



PRIVACY IMPACT ASSESSMENT (PIA)

For the

DCAA Management Information System

Defense Contract Audit Agency

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR** Enter DITPR System Identification Number
- Yes, SIPRNET** Enter SIPRNET Identification Number
- No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes**
- No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- Yes**
- No**

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office

Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Yes

Enter OMB Control Number

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

5 U.S.C. 301, Departmental Regulations and E.O. 9397 (SSN).

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

DMIS is DCAA's primary management information system that supports DCAA's mission of performing contract audits for the Department of Defense and providing accounting and financial advisory services regarding contracts and subcontracts to all DoD. Records relating to audit work performed in terms of hours expended by individual employees, dollar amounts audited, exceptions reported, and net savings to the government as a result of those exceptions; records containing employee data; name, Social Security Number, time and attendance, and work schedule; and records containing office information, e.g., duty station address and telephone number.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Privacy of PII is of critical importance to the employees and the DCAA. Managing the risk to prevent the release of PII is the responsibility of the DMIS administrators, file custodians, business process owners and the individual employees who access and utilize that information. The risks are mitigated by the application of a strict access security model and training. The following briefly describes steps taken in more detail:
Access to the information is controlled through a strictly enforced role based security model. The number of necessary users with access to the records that contain PII is kept to a minimum by close monitoring of the role allocation.

Administrative access to the application is required to modify the roles based security model.
Physical security to the DCAA owned and managed servers is only allowed after access to the complex (grounds), building, and cipher locked door and requires prior authorization from the Data Center Manager. Server administrators possess a Secret clearance as per DoD policy.
Access to DMIS is provided on a need to know basis, and via a valid CAC and Public Key Infrastructure (PKI) enabled authentication. All employees (to include contractors) receive mandatory DoD sponsored Privacy Act and PII protection and spillage training annually to help safeguard the PII.

DCAA provides mandatory Information Awareness training for all employees and all contractors. This training includes safe handling procedures that cover receiving, viewing, printing, forwarding, storing, and shredding of PII data.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

Within the DoD Component.

Specify.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify.

N/A

Other (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

Yes

No

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Users have the opportunity to object at the time of collection.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

Yes

No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

Individuals have the opportunity to give or withhold their consent at the time of collection.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|---|--|
| <input type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input checked="" type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

Any PII data that will be collected would be by a Federal Government Form or document that contains a Privacy Act statement or Advisory In accordance with the applicable regulations.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

- | | | |
|---|---|--|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Other Names Used | <input checked="" type="checkbox"/> Social Security Number (SSN) |
| <input type="checkbox"/> Truncated SSN | <input type="checkbox"/> Driver's License | <input type="checkbox"/> Other ID Number |
| <input type="checkbox"/> Citizenship | <input type="checkbox"/> Legal Status | <input type="checkbox"/> Gender |
| <input type="checkbox"/> Race/Ethnicity | <input type="checkbox"/> Birth Date | <input type="checkbox"/> Place of Birth |
| <input type="checkbox"/> Personal Cell Telephone Number | <input type="checkbox"/> Home Telephone Number | <input type="checkbox"/> Personal Email Address |
| <input type="checkbox"/> Mailing/Home Address | <input type="checkbox"/> Religious Preference | <input type="checkbox"/> Security Clearance |
| <input type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> Mother's Middle Name | <input type="checkbox"/> Spouse Information |
| <input type="checkbox"/> Marital Status | <input type="checkbox"/> Biometrics | <input type="checkbox"/> Child Information |
| <input type="checkbox"/> Financial Information | <input type="checkbox"/> Medical Information | <input type="checkbox"/> Disability Information |
| <input type="checkbox"/> Law Enforcement Information | <input type="checkbox"/> Employment Information | <input type="checkbox"/> Military Records |
| <input type="checkbox"/> Emergency Contact | <input type="checkbox"/> Education Information | <input type="checkbox"/> Other |

If "Other," specify or explain any PII grouping selected.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

PII is collected from the individual and existing DoD information systems or forms.

(3) How will the information be collected? Indicate all that apply.

- | | |
|--|---|
| <input checked="" type="checkbox"/> Paper Form | <input checked="" type="checkbox"/> Face-to-Face Contact |
| <input type="checkbox"/> Telephone Interview | <input type="checkbox"/> Fax |
| <input type="checkbox"/> Email | <input type="checkbox"/> Web Site |
| <input type="checkbox"/> Information Sharing - System to System | |
| <input checked="" type="checkbox"/> Other | |

Flat file transfer from other DoD information systems.

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

To process time keeping.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

PII within DMIS is strictly limited to mission and administrative use.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

- Yes** **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

- Users**
- Developers**
- System Administrators**
- Contractors**
- Other**

If "Other," specify here.

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

- Security Guards**
- Identification Badges**
- Key Cards**
- Safes**
- Cipher Locks**
- Combination Locks**
- Closed Circuit TV (CCTV)**
- Other**

If "Other," specify here.

(2) Technical Controls. Indicate all that apply.

- User Identification**
- Password**
- Intrusion Detection System (IDS)**
- Encryption**
- External Certificate Authority (CA) Certificate**
- Other**
- Biometrics**
- Firewall**
- Virtual Private Network (VPN)**
- DoD Public Key Infrastructure Certificates**
- Common Access Card (CAC)**

Host Based Intrusion Prevention.

(3) Administrative Controls. Indicate all that apply.

- Periodic Security Audits**
- Regular Monitoring of Users' Security Practices**
- Methods to Ensure Only Authorized Personnel Access to PII**
- Encryption of Backups Containing Sensitive Data**
- Backups Secured Off-site**
- Other**

If "Other," specify here.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

Yes. Indicate the certification and accreditation status:

- | | | | |
|-------------------------------------|--|----------------------|---|
| <input checked="" type="checkbox"/> | Authorization to Operate (ATO) | Date Granted: | <input type="text" value="01/30/2013"/> |
| <input type="checkbox"/> | Interim Authorization to Operate (IATO) | Date Granted: | <input type="text"/> |
| <input type="checkbox"/> | Denial of Authorization to Operate (DATO) | Date Granted: | <input type="text"/> |
| <input type="checkbox"/> | Interim Authorization to Test (IATT) | Date Granted: | <input type="text"/> |

No, this DoD information system does not require certification and accreditation.

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Each user or process is authorized the most restrictive set of privileges or access needed for the performance of authorized tasks.

Information system owners identify authorized users and their respective access authorizations. Emergency and temporary access authorizations to the information system are explicitly approved by designated organization officials, monitored, and removed as soon as no longer required

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

Individual data owners, systems administrators, and database administrators are responsible to manage and secure any PII data which reside in DMIS.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

Describe here.