



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Sponsorship Verification System (SVS)

USMC, MCAS New River

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.

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
10 U.S.C.5041, Headquarters, Marine Corps
E.O. 9397 (SSN)
MARADMIN 533/08, "Internal Housekeeping"

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 purpose of this system is to verify sponsorship of visiting personnel aboard MCAS New River. Individual personal information being collected is limited to names, vehicle information, drivers license, and law enforcement information.

Other information collected is: date of visit, duration of visit, purpose of visit, on base destination, and organization with which the visitor is affiliated.

The system is CAC authorized and maintained on the Share Portal (2003). Only CAC authorized sponsors may provide information on those being sponsored without physically being at the visitor's center.

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

There are minimal privacy risks to the system. All individuals who have access to the Share Portal have access to the personal information residing on it and could potentially lead to a data compromise. Also, names associated with other individuals could lead to the compromise of another individual's personal information.

In order to safeguard the information, standard operating procedures will be followed to mitigate any privacy risks. Users and database administrators will be designated and those with access will be regularly reviewed in order to determine that they still warrant access to the database. Access to the Share Portal will be limited to individuals with need to know.

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.

If the sponsor objects to providing personal information to the SVS they will be required to be present at the time of registration of their visitors. The same personal information will then be collected and recorded.

(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.

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

The use of the information at the visitor's Center is required. MARADMIN 533/08 requires all visitors provide the aforementioned information in order to be granted base access.

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 will be included on the form and a security screen will be incorporated on the SVS web site for the sponsors to read. Individuals are provided a Privacy Act Statement each time personal information is collected explaining the purpose of the collection.

Systems of Records Notice NM05580-1 Security Incident System (January 9, 2007, 72 FR 959)
AUTHORITY: 10 U.S.C. 5013, Secretary of the Navy: 10 U.S.C. 5041, Headquarters, Marine Corps: and E.O. 9397 (SSN). PRINCIPLE: Individuals involved in or witnessing or reporting incidents requiring the attention of base, station, or activity security personnel. PURPOSE: To track and prosecute offenses, counsel victims, and other administrative actions; to support insurance claims and civil litigation; to revoke base, station or activity driving privileges. ROUTINE USE: May specifically be disclosed outside the DOD as a routine use pursuant to 5 U.S.C. 552a (b)(3). DISCLOSURE is mandatory.

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.