PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

IDENTICARD SYSTEMS RECORDS

2. DOD COMPONENT NAME:

Department of Defense Inspector General

3. PIA APPROVAL DATE:

11/28/17

Mission Support Team, Office of Security

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [x] From Federal employees and/or Federal contractors
- [ ] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

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

Identicard Systems Records are collected and maintained by DOD OIG Office of Security to manage the issuance of credentials to DoD OIG employees. Credentials are issued only to full time employees who are permanently assigned to the DOD OIG. The credentials authorize the employee access to all DoD facilities, records, and information to perform law enforcement and other official activities, as required under the IG Act (5 U.S.C Appendix 3). Information collected to produce credentials is limited to name, truncated social security number, job title, security clearance, and a photo for the credential. Security also uses the Indenticard system to produce Law Enforcement (LE) Officer Identification Cards for Separating/Retired Law Enforcement Officials IAW Law Enforcement Officers Safety Act. For retired LE Identification badges additional PII is collected to confirm eligibility, including SF-50 showing retirement and NCIS check.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

Mission-related use - PII is collected to produce credentials that authorize the employee access to DoD facilities, records, and information necessary to perform their official activities and the IG mission.

Administrative - Credentialing program allows the security office to activate and revoke access based on an individual's status and duties.

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

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

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Individuals may object to the collection of their PII, but it is necessary to collect PII in order to produce the DoD OIG credential, retired law enforcement officer identification card, or courier card.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] No

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

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

Information is collected and maintained in accordance with all applicable rules and regulations as required to carry out the mission of the DOD OIG under the IG Act.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

- [x] Privacy Act Statement
- [ ] Privacy Advisory
- [ ] Not Applicable

Individuals who provide PII directly to Office of Security are informed either through a Privacy Act Statement or verbal advisement that the information is being collected in connection with official business, such as, an investigation or personnel management functions, and that the information collected may be used in furtherance of other official matters consistent with the purpose for which the information was collected.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

[X]	Within the DoD Component	Specify.	DOD OIG Office of Security
[ ]	Other DoD Components	Specify.	
[ ]	Other Federal Agencies	Specify.	
[ ]	State and Local Agencies	Specify.	
[ ]	Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	
[ ]	Other *(e.g., commercial providers, colleges).*	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

- [X] Individuals
- [ ] Existing DoD Information Systems
- [ ] Other Federal Information Systems
- [ ] Databases
- [ ] Commercial Systems

-DoD OIG Credentials and courier cards - Individual provides all information

-Law Enforcement Officer Identification Card (Separated) - Individual provides most information to component, who may add other required documentation, such as National Investigative Service Check and SF-50, to complete Action Memo necessary for verification of eligibility.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [ ] E-mail
- [ ] Face-to-Face Contact
- [ ] Fax
- [ ] Information Sharing - System to System
- [ ] Other *(If Other, enter the information in the box below)*
- [ ] Official Form (*Enter Form Number(s) in the box below)*
- [X] Paper
- [ ] Telephone Interview
- [ ] Website/E-Form

k. 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 must be consistent.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier CIG-22

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. GRS 5.6, Item 120

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Destroy mandatory and optional data elements housed in the agency identity management system and printed on the identification card 6 years after terminating an employee or contractor's employment, but longer retention is authorized if required for business use.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

1) Public Law 95-452 as amended, Inspector General Act of 1978, § 2;

2) 10 U.S. Code § 1585a, "Special agents of the Defense Criminal Investigative Service: authority to execute warrants and make arrests";

3) Department of Defense Directive (DoDD) 5210.56, "Arming and Use of Force," dated November 18, 2016;

4) Department of Defense Instruction (DoDI) 5525.12, "Implementation of the Amended Law Enforcement Officers Safety Act of 2004 (LEOSA)," dated February 13, 2014;

5) DoDD 5525.12, "Implementation of the Law Enforcement Officers Safety Act of 2004," dated September 14, 2011.

6) Inspector General Instruction 5200.3, "Credential Program," dated Oct 7, 2011.

7) Law Enforcement Officers Safety Act of 2004, 108 Pub. L. 227 as amended by the Law Enforcement Officers Safety Act Improvements Act of 2010, Pub. L 111-272

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

OMB control number not required, system does not collect records from 10 or more members of the public in a 12-month period.