



PRIVACY IMPACT ASSESSMENT (PIA)

For the

OTMFPC Registration Web site

CERDEC - PM C4ISR OTM

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.

Child of Team C4ISR Acquisition Network

10 U.S.C. 3013, Secretary of the Army; Department of Defense Directive 8500.1, Information Assurance (IA); DoD Instruction 8500.2, Information Assurance Implementation; AR 25-1, Army Knowledge Management and Information Technology; Army Regulation 25-2, Information Assurance.

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.

Collect information about persons registering for four C4ISR & Network Modernization events occurring yearly: Mid-Planning Conference, Final Planning Conference, Presentation Days and Range 1 In-Processing. This will be an on-going requirement.

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

Risk: PII location
Mitigation: PII data is maintained in a controlled facility. Physical entry is restricted by the use of locks, guards, and is accessible only to authorized personnel. Facility is equipped with alarms, cameras, and personnel on around the clock.

Risk: Electronic access to records
Mitigation: Access to records is limited to person(s) with an official "need to know" who are responsible for servicing the record in performance of their official duties. Access to computerized data is role-based and further restricted by passwords, which are changed periodically.

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.

Internal use for Joint Base McGuire-Dix-Lakehurst NJ and CERDEC- C4ISR & Net Mod

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.

C4ISR & Net Mod requires event attendees to provide their name so we can identify who they are; their status as a US citizen so they may attend C4ISR & Net Mod events, which require attendees to be US citizens; emergency contact information for attendees safety while on Fort Dix ranges; and drivers license numbers for positive identification at Joint Base MDL controlled access areas.
No internal controls exist to gather PII.

(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.

Without the PII information, the registrant will not be allowed to attend C4ISR & Net Mod events.
No internal controls exist to gather PII

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.

DRIVERS LICENSE INFORMATION
Why do we ask for your driver's license number?
A CAC or Military ID is required for access to Joint Base MDL (McGuire, Dix and Lakehurst). If you do not possess a CAC or Military ID, your Driver's License will be an authorized form of ID during the conference period, whereupon your name and driver's license number will be checked. We request your driver's license number during the registration process to forward to Joint Base MDL security. Your driver's license number will be stored with your account when created, and deleted at the end of the conference. Your driver's license number is not shared with any other agency or organization except Joint Base MDL security.

What if I refuse to provide my driver's license number?
If you desire to not provide your driver's license number, please send your driver's license number to C4ISR & Net Mod by FAX: 609-562-4066 or ENCRYPTED E-MAIL: christy.l.glab.civ@mail.mil

EMERGENCY CONTACT INFORMATION
We request your emergency contact information and medical information during the registration process only to use in case of an emergency during your attendance at our event. Your information will be store with your account when it is created, but not shared with any other agency or organization. It will only be used in the event of an emergency when you are on site at our event.

DATA SECURITY (AFTER EACH WHY STATEMENT)
How secure is this data?
Security during registration is ensured using a 128-bit Secure Socket Layer (SSL) connection. This is the highest industry standard and establishes an encrypted session between your computer and our servers hosted on the .mil domain. We use the same technology that other major companies operating on on the World Wide Web (WWW) use to protect personal information and guard against identity theft. Look for the little yellow padlock at the bottom of your browser window to ensure that you have established a secure connection. No alternate means of registration exists as this is the most secure method of protecting your information.

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.