DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

CM

DCAA REGULATION NO. 5410.10

October 24, 2006

DCAA PRIVACY PROGRAM
(RCS: DD-COMP(A)1379)

References: (a) Title 5, United States Code, Section 552a (http://www.access.gpo.gov/uscode/title5/parti_chapter5_subchapterii_.html)

(b) DoD 5400.11-R, DoD Privacy Program (http://www.defenselink.mil/privacy)

(c) DCAAR 5410.8, DCAA Freedom of Information Act Program (http://www.dcaa.mil (under FOIA))

(d) Office of Management & Budget (OMB) Memorandum M-03-22, dated September 26, 2003, subject: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (http://www.whitehouse.gov/omb/memoranda/m03-22.html)

(e) DCAAR 8500.1, Information Assurance (IA) Program (available on DCAA's Intranet)

(f) Secretary of Defense Memorandum, dated October 28, 2005, subject: Department of Defense (DoD) Privacy Impact Assessment (PIA) Guidance (http://www.defenselink.mil/privacy/DoD_PIA_Guidance_Oct_28_2005.pdf)

(g) DCAAP 5410.18, The Privacy Act: An Employee Guide to Privacy (available on DCAA's Intranet)

1. REISSUANCE AND PURPOSE. This regulation provides policies and procedures for the Defense Contract Audit Agency's implementation of the Privacy Act of 1974 and is intended to promote uniformity within the Agency.

2. CANCELLATION. The May 16, 2000, edition of this regulation is canceled.

3. APPLICABILITY AND SCOPE.

3.1. This regulation applies to all DCAA organizational elements and takes precedence over all regional regulatory issuances that supplement the DCAA Privacy Program.

3.2. This regulation shall be made applicable by contract or other legally binding action to contractors whenever a DCAA contract provides for the operation of a system of records or portion of a system of records to accomplish an Agency function.

4. DEFINITIONS.

4.1. Individual. An individual is a citizen of the United States or an alien lawfully admitted for permanent residence.

4.2. Privacy Impact Assessment (PIA). A PIA is an analysis of how information is handled: (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

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

4.4. System of records. A group of any records under the control of DCAA from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Systems of records must have a system notice published in the Federal Register and are subject to the provisions of this regulation. All other records fall under the provisions of the Freedom of Information Act (FOIA) (reference c).

5. POLICY. It is DCAA policy that personnel will comply with the DCAA Privacy Program and the Privacy Act of 1974. Strict adherence is necessary to ensure uniformity in the implementation of the DCAA Privacy Program and to create conditions that will foster public trust. It is also Agency policy to safeguard personal information contained in any system of records maintained by DCAA organizational elements and to make that information available to the individual to whom it pertains to the maximum extent practicable. DCAA policy specifically requires that DCAA organizational elements:

5.1. Collect, maintain, use, and disseminate personal information only when it is relevant and necessary to achieve a purpose required by statute or Executive Order.

5.2. Collect personal information directly from the individuals to whom it pertains to the greatest extent practical.

5.3. Inform individuals who are asked to supply personal information for inclusion in any system of records:

5.3.1. The authority for the solicitation.

5.3.2. Whether furnishing the information is mandatory or voluntary.

5.3.3. The intended uses of the information.

5.3.4. The routine disclosures of the information that may be made outside of DoD.

5.3.5. The effect on the individual of not providing all or any part of the requested information.

5.4. Ensure that records about individuals containing personal information are accurate, relevant, timely, and complete for the purposes for which they are being maintained.

5.5. Keep no record that describes how individuals exercise their rights guaranteed by the First Amendment to the U.S. Constitution, unless expressly authorized by statute or by the individual to whom the records pertain or is pertinent to and within the scope of an authorized law enforcement activity.

5.6. Notify individuals whenever records pertaining to them are made available under compulsory legal processes, if such a process is a matter of public record, and to obtain prior written consent to disclosure from the individual, unless the information requested is disclosed to the individual concerned, or is subject to disclosure as a routine use, or may otherwise be disclosed under any exemption established in 5 U.S.C. § 552a(b), or as allowed by other applicable authority.

5.7. Establish safeguards to ensure the security of personal information and to protect this information from threats or hazards that might result in substantial harm, embarrassment, inconvenience, or unfairness to the individual.

5.8. DCAA personnel involved in the design, development, operation, or maintenance of any system of records shall adhere to the requirements of this regulation, DCAAR 8500.1 (reference e), and DCAAP 5410.18 (reference g).

5.9. Assist individuals in determining what records pertaining to them are being collected, maintained, used, or disseminated.

5.10. Permit individuals access to their personal information maintained in any system of records, and to correct or amend that information, unless an exemption for the system has been properly established.

5.11. Provide to an individual, upon request, an accounting of all disclosures of the information pertaining to them except when disclosures are made:

5.11.1. To DoD personnel in the course of their official duties.

5.11.2. Under DoD 5400.11-R (reference b).

5.11.3. As stated in the system notice or under DoD Blanket Routine Uses.

5.11.4. To another agency or to an instrumentality of any governmental jurisdiction within or under control of the United States conducting law enforcement activities authorized by law.

5.12. Advise individuals on their right to appeal any denial of access to or amendment of any record pertaining to them, and their right to file a statement of disagreement if amendment of a record is denied.

6. RESPONSIBILITIES.

6.1. Headquarters.

6.1.1. The Assistant Director, Resources has overall responsibility for the DCAA Privacy Program and will serve as the sole appellate authority for appeals to decisions of initial denial authorities.

6.1.2. Under the direction of the Assistant Director, Resources, the Chief, Administrative Management Division shall:

6.1.2.1. Establish, issue, and update policies for the DCAA Privacy Program; monitor compliance with this regulation; and provide policy guidance for the DCAA Privacy Program.

6.1.2.2. Resolve conflicts that may arise regarding implementation of DCAA Privacy Program policy.

6.1.2.3. Designate an Agency privacy adviser, as a single point of contact, to coordinate on matters concerning Privacy Act policy.

6.1.2.4. Make the initial determination to deny an individual's written Privacy Act request for access to or amendment of documents filed in any Agency system of records. This authority cannot be delegated.

6.1.3. The DCAA privacy adviser under the supervision of the Chief, Administrative Management Division shall:

6.1.3.1. Manage the DCAA Privacy Program in accordance with this regulation and applicable DCAA policies, as well as DoD and Federal regulations.

6.1.3.2. Provide guidelines for managing, administering, and implementing the DCAA Privacy Program.

6.1.3.3. Implement and administer the DCAA Privacy Program at Headquarters.

6.1.3.4. Ensure that the collection, maintenance, use, or dissemination of records of identifiable personal information is in a manner that assures that such action is for a necessary and lawful purpose; that the information is timely and accurate for its intended use; and that adequate safeguards are provided to prevent misuse of such information.

6.1.3.5. Review and coordinate proposed PIAs to confirm that privacy implications have been identified and evaluated to ensure the proper balance is struck between an individual's privacy and the Agency's information requirements.

6.1.3.6. Prepare promptly any required new, amended, or altered system notices for systems of records subject to the Privacy Act and submit them to the Defense Privacy Office for subsequent publication in the Federal Register.

6.1.3.7. Prepare the annual Privacy Act Report as required by DoD 5400.11-R, DoD Privacy Program.

6.1.3.8. Conduct training on the DCAA Privacy Program for Agency personnel.

6.1.4. Heads of Principal Staff Elements are responsible for:

6.1.4.1. Reviewing all regulations or other policy and guidance issuances for which they are the proponent to ensure consistency with the provisions of this regulation.

6.1.4.2. Ensuring that the provisions of this regulation are followed in processing requests for records located in systems of records.

6.1.4.3. Forwarding to the DCAA privacy adviser any Privacy Act requests received directly so that the request may be administratively controlled and processed.

6.1.4.4. Ensuring the prompt review of all Privacy Act requests and, when required, coordinating those requests with other organizational elements.

6.1.4.5. Providing recommendations to the DCAA privacy adviser regarding the releasability of DCAA records to individuals, along with the responsive documents.

6.1.4.6. Providing the appropriate documents, along with a written justification for any denial, in whole or in part, of a request for records to the DCAA privacy adviser (reference b, paragraph C3.2). The portions of the documents to be excised should be bracketed in red pencil, and the specific exemption or exemptions cited that provide the basis for denying the requested records.

6.1.5. The Chief Information Officer (CIO) is responsible for completing actions in accordance with reference f:

6.1.5.1. Ensuring that personal information in electronic form is only acquired and maintained when necessary, and that the supporting information technology (IT) that is being developed and used protects and preserves the privacy of individuals.

6.1.5.2. Providing for the planning, coordination, integration, and oversight of all DCAA information assurance (IA) activities (reference e).

6.1.5.3. Serving as the Agency's PIA review official.

6.1.5.4. Ensuring that new or modified IT systems that collect, maintain, or disseminate information in identifiable form and/or new electronic collections of information in identifiable form, for 10 or more persons (excluding DoD personnel), have a PIA performed by the office responsible for the IT system (reference d). (Refer to Enclosure 1 for the DoD PIA format.)

6.1.5.5. Ensuring PIAs are completed before developing, procuring, or modifying the IT system; and acquiring appropriate coordinations with the office submitting the request, the IA official, and the Chief, Administrative Management Division, Headquarters.

6.1.5.6. Forward all PIAs for IT systems and projects to OMB.

6.1.5.7. Post approved PIAs or summary PIAs on the Agency's public web site.

6.1.6. The General Counsel is responsible for:

6.1.6.1. Ensuring uniformity is maintained in the legal position, and the interpretation of the Privacy Act, DoD 5400.11-R, and this regulation.

6.1.6.2. Consulting with DoD General Counsel on final denials that are inconsistent with decisions of other DoD components, involve issues not previously encountered, or raise new or significant legal issues of potential significance to other Government agencies.

6.1.6.3. Providing advice and assistance to the Assistant Director, Resources; regional directors; the Chief Information Officer; and the regional privacy officer, through the DCAA privacy adviser, as required, in the discharge of their responsibilities.

6.1.6.4. Coordinating Privacy Act litigation with the Department of Justice.

6.1.6.5. Coordinating on Headquarters denials of initial requests and appeals.

6.2. Regional Directors:

6.2.1. Are responsible for the overall management of the Privacy Program within their respective regions.

6.2.2. Shall, as designee of the Director, make the initial determination to deny an individual's written Privacy Act request for access to or amendment of documents filed in any Agency system of records. This authority cannot be delegated.

6.2.3. Are responsible for providing direction to the appropriate regional manager who is responsible for the management and staff supervision of the program and for designating a regional privacy officer.

6.2.4. Regional privacy officers shall:

6.2.4.1. Implement and administer the DCAA Privacy Program throughout the region.

6.2.4.2. Ensure that the collection, maintenance, use, or dissemination of records of identifiable personal information is done in accordance with this regulation and in a manner that assures that such action is for a necessary and lawful purpose; that the information is timely and accurate for its intended use; and that adequate safeguards are provided to prevent misuse of such information.

6.2.4.3. Prepare input for the annual Privacy Act Report when requested by the DCAA privacy adviser.

6.2.4.4. Conduct training on the DCAA Privacy Program for regional and FAO personnel.

6.2.4.5. Provide recommendations to the regional director through the appropriate regional manager regarding the releasability of DCAA records to individuals.

6.2.5. Managers, Field Audit Offices (FAOs), shall:

6.2.5.1. Ensure that the provisions of this regulation are followed in processing requests for records.

6.2.5.2. Forward to the regional privacy officer any Privacy Act requests received so that the request may be administratively controlled and processed.

6.2.5.3. Ensure the prompt review of all Privacy Act requests and, when required, coordinate those requests with other organizational elements.

6.2.5.4. Provide recommendations to the regional privacy officer regarding the releasability of DCAA records to individuals, along with the responsive documents.

6.2.5.5. Provide the appropriate documents, along with a written justification for any denial, in whole or in part, of a request for records to the regional privacy officer (reference b, paragraph C3.2). The portions of the documents to be excised should be bracketed in red pencil, and the specific exemption or exemptions cited that provide the basis for denying the requested records.

6.3. DCAA employees shall:

6.3.1. Not disclose any personal information contained in any system of records, except as authorized by this regulation.

6.3.2. Not maintain any official records that are retrieved by name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual without identifying the statute or Executive Order authorizing the collection of such information and ensuring that a notice for the system of records has been published in the Federal Register.

6.3.3. Report any disclosures of personal information from a system of records.

6.3.4. Report the use of any system of records not authorized by this regulation to the appropriate Privacy Act officials for action.

7. PROCEDURES. Procedures for processing material in accordance with the Privacy Act of 1974 are outlined in reference b.

8. REPORTS. The annual Privacy Act report has been assigned Report Control Symbol DD-COMP(A)1379. Reporting requirements are prescribed and detailed in DoD 5400.11-R (reference b).

9. EFFECTIVE DATE. This regulation is effective immediately.

/s/

William H. Reed
Director

Enclosure:
DoD PIA Format

ENCLOSURE

DOD PRIVACY IMPACT ASSESSMENT (PIA) FORMAT

(Use N/A where appropriate)

1. Department of Defense (DoD) Component.

2. Name of Information Technology (IT) System.

3. Budget System Identification Number (SNAP-IT Initiative Number).

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)).

5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable).

6. Privacy Act System of Records Notice Identifier (if applicable).

7. OMB Information Collection Requirement Number (if applicable) and Expiration Date.

8. Type of authority to collect information (statutory or otherwise).

9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup).

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.).

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a Component program, etc.)

13. Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.).

14. Describe whether the system derives or creates new data about individuals through aggregation.

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.).

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November 11, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.

20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

Preparing Official _____ (signature) _____ (date)
Name
Title:
Organization:
Work Phone Number:
Email:

Information Assurance Official _____ (signature) _____ (date)
Name:
Title:
Organization:
Work Phone Number:
Email:

Privacy Officer _____(signature) _____ (date)
Name:
Title:
Organization:
Work Phone Number:
Email:

Reviewing Official _____ (signature) _____ (date)
Name:
Chief Information Officer
Organization:
Work Phone Number:
Email: