



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

DCAA Integrated Information Network (IIN)
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.

-Federal Records Act (FRA), 44 U.S.C. Chapters 21, 29, 31 and 33.  
-Responsibility for custody, use, and withdrawal of records, 44 U.S.C. 2108  
-Inspection of agency records, 44 U.S.C. 2906  
-Restrictions On The Use Of Records, 36 CFR §1256 OMB Circular A-130, "Management of Federal Information Resources  
- 36 CFR Subchapter B  
-DoD Directive 5015.2, Records Management Program

**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.

DCAA IIN is a office automation environment where user groups are able to store and retrieve electronic files.

The DCAA IIN contains two (2) general categories of information about individuals:

Information about users of the system; account information, audit trail information, and Information contained in records and other documentary materials received, for storage in the DCAA, from various sources, e.g.. DoD Agencies, DCAA Field Offices, and other Federal Agencies.

(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 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, roles based security model. The number of necessary users with access to the documents that contain PII is kept to a minimum by close monitoring of the role allocation.

Administrative access to the IIN 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 Top Secret clearance as per DoD policy.

Access to DCAA IIN 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.

N/A

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

Specify.

N/A

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

Specify.

N/A

**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, the IIN does not collect PII, but may contain records that collect Privacy Act data as a part of a business process.

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

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.

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

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

The data elements obtained vary greatly depending on individual data owner needs.

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

The DCAA IIN was not designed to collect or extract personally identifiable information subject to the provisions of the Privacy Act of 1974, as amended. However, personally identifiable information may be introduced into the system by an individual user in the course of performing his or her duties, and such information may be covered by a system of records applicable to that office, function, or individual. NARA has not published a system of record notice covering this random occurrence of personally identifiable information in the system. Moreover, no such notice is required.

It should be noted that some personally identifiable information in IIN may be covered by one or more Privacy Act system of records notices.

RDCAA 152.1 The Enhanced Access Management System (TEAMS)

RDCAA 152.2 Personnel Security Data Files  
RDCAA 215.1 Voluntary Leave Transfer Program  
RDCAA 240.3 Legal Opinions  
RDCAA 240.5 Standards of Conduct, Conflict of Interest  
RDCAA 358.3 Grievance and Appeal Files  
RDCAA 367.5 Employee Assistance Program (EAP) Counseling Records  
RDCAA 590.8 DCAA Management Information Systems (DMIS)  
RDCAA 590.14 Access Request Records

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

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

If "Other," describe here.

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

Any Privacy Act data contained in DCAA IIN are for the business purposes of the individual data owner. DCAA IIN is designed to provide controlled access to data by authorized users who are the owners of the data. The system serves as a office automation environment and does not contain personally identifiable information (PII). Individual data owners are responsible to manage and secure any PII data that resides in the DCAA IIN according to agency directives.

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

Any Privacy Act data contained in DCAA IIN is collected for administrative purposes. The system does not have any mechanisms designed to recognize, process, or extract PII data.

**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.

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> <b>Security Guards</b>       | <input checked="" type="checkbox"/> <b>Cipher Locks</b>      |
| <input checked="" type="checkbox"/> <b>Identification Badges</b> | <input checked="" type="checkbox"/> <b>Combination Locks</b> |
| <input type="checkbox"/> <b>Key Cards</b>                        | <input type="checkbox"/> <b>Closed Circuit TV (CCTV)</b>     |
| <input checked="" type="checkbox"/> <b>Safes</b>                 | <input type="checkbox"/> <b>Other</b>                        |

If "Other," specify here.

**(2) Technical Controls.** Indicate all that apply.

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> <b>User Identification</b>                  | <input type="checkbox"/> <b>Biometrics</b>  |
| <input checked="" type="checkbox"/> <b>Password</b>                             | <input checked="" type="checkbox"/> <b>Firewall</b>                                   |
| <input checked="" type="checkbox"/> <b>Intrusion Detection System (IDS)</b>     | <input checked="" type="checkbox"/> <b>Virtual Private Network (VPN)</b>              |
| <input checked="" type="checkbox"/> <b>Encryption</b>                           | <input checked="" type="checkbox"/> <b>DoD Public Key Infrastructure Certificates</b> |
| <input type="checkbox"/> <b>External Certificate Authority (CA) Certificate</b> | <input checked="" type="checkbox"/> <b>Common Access Card (CAC)</b>                   |
| <input type="checkbox"/> <b>Other</b>   |   |

If "Other," specify here.

**(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"/> | <b>Authorization to Operate (ATO)</b>            | <b>Date Granted:</b> | <input type="text" value="03/14/2014"/> |
| <input type="checkbox"/>            | <b>Interim Authorization to Operate (IATO)</b>   | <b>Date Granted:</b> | <input type="text"/>                    |
| <input type="checkbox"/>            | <b>Denial of Authorization to Operate (DATO)</b> | <b>Date Granted:</b> | <input type="text"/>                    |
| <input type="checkbox"/>            | <b>Interim Authorization to Test (IATT)</b>      | <b>Date Granted:</b> | <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 designed organization officials, monitored, and removed as soon as not 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 are responsible to manage and secure any PII data which reside in IIN.

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

Describe here.