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

2. DOD COMPONENT NAME:

Defense Security Cooperation Agency

3. PIA APPROVAL DATE:

01/24/22

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
- [ ] From Federal employees and/or Federal contractors
- [x] 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)*

- [x] New DoD Information System
- [ ] New Electronic Collection
- [ ] 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 a cloud-based workflow automation platform that enables enterprise organizations to improve operational efficiencies by streamlining and automating routine work tasks. ServiceNow serves as a help desk, ticketing and catalog system, Portfolio and Project Management and Knowledge Management system, currently hosted on Government Community CLoud (GCC). The following PII is collected in the system: User ID (firstname.lastname), first name, middle name, last name, name of manager, gender, photograph, title, geolocation, address, department, country, telephone numbers (business, home and mobile), email address, employee number (EDIPI), education status, etc.

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)*

This PII is collected for identification, authentication, and administrative use purposes.

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.

Employees implicitly consent to the capture and use of their PII at the time of employment. Prior to the collection of PII, users are provided appropriate Privacy Act Statement via DD Form 2875 and 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.

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 implicitly consent to the capture and specific use of their Pll upon completion of 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.

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.)*

☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

Upon the collection of PII, individuals subject to the Privacy Act are provided appropriate Privacy Act Statements. For access, DD Form 2875, System Authorization Access Request (SAAR) is completed, and the form includes the following Privacy Act Statement:

Authority: Executive Order 10450, 9397; and 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. NOTE: Records may be maintained in both electronic and/or paper form.

Routine Use: None.

Disclosure: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this 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)*

☒ Within the DoD Component	Specify.	Defense Security Cooperation Agency
☐ 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.	CONTRACTOR: ServiceNow The contract contain provisions to ensure the confidentiality and security of PII are in place to manage data risks, including language addressing the completion of orientation and annual privacy training for contractor employees. See Privacy Clauses 52.224-1, 52-224-2 and 52-224-3.
☐ 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)*

☒ Individuals ☒ Databases

☒ Existing DoD Information Systems ☐ Commercial Systems

☒ Other Federal Information Systems

DSCA systems and locations such as - DSAMS, SCIP, JSP SharePoint, DAI, DSCA Mechanicsburg Active Directory, AWS Okta users, Socium, ISG, CWD, DSCUW, HTDC, etc.

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
- [x] Other *(If Other, enter the information in the box below)*
- [ ] Official Form (*Enter Form Number(s) in the box below)*
- [ ] Paper
- [ ] Telephone Interview
- [x] Website/E-Form

Production Instance:
User Records will be automatically created by an integration with DSCA OKTA.

All PII Fields that are needed in ServiceNow exist in OKTA and will be pushed automatically into ServiceNow from OKTA on a schedule.

All group membership data will be created/managed/updated in OKTA and will be pushed automatically into ServiceNow on a schedule.

All roles will NOT be added in OKTA. Instead, they will be manually assigned to groups in ServiceNow, and users will inherit their roles from the groups which they are members of.

Dev/Test:
Most Users and Groups will function identically as production.

Exceptions: Some users may be manually granted additional groups and roles in the Test environment for the purpose of testing new functionality.

Some Groups may be manually created in the Dev. Environment for the purposes of development and testing. These can be pushed into the test environment through an automated tool that uses “Update Sets” to capture all development code and data.

Once all the Code has been tested, demonstrated, and approved, we will NOT be using update sets to add the groups to Production. Instead, we will use the Request Process + SAAR process to have the groups added to OKTA via Service Desk. This will then update the production environment automatically on a schedule.

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: Pending OATSD-PCLT Confirmation

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. 5.8, item 010 (DAA-GRS

(2) If pending, provide the date the SF-115 was submitted to NARA. 12/2/2021

(3) Retention Instructions.

Program Manager for the IT system ServiceNow has been directed to complete SD Form 828 for determination of disposition. Request has been submitted to OSD/WHS Records Manager. Technical and Administrative Help Desk Operational Records DESCRIPTION: Records related to technical and administrative help desk operations.

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; 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; DoD Instruction 8550.01, DoD Internet Services and Internet-Based Capabilities; Executive Order 10450, 9397 and Public Law 99-474.

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.

This system will not require OMB clearance since it is not the entry point for the information being collected and the data is coming from other systems.