful purposes to the detriment of the individual.

Maintain. In the context of the Privacy Act, "maintain" includes collecting, using, or disseminating, as well as just keeping and holding, personal information contained in a Privacy Act system of records.

Official Use. Within the context of this Instruction, this term is used when officials and employees of a DoD Component have a demonstrated need for the use of any record or the information contained therein in the performance of their official duties, subject to DoD 5200.01-R, Volume 3, DoD Information Security Program: Protection of Classified Information.

Personal Information. Information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc. Such information is also known as personally identifiable information (PII) (i.e., information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, and biometric records, including any other personal information which is linked or linkable to a specified individual).

Personally Identifiable Information (PII). Any information about an individual maintained by an agency, which can be used

to distinguish, trace, or identify an individual's identity, including personal information which is linked or linkable to an individual.

Privacy Impact Assessment. An analysis of how information is handled: (a) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (b) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and (c) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

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

Record. Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic, etc.), about an individual that is maintained by a DoD Component, including, but not limited to, his or her education, financial transactions, medical history, or criminal or employment history and that 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.

Risk Assessment. An analysis considering information sensitivity, vulnerabilities, and cost in safeguarding personal information processed or stored in the facility or activity.

Routine Use. The disclosure of a record outside DoD for a use that is compatible with the purpose for which the information was collected and maintained by DoD. The routine use must be included in the published system notice for the system of records involved.

System Manager. The DoD component official who is responsible for the operation and management of a system of records.

System of Records. A group of records under the control of a DoD component from which personal information about an individual is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned, that is unique to the individual.

Enclosure 2: DISAI 210-225-2

INDIVIDUAL ACCESS TO PRIVACY ACT INFORMATION

1. If an individual has been given access to his or her personnel file as a result of a Privacy Act request, the file will continue to be available to the individual for review without the submission of a second request.

2. A requester does not need to state a reason or otherwise justify a Privacy Act request and may be accompanied by another person when Privacy Act records are requested in person rather than in writing. In this case, the requester may be required to furnish a statement authorizing discussion of the records in the presence of the other person. If a requester asks another person to obtain a record on his or her behalf, the requester must provide a notarized statement appointing that person as his or her representative, authorizing the person access to the records, and affirming that such access will not constitute an invasion of the requester's privacy or a violation of rights under the Privacy Act.

3. The requester will not be charged a fee for making a readable copy to satisfy the request, to review a record, or to provide a copy in response to a request by mail.

4. A medical record will be disclosed to the individual to whom it pertains unless the system manager determines providing the record could have an adverse effect on the requester. In such case, the requester will be advised the information will be sent to a doctor named by the requester. If the doctor refuses to disclose the record to the patient, the requester must provide a statement to the system manager noting the doctor's refusal. At this point, the system manager must provide the requested record directly to the requester.

5. An individual requesting access to investigatory records compiled by another agency, but in the custody of DISA, will be referred to the originating agency.

6. An individual is not entitled to have access to any information compiled in reasonable anticipation of a civil action or proceeding nor is an individual entitled to have a record created in response to a request for information.

7. Copies of classified records will be released only to persons authorized to receive such material.