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:

ServiceNow Cloud Platform

2. DOD COMPONENT NAME:

Department of Defense Inspector General

3. PIA APPROVAL DATE:

12/11/2024

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.

ServiceNow is an enterprise solution that supports the DoD OIG Office of the Chief Information Officer in streamlining information technology (IT) service management. ServiceNow allows for a seamless ticketing, process, and dashboard capability to support service desk and IT operations. ServiceNow provides a self-service ticketing system that assists in processing and cataloging IT customer service requests for access to DoD OIG resources, services, information systems, and databases to support mission accomplishment. ServiceNow collects privacy-related information to properly route tickets and resources to the appropriate individuals. It also provides oversight of DoD OIG users by maintaining user access requests, attempts to access, granting of access, user agreements, and all associated record of user actions. ServiceNow is built on modern web and cloud based technologies. The platform includes easy-to-use, point-and-click customization tools to help DoD OIG users create solutions for unique business requirements. The following PII is collected to send automated electronic mail to the user that will inform them of their ticket status: user ID, first, middle, and last name, work or personal email address, and employee number (EDIPI). Other privacy-related information collected can include: name of manager, gender, title, geo-location, internet protocol (IP) address, address, department, country, telephone numbers (business, home, and mobile), and education status.

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)*

PII is collected for identification, authentication, and administrative use purposes. PII is required to track user access to systems, applications, databases, and other digital technologies controlled by the DoD OIG. ServiceNow also serves as an accountability mechanism that will allow for a seamless ticketing, process, and dashboard tracking capability for service desk operations.

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.

Users consent to the capture and use of their PII at the time of employment. Prior to the collection of PII, users are provided the appropriate Privacy Act Statement via IG Form 21, Network Access User Agreement, and DD Form 2875, System Authorization Access Request. Users are given an opportunity to object to any collection of PII at that time. However, if the requested information is not provided, the potential user will not receive access to the system to perform their duties in support of the DoD OIG mission.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [x] Yes [ ] 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.

Users consent to the capture and specific uses of their PII upon completion of IG Form 21 and DD Form 2875 for account creation and access. However, if the requested information is not provided, the potential user will not receive access to the system to perform their duties in support of the DoD OIG mission.

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

Users are provided a Privacy Act Statement (PAS) when the IG Form 21 and DD Form 2875 are completed. Otherwise, the following PAS applies:

AUTHORITY: Public Law 99-474, the Computer Fraud and Abuse Act.
PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information.
ROUTINE USE: In addition to the disclosures permitted by 5 U.S.C. 552a, Section (b), Conditions of Disclosure, information may also be disclosed for any of the reasons listed in System of Records Notice DoD-0015, Enterprise Identity, Credential, and Access Management Records, from the Office of the Secretary, published in the Federal Register (FR) at 87 FR 241 and DoD-0019, Information Technology Access and Audit Records, from the Office of the Secretary, published at 88 FR 169.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of the submitted request.

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 employees with a need-to-know
[X] Other DoD Components	Specify.	As listed in the applicable SORN.
[X] Other Federal Agencies	Specify.	As listed in the applicable SORN.
[X] State and Local Agencies	Specify.	As listed in the applicable SORN.
[X] 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.	CONTRACTOR: Carahsoft Technology Corp. The contract contains privacy provisions for Privacy Act compliance, mandatory PII training completion, and caution on disclosure of information.
[ ] 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 [ ] Databases
[X] Existing DoD Information Systems [ ] Commercial Systems
[ ] Other Federal Information Systems

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

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

- System-to-system within the DoD OIG NIPRnet.
- IG Form 21 and DD Form 2875.

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 DoD-0015 and DoD-0019.

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 3.2 items 30 & 31

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

(3) Retention Instructions.

Item 30 -- Destroy when business use ceases.
Item 31 -- Destroy 6 years after password is altered or user account is terminated, 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.

10 U.S.C. 134, Under Secretary of Defense for Policy;
Executive Order (EO) 10450, Security Requirements for Government Employment;
EO 9397, Numbering System for Federal Accounts Relating to Individual Persons, as amended;
Public Law 99-474, Computer Fraud and Abuse Act of 1986;
DoD Directive (DoDD) 5101.1, DoD Executive Agent;
DoDD 5105.65, Defense Security Cooperation Agency (DSCA);
DoDD 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation; and
DoD Instruction 8500.01, Cybersecurity.

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.

[X] 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.

DD Form 2875, System Authorization Access Request (SAAR)
OMB No. 0704-0630
OMB approval expires: 20250531