PRIVACY IMPACT ASSESSMENT (PIA)

For the

Intranet Services (IS)/iComplaints
Defense Information Systems Agency (DISA)

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**	☐	**New Electronic Collection**
☒	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

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	814
☐	**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 K890.16

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.

The following authority allows iComplaints to collect the following data:

- MEMORANDUM FOR SERVICES DIRECTORATE: SUBJECT: (U) Interim Authorization to Operate (IATO) for DISA Intranet Services, eMASS System ID 13, DITPR ID 814

- 10 U.S.C. Chapter 8: DoD Directive 5109; Defense Information Systems Agency (DISA)

- DoD Instruction (DoDI) 8510.01; SUBJECT: Risk Management Framework (RMF) for DoD Information Technology (IT)

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.

DISA Intranet Services (IS) provides DISA employees with web-based technologies that integrate information from many disparate applications and services and presents it to users via a consistent user interface. One of the these applications is the iComplaint system. Although the PII assessment title is IS, all the data presented is specifically for the iComplaint system.

The iComplaints system is an enterprise-level application that provides all necessary capability to collect, track, manage, process, and report on DISA Equal Employment Opportunity (EEO) discrimination complaint cases, via a web-based interface. The system contains information pertaining to applicants who file a formal or internal EEO complaint.

The type of Personally Identifiable Information (PII) collected is personal, employment, and work.

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

Safeguards are implemented to detect and minimize unauthorized disclosure, modification and/or destruction of data, therefore, the risk impact to an individual's privacy is believed to be minimal. The iComplaints system is protected by firewalls, host-based security, encrypted traffic to and from data repositories, and by an SSL-enabled front-end proxy.

Data at rest within iComplaints user repositories is further protected by Transparent Data Encryption. The iComplaints application is CAC-enabled and username/password protected, requiring both a valid CAC (Common Access Card) and valid iComplaints login credentials to access the system. The system is only accessible from the DISANET network, which provides another layer of security.

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. Defense Information Systems Agency (DISA)

☒ **Other DoD Components.**

Specify. Defense Criminal Investigation Service

☒ **Other Federal Agencies.**

Specify. Equal Employment Opportunity Commission (EEOC)

☐ **State and Local Agencies.**

Specify.

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

Specify. Nova Corporation There is no contract language in the PWS specifically concerning PII, there is this statement, but it refers to the Privacy act of 1974 (see section 2.K).

☐ **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.

Entry of PII is a necessary condition of involvement for an EEO complaint. Individuals involved with an EEO complaints will be made aware, through an interview process, that they are voluntarily providing PII when they submit this complaint. Individuals have the right to refuse disclosure and halt the complaint process at any time, up to the point when/if civil litigation begins; the PII would then become part of the legal case file.

(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 are made to understand, through an interview process, that they are providing PII voluntarily for an EEO complaint.

(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.

☒	**Privacy Act Statement**	☐	**Privacy Advisory**
☐	**Other**	☐	**None**

Describe each applicable format.

A hard copy of the Privacy Act Statement describing the DISA practices regarding the use, maintenance, and collection of PII is provided to the individual submitting the complaint.

The Privacy Act of 1974 applies. The Contractor may be required to have access to highly sensitive and proprietary information for the performance of this Task Order. The Contractor shall not divulge any information about data processing activities or functions, or any other knowledge that may be gained, to anyone who is not authorized to have access to such information. The Contractor shall observe and comply with the security provisions in effect at computer centers. Any required identification badges shall be worn and displayed at all times. A Department of Defense Contract Security Classification Specification, Form DD 254, must be completed. A DISA Non-Discloser Agreement (NDA) must be completed by each employee prior to commencement of work.

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.