DEFENSE INTELLIGENCE AGENCY
WASHINGTON, DC 20340-5100

DIAI 5400.001
19 May 2014
OPR: FAC

Privacy and Civil Liberties Program

References:

(a) DIA Instruction 5400.001, "Defense Intelligence Agency Privacy Program," 1 August 2008 (canceled)
(b) DIAI 5415.003, "DIA Privacy and Civil Liberties Protection Policy for Operating Within the Information Sharing Environment," 22 April 2009 (canceled)
(c) Title 5, United States (U.S.) Code, Section 552a, "The Privacy Act of 1974," as amended
(d) DoD Directive 5400.11, "Department of Defense Privacy Program," Change 1, 1 September 2011
(e) OMB Memorandum for the Heads of Departments and Agencies, M-06-15, "Safeguarding PII," 22 May 2006
(f) through (r), see Enclosure 1

1. Purpose.

1.1. Replaces References (a) and (b).

1.2. Assigns responsibilities and establishes procedures for the Defense Intelligence Agency (DIA) Privacy and Civil Liberties Program.

1.3. Implements References (c) through (q).

1.4. Applies to all DIA centers, directorates, offices, and combatant command directorates for intelligence (hereafter referred to as DIA elements) and all DIA civilian employees, military personnel, and contractors (hereafter referred to as DIA employees).

1.5. Pertains to all information processed, produced, used, or stored by DIA or within DIA records systems.

2. Definitions – see Enclosure 2.

3. Responsibilities.

3.1. The Director, DIA, must ensure compliance with the Privacy Act of 1974 (Reference (c)).

3.2. The Deputy Director, DIA, must appoint the Agency's Privacy and Civil Liberties Officer (PCLO) in order to meet the concerns expressed in the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458) (Reference (f)), regarding the protection of privacy and civil liberties.

3.3. The Vice Director for Mission Services must:

3.3.1. Serve as the Agency's PCLO. The PCLO is responsible for ensuring that the Agency is in compliance with applicable statutory laws.

3.3.2. Serve as the Senior Agency Official for Privacy.

3.4. The Office of Facilities and Services (FAC) Records Management and Information Services Branch must:

3.4.1. Implement the Privacy and Civil Liberties Program.

3.4.2. Ensure valid and legal requirements are identified for the collection of personally identifiable information (PII) and provide direction and guidance to guarantee compliance with References (c), (d), (g), and (h).

3.4.3. Assess privacy and civil liberties requirements when reviewing regulations, policies, procedures, or guidelines related to the mission of DIA.

3.4.4. Submit Section D (Privacy Report Section) of the Federal Information Security Management Act to the Office of the Director of National Intelligence and the Department of Defense (DoD) Privacy and Civil Liberties Office.

3.4.5. Submit quarterly reports on the activities of the civil liberties program in accordance with Reference (g).

3.4.6. Provide an annual Privacy Act "State of Health" report documenting the status of the Privacy and Civil Liberties Program.

3.4.7. Publish component privacy procedural rules, exemption rules, and system notices in the Federal Register.

3.4.8. Respond to any breach (loss, theft, or compromise) of PII by initiating an inquiry regarding the circumstances surrounding the breach in order to determine the need for further action.

3.4.9. Initiate procedures to receive, investigate, respond to, and redress complaints from individuals who allege violation of their privacy or civil liberties.

3.4.10. Provide the Office of the Inspector General (OIG) with DIA's privacy protection policies and procedures, respond to any review of the program that is directed, and coordinate privacy and civil liberties activities to avoid duplication of effort.

3.4.11. Process requests for access to personal information in a system of records.

3.5. The Office of the Chief Information Officer must:

3.5.1. Ensure that information protected under the Privacy Act, in electronic format, is secure across the global information technology enterprise.

3.5.2. Establish technical safeguards that are adequate to protect information against unauthorized disclosure, access, or misuse.

3.5.3. Conduct a privacy impact assessment (PIA) on any DIA information system that collects, maintains, uses, or disseminates PII regarding members of the public, federal personnel, contractors, or foreign nationals employed at U.S. military facilities internationally.

3.5.4. Report any loss, theft, or compromise of PII contained in DIA information systems to the PCLO and FAC Records Management and Information Services Branch, and make the appropriate notifications pursuant to Office of Management and Budget requirements, in accordance with Reference (h).

3.5.5. Assist the PCLO and FAC Records Management and Information Services Branch with conducting an inquiry into the loss, theft, or compromise of PII contained with DIA information systems by providing an assessment of the circumstances with a recommended course of action.

3.6. The Office of the General Counsel (OGC) must:

3.6.1. Provide the PCLO and FAC Records Management and Information Services Branch legal advice and recommendations regarding all aspects of the Privacy and Civil Liberties Program.

3.6.2. Review all Federal Register publication requirements and privacy impact assessments for legal compliance.

3.7. The Office of the Chief Financial Officer (CFO) must:

3.7.1. Ensure that applicable Federal Acquisition Regulation Privacy Act clauses are included in contracts that provide for the creation of a system of records. A systems of records is required when a contracted activity involves the collection of PII on behalf of DIA.

3.7.2. Advise any contractor collecting or maintaining PII, when operating on behalf of DIA, to notify the CFO of any loss, theft, or compromise of data immediately following the incident.

3.7.3. Report any incident of loss, theft, or compromise of data to the PCLO and assist with inquiries regarding the incident.

3.7.4. Advise the contractor responsible for maintaining PII that pursuant to the contract privacy act clause, the contractor must cooperate fully with any inquiry.

3.8. The OIG must:

3.8.1. Provide oversight of the Privacy and Civil Liberties Program.

3.8.2. Determine the best investigative course of action, in consultation with the PCLO, should there be loss, theft, or compromise of PII.

3.8.3. Assist the PCLO by conducting an investigation regarding the loss, theft, or compromise of PII in accordance with Reference (g).

3.8.4. Report any loss, theft, or compromise of PII discovered during the course of any OIG inspection activity.

3.9. The Office of Security must:

3.9.1. Provide the PCLO with a report documenting misuse of PII discovered during the course of monitoring procedures.

3.9.2. Assist the PCLO by conducting an investigation regarding the loss, theft, or compromise of PII in accordance with Reference (q).

3.9.3. Provide the PCLO a copy of DIA Form 43, Report of Survey, when the resulting report involves the accountability of a laptop, wireless communications devices, or computer processing unit containing PII.

3.10. The Office of Corporate Communications must review Federal Register publication requirements as necessary prior to public release, in accordance with Reference (m).

3.11. The Equal Opportunity and Diversity Office must refer any complaints alleging a violation of privacy or civil liberties to the PCLO.

3.12. DIA elements and employees must:

3.12.1. Implement and adhere to all privacy and civil liberties protection requirements.

3.12.2. Identify privacy or civil liberties issues or concerns and bring them to the attention of the PCLO or FAC Records Management and Information Services Branch. Report the actual incident on DIA Form 540-2, "Privacy/Civil Liberties Incident Reporting Form," located on the FAC Source website.

3.12.3. Ensure completion of the annual privacy or civil liberties training via the Advanced Global Intelligence Learning Environment (AGILE) or computer disk based training if connectivity to AGILE is limited or unavailable.

3.12.4. Document the use of PII, through a system of records notice (SORN) and privacy impact assessment. The SORN PIA assessment checklist provides detailed guidance on submission procedures in accordance with Enclosure 3.

4. Procedures.

4.1. To the maximum extent practicable, PII will be collected directly from the individual to whom it pertains. Protection of the privacy and civil liberties of DIA employees will be consistent with operational requirements.

4.2. Posting of Social Security Numbers, completely or in part, on any public facing or open government website in any form, is not permissible.

4.3. Release of documents containing PII to third parties outside of the government is permissible only with agreement from the recipient of the information that they will not post it to any public facing websites or open government sites. Such releases must be coordinated with the DIA PCLO and OGC.

4.4. Removal of information containing PII in its original or copied paper or electronic form beyond government premises or control is not allowed. The DIA PCLO and OGC approve exceptions to this guidance.

4.5. A DIA Form 43, "Report of Survey," will be completed when the report is related to accountability of laptops, wireless communications devices, or computer processing unit containing PII. This information will be forwarded to FAC Records Management and Information Services Branch.

4.6. Transfer of information.

4.6.1. Transfer of PII via electronic means to unsecure or non-governmental email addresses is not authorized. For example, PII data may not be transferred using service providers such as America on-line, Google mail, Hotmail, Yahoo, Comcast or Verizon.

4.6.2. Transfer of personal information, other than your own, to an official government or military domain is permissible. Prior to transmitting to an official email address containing a military (shown as .mil) or government (shown as .gov) domain, adhere to the

following precautions:

4.6.3. Ensure you are authorized to transmit the information.

4.6.4. Verify recipient email address prior to transmission.

4.6.5. Utilize encryption software, if available.

4.6.6. Embed a privacy act caveat in the email "UNCLASSIFIED//FOUO//PRIVACY ACT – DATA.

4.7. Any DIA employee involved with the loss, theft, or willfull and wrong disclosure or compromise of protected personal information may be subject to criminal prosecution and/or administrative action, up to and including removal from federal service.

4.8. Social Security Numbers.

4.8.1. It is unlawful for any federal, state, or local government agency to deny an individual any right, benefit, or privilege provided by law because the individual refuses to provide their Social Security Number.

4.8.2. When providing a Social Security Number, it must be on an official form, such as a Standard Form, Optional Form, DoD Form, or DIA Form.

4.8.3. Individuals providing their Social Security Number must be informed of the use, statute, regulation, or rule authorizing the solicitation and whether providing the number is voluntary or mandatory.

4.9. When an individual receives a request to furnish personal information, a Privacy Act Statement (PAS) is required regardless of the medium used to collect the information. The PAS enables the individual to make an informed decision on whether to provide the information requested. The PAS can be part of the official form and it does not require a signature.

4.10. In some cases, it may not be practical to collect personal information directly from the individual. Examples of third party collection are verification of information for security or employment suitability.

4.11. Records management. DIA file plans must identify files which contain PII (whether hardcopy or electronic copy) by including "PA" next to the file series in accordance with Reference (r) and the DIA Records Management User's Guide located on the FAC Source webpage.

4.12. Marking, transmitting, and handling PII. Treat all unclassified records containing PII as "For Official Use Only (FOUO)." When transmitting records containing PII via email, use the following caveat: "UNCLASSIFIED//FOUO//PRIVACY ACT DATA." DIA Form 540-1, "Cover Sheet for Privacy Related Documents," is used as a coversheet when handling records that contain PII. The form islocated on the FAC Source webpage.

for David R. Shedd
MICHAEL T. FLYNN
Lieutenant General, USA
Director

E2. Definitions
E3. System of Records Notice/Privacy Impact Assessment Checklist
E4. System of Records Notice Format
E5. Procedures for Submitting a Privacy/Civil Liberties Complaint

Enclosure 1.

ADDITIONAL REFERENCES

(f) Public Law 108-458, Intelligence Reform and Terrorism Prevention Act of 2004, 15 December 2004
(g) DoD Instruction 1000.29, "DoD Civil Liberties Program," 17 May 2012
(h) Intelligence Community Directive (ICD) 107, "Civil Liberties and Privacy," 31 August 2012
(i) OMB Memorandum for Chief Information Officers, M-06-19, "Reporting Incidents Involving PII and Incorporating the Cost for Security in Agency Information Technology Investments," 12 July 2006
(j) E-Government Act of 2002, 17 December 2002
(k) DIA Instruction 5000.035, "Acquisition Regulation Supplement and Instruction (DARSI)," Change 1, 26 March 2012
(l) DIAI 5400.002, "Freedom of Information Act Program," 9 May 2014
(m) DIAI 5400.005, "Prepublication Review of Information Prepared for Public Release," 19 November 2013
(n) DIAI 8500.001, "DoD SCI – DoDIIS Community Information Assurance Program," 20 March 2008
(o) Public Law 110-53, 9/11 Commission Act of 2007, 3 August 2007
(p) DoD Manual 8910.1-M, "Department of Defense Procedures for Management of Information Requirements," 30 June 1998
(q) DIA Manual 60-1, "Administrative Investigations," 28 April 1997
(r) DIAI 5015.001A, "Records Management Program," 20 May 2011

Enclosure 2.

DEFINITIONS

Breach – For personally identifiable information, any information, in paper or electronic form, that is lost, misplaced, stolen, or accessed by unauthorized personnel or improperly disseminated.

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

Complaint – An assertion alleging a violation of privacy and/or civil liberties.

Federal Information Security Management Act (FISMA) of 2002 – Act that provides the framework for securing Federal Government information technology, including both unclassified and national security systems.

Federal Register – The official journal of the Federal Government of the United States that contains most routine publications and public notices of government agencies.

Individual – A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence.

Information Management Control Officer (IMCO) – Oversees the management, control, approval process, and tracking of all component internally generated collections to preclude DoD resources from being expended on redundant and obsolete information collections.

Personally Identifiable Information (PII) – Any information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etcetera, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date of birth, mother's maiden name, etcetera.

Personal identifier – A name, identifying symbol, or other identifying particular assigned to an individual for access or identification in a system of records.

Privacy and civil liberties violation – Privacy and civil liberties violations do not include equal opportunity complaints as identified by the Equal Opportunity and Diversity Office (EO). Visit the EO Source webpage for information on the subject.

Privacy impact assessment (PIA) – An analysis of information that ensures adherence to applicable legal, regulatory and policy requirements regarding privacy, in order to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Record – An item, collection, or grouping of information about an individual maintained by or on behalf of the Agency.

Routine use – With respect to the disclosure of a record, the use of such record for a purpose, which is compatible with the reason it was originally collected.

System – An organized assembly or resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions.

System of records (SOR) – A group of any records under the control of any agency from which information is retrievable by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

System of records notice (SORN) – A SORN is an analysis of paper or electronic records under the control of DIA to ensure collection of the records in a manner that protects privacy. It is the notice posted to the Federal Register documenting the SOR.

U.S. Citizen – A born or naturalized citizen of the United States.

U.S. Person - For intelligence oversight purposes; one of the following, a U.S. Citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of U.S. Citizens or permanent resident aliens; or a corporation incorporated in the United States, except for those directed and controlled by a foreign government or governments.

Enclosure 3.

SYSTEM OF RECORDS NOTICE PRIVACY IMPACT ASSESSMENT CHECKLIST – EXAMPLE

1. Personally Identifiable Information (PII). Any information collected or maintained by an agency about an individual, including, but not limited to education, financial transactions, medical history, and criminal or employment history and information containing the individual's name, social security number, date or place of birth, mother's maiden name, biometric records, or other personal information that is linked to a specifically-identifiable individual.

2. U.S. Persons:

2.1. For intelligence purposes:

2.1.1. A citizen of the United States, an unincorporated association organized in the United States or substantially composed of U.S. citizens, or permanent resident aliens, an alien known by the intelligence agency concerned to be a permanent resident alien, or a corporation incorporated in the United States (except for a corporation directed and controlled by a foreign government or governments).

2.1.2. Does the system collect, maintain, or disseminate PII on agency employees to include civilian, military, or contract personnel? Yes / No

2.1.3. Does the system collect, maintain, or disseminate PII on members of the public? Yes / No.

2.1.4. Does the system collect, maintain, or disseminate PII on U.S. persons? Yes / No.

2.1.5. Is the information retrievable by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual (as defined in the PII definition above)? Yes / No.

2.1.6. Type of system: paper or electronic?

2.1.7. Is the information collected in paper or electronic form, verbally, migrated from another system, etcetera?

2.1.8. If the system is electronic, where does it reside? Joint Worldwide Intelligence Communications System, Secret Internet Protocol Routing Network, Non-secure Internet Protocol Router Network.

Enclosure 4.

SYSTEM OF RECORDS NOTICE FORMAT

1. A system of records notice (SORN) published in the Federal Register must include information on the existence and charter of the system of records maintained by an agency.

2. The Federal Register is the official journal of the Federal Government of the United States that contains most routine publications and public notices of government agencies. All SORNs will include the following information:

2.1. System Name

2.2. System Locations

2.3. Categories of individuals covered by the system

2.4. Categories of records in the system

2.5. Authority for maintenance of the system

2.6. Purpose

2.7. Routine uses of records maintained in the system, including categories of users and the purposes of such uses

2.8. Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system

2.9. Storage

2.10. Irretrievability

2.11. Safeguards

2.12. Retention and disposal

2.13. System Manager(s) and address

2.14. Notification procedures

2.15. Record access procedures

2.16. Contesting records procedures

2.17. Record source categories

2.18. Exemptions claimed for the system

Enclosure 5.

PROCEDURES FOR SUBMITTING A PRIVACY/CIVIL LIBERTIES COMPLAINT

1. Prior to filing a complaint, ensure the compliant relates to a privacy, civil liberty right or freedom, as defined in Enclosure 2.

2. When filing a complaint, indicate the following:

2.1. The nature of the violation

2.2. When the violation occurred or whether it is ongoing.

2.3. State where the violation occurred.

2.4. Provide an explanation of the violation.

2.5. Submit the complaint via email to: ~DIA_Privacy_Civil_Liberties_Office. The Office of Facilities and Services, Privacy and Civil Liberties Program will provide acknowledgement and after thorough review, notification of any pending action.