



PRIVACY IMPACT ASSESSMENT (PIA)

For the

| |
|---|
| Sensormatic Electronics CCURE 800 (CCURE) |
|---|

| |
|---|
| Department of the Navy - NAVAIR - FRC Southeast, Jacksonville, FL |
|---|

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
- 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.

SORN authorities:

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
OPNAVINST 5530.14C, Navy Physical Security
Marine Corps Order P5530.14, Marine Corps Physical Security Program Manual
E.O. 9397 (SSN), as amended
5 U.S.C.301, Departmental Regulations; 10 U.S.C. 113, Secretary of Defense

10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 8013, Secretary of the Air Force; DoD Directive 8521.01E, Department of Defense Biometrics; DoD Directive 8500.1, Information Assurance (IA); DoD Instruction 8500.2, Information Assurance Implementation; Army Regulation 25-2, Information Assurance; DoD Directive 2310.7, Personnel Accounting-Loses Due to Hostile Acts; DoD Directive 5110.10, Defense Prisoner of War/Missing in Action Office; DoD Instruction 2310.5, Accounting for Missing Persons; and E.O.9397 (SSN).

5 U.S.C. 301 Departmental regulations; 10 U.S.C. 113, Secretary of Defense, Note at Pub.L. 106-65; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 18 U.S.C. 1029, Fraud and

related activity in connection with access devices; 18 U.S.C. 1030, Fraud and related activity in connection with computers; 40 U.S.C. Chapter 25, Information technology management; 50 U.S.C. Chapter 23, Internal Security; Pub.L. 106-398, Government Information Security Act; Pub.L. 100-235, Computer Security Act of 1987; Pub. L. 99-474, Computer Fraud and Abuse Act; ; E.O. 12958, Classified National Security Information as amended by E.O., 13142 and 13292; E.O. 10450, Security Requirements for Government Employees; and E.O. 9397 (SSN).

10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; and E.O. 9397 (SSN).

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 CCURE System provides remote entry/exit monitoring, video surveillance, badge-activated access, and alarm capabilities (the Intrusion Detection System (IDS)) at various buildings at Fleet Readiness Center-Southeast, NAS, Jacksonville, FL, and In Service Support Center-Jacksonville, Cecil Commerce Center, Jacksonville, FL. CCURE consists of a network of electronic door switches, badge readers, and video cameras which provide input to a central server, for processing by the software. Data provided by input devices is then transmitted to NMCI computers at manned security points. Data is also recorded to an internal database; with video input recorded on tape, to be used for statistical information on personnel access to controlled areas, and investigative purposes. Badge readers and sensors permit access of authorized personnel to controlled areas, relay door status, intrusion detection and alarms to the server. This information is relayed to NMCI computers at manned security points to facilitate real-time electronic monitoring of unmanned access points and buildings. System is monitored around-the-clock to enable immediate response in case of unauthorized access.

Personal Information consist of: Full name, truncated SSN, DoD ID number, employee number, citizenship, legal status, birth date, Driver license number, home address, employment information: local department, code, and office contact information; emergency contact, personal cell phone number, spouse information: name, age, and marital status; home telephone number.

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

Identity theft: This system is locked down by permissions only and no one has access to PII except for a few high level personnel with a need to know. The CCURE software requires a username and password and the computer is PKI protected and the data is encrypted. Upon entry of the system a banner identities a Privacy Act Statement notifying individuals that the system contains PII information and their responsibility to maintain.

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.

Employees, contractors, and visitors may object verbally, but access to FRCSE spaces would be denied.

(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.

Employees, contractors, and visitors may object verbally, but access to FRCSE spaces would be denied.

[Empty rectangular box]

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

[Large empty rectangular box for providing reasons]

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.

Privacy Act Statement on Form 5500-17, Visit Request

[Large empty rectangular box for describing applicable formats]

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.