



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Knowledge Network (K-NET)

Department of the Navy - DON/AA - NCIS

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.

10 U.S.C. 5013, Secretary of the Navy; 18 U.S.C. 2510-2520 and 3504; 47 U.S.C. 605; DoD Directive 5210.48, Polygraph and Credibility Assessment Program; DoD Regulation 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons; DoD Directive 5505.9, Interception of Wire, Electronic, and Oral Communications for Law Enforcement; Secretary of the Navy Instruction 5430.107, Mission and Functions of the Naval Criminal Investigative Service; Secretary of the Navy M-5510.30, Department of the Navy Personnel Security Program; Secretary of the Navy M-5510.36, Department of the Navy Information Security Program; OPNAVINST 5530.14, Navy Physical Security and Law Enforcement; MCO 558.2, Law Enforcement Manual; E.O. 10450, Security Requirements for Government Employees, in particular sections 2, 3, 4, 5, 6, 7, 8, 9, and 14; E.O. 12333, United States Intelligence Activities and E.O. 9397 (SSN) as amended.

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.

The NCIS Knowledge Network (KNET) is a system that provides complete end-to-end unclassified knowledge management capability to users. KNET provides integrated analytical and knowledge management capabilities across multiple internal and external sources of criminal investigative, counterintelligence, and counterterrorism. More specifically, KNET consists of tools that allow users to search unclassified disparate data sources from one common interface, perform entity extraction of key objects and concepts contained in message traffic and databases, visualize relationships between objects, collaborate, and report.

KNET provides users access to the following type of information, which may or may not include personal information: Official law enforcement investigative reports prepared by NCIS, DON, Department of Defense (DoD), or other Federal, state, local, tribal, or foreign law enforcement or investigative bodies. Biographic data, intelligence/counterintelligence debriefing reports, information concerning subjects and/or co-subjects of investigations. The information may be of criminal, counterintelligence, or general investigative interest. It is important to note that this data originates in other IT systems and applications. For example, investigative reports data is obtained via an interface with NCIS Case Management System. KNET also retrieves information from the National Law Enforcement Telecommunication System (NLETS) which is the pre-eminent interstate law enforcement network in the nation for the exchange of law enforcement and related justice information.

The PII that can be accessed via KNET includes: Name, Citizenship, Race/Ethnicity, Mailing/Home Address, Marital Status, Law Enforcement Information, Other Names Used, Driver's License, Birth Date, Biometrics, Employment Information, Social Security Number, Other ID Number, Gender, Place of Birth, Security Clearance and Military Records.

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

The perceived threats are primarily computer hackers, disgruntled employees, state sponsored information warfare, and acts of nature (e.g., fire, flood). All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that KNET, with its extensive collection of PII, could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA are in place. Since KNET operates on NMCI Network, there is a risk that security controls could be disabled for maintenance and other purposes. The risk would be that the security controls would not be reset. All systems are vulnerable to "insider threats". KNET administrators are vigilant to this threat by limiting access to those individuals who have a defined need to access the information. There are defined criteria to identify who should have access to KNET. These individuals have gone through extensive background and employment investigations.

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.

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

Specify.

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.

(2) If "No," state the reason why individuals cannot object.

KNET does not collect PII directly from the individual. PII is collected from an originating source, such as an official investigative report. KNET interfaces with other IT systems (i.e., NCIS Case Management System and National Law Enforcement Telecommunications System) and provides users access to such reports in order to integrate analytical and knowledge management capabilities across multiple internal and external sources of criminal investigative, counterintelligence, and counterterrorism. This allows users to collaborate better and develop relationships between various sources of information.

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.

[Empty rectangular box]

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

KNET does not collect PII directly from the individual. PII is collected from an originating source, such as an official investigative report. KNET interfaces with other IT systems (i.e., NCIS Case Management System and National Law Enforcement Telecommunications System) and provides users access to such reports in order to integrate analytical and knowledge management capabilities across multiple internal and external sources of criminal investigative, counterintelligence, and counterterrorism. This allows users to collaborate better and develop relationships between various sources of information.

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.

KNET does not collect PII directly from the individual.

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.