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:

SENSORMATIC ELECTRONICS CCURE 9000

2. DOD COMPONENT NAME:

Department of the Navy

3. PIA APPROVAL DATE:

NAVAIRSYSCOM / (FLEET READINESS CENTER SOUTHEAST (FRC SE))

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
- [ ] Existing DoD Information System
- [x] 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.

Shore Application-- Machine Specific. Public Safety Devices 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.

System 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 whose central server is located at the command's server farm at Fleet Readiness Center South East, NAS Jacksonville, FL. The 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. The CCURE server is within the command's accreditation boundary and is included in the CCURE ATO package (emass #4446).

PII collected from military and civil service only consist of: Full name, date of birth, photo, citizenship, employment information to include rank/grade, employee's home/mailing address, home and official duty telephone number(s), emergency contact information, employment information: Supervisor name and work phone number is collected and other information: Spouse information may be collected if applicable for access to controlled FRCSE spaces. PII collected from DoD Contractors only consist of: Name, home/mailing address, telephone number, employer name and emergency contact name and telephone number. We also collect vehicle tag number and make/model of vehicle for authorized parking registration purposes to all these individuals who need it.

Records Management Information: This application will maintain personnel security records. CCURE application collects and maintains facility access control lists.

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)*

Identification, verification, authentication and access control of individuals' requirement to access secure spaces from the requesting supervisor for badging activities and vehicle decals.

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

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.

Employees, contractors, and visitors may consent to specific uses verbally.

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

PRIVACY ACT STATEMENT

AUTHORITY: 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps and Marine Corps Order P5530.14, Marine Corps Physical Security Program Manual; and E.O. 9397 (SSN), as amended.
PRINCIPLE PURPOSE: To readily identify all personnel who are allowed to access Naval Air Station Jacksonville and the Fleet Readiness Center Southeast (FRCSE) in the furtherance of the Center's Mission; and to comply, verify and update the Center authorized visitor list in support of administrative and security measures.
ROUTINE USES: Data / information collected and entered into the CCURE application as part of the process for issuing access badges to FRCSE's command facilities.
DISCLOSURE: Furnishing personal information on this form is totally voluntary, but failure to do so may result in disapproval of NAS Jacksonville and entry to the FRCSE's command spaces.

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.	FRCSE Command Security & Supervisory Security Government Personnel Administrators Only. No FRCSE Administrators are DoD Contract personnel.
[ ] 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.	
[ ] 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
[ ] Existing DoD Information Systems
[ ] Commercial Systems
[ ] Other Federal Information Systems

Military/Civil Service Individuals: Personnel fill out the following forms: FRCSE Form 5500.17, FRCSE Visit Access / Badge Request and/or SECNAV Form 5512/1, DON Local Population ID Card/Base Access Pass Registration

DoD Contractors: Information is collected face-to-face verbally from the contractor individual

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

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

E-mail: Encrypted email sent to badging office from supervisors to request badging services for new employees, updates and renewals.
Face-to-Face Contact: Verbal information collected (as applicable) and visual verification of identity from DoD Contractors.

Paper: FRCSE Form 5500.17, FRCSE Visit Access / Badge Request and/or SECNAV Form 5512/1, DON Local Population ID Card/Base Access Pass Registration.

Face to Face: Information is collected face-to-face verbally from the DoD contractor employees.

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 NM5512-2

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. DAA-NU-2015-0005-00

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

(3) Retention Instructions.

Individual Record SSIC: 5500.10b / Large Aggregation Disposition SSIC: 5000-52
Disposition Instruction: TEMPORARY. Cut off at end of calendar year. Destroy 3 years after cutoff.

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. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; OPNAVINST 5530.14E, Navy Physical Security and Law Enforcement Program; Marine Corps Order P5530.14, Marine Corps Physical Security Program Manual; and E.O. 9397 (SSN), as amended.

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.

CCURE does collect PII information from more than 10 DoD Contractors annually. PII collected from DoD Contractors only consist of: Name, home/mailing address, telephone number, employer name and emergency contact name, telephone number, vehicle tag number and make/model of vehicle for authorized parking registration purposes.