



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Global Combat Support System - Marine Corps (GCSS-MC)

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.defenseink.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.

- Title 10 US Code 5013, Secretary of the Navy
- Title 10 US Code 5041, Headquarters, Marine Corps
- Deputy Secretary of Defense, "Department of Defense Reform Initiative Directive #54 - Logistics Transformation Plans", 23 March 2000
- ALMAR 006/04, "Marine Corps Logistics Modernization," 2 February 2004
- GCSS-MC, "Capability Development Document," 22 December 2005, Requirements 1004.2, 1004.4, 1004.5, and 1004.6

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.

GCSS-MC is the enterprise-wide portfolio of Marine Corps logistics and Combat Service Support (CSS) IT capabilities designed to support both improved and enhanced Marine Air Ground Task Force (MAGTF) CSS functions, MAGTF Commander and Combatant Commander/Joint Task Force (CC/JTF) combat support information requirements, and eliminate "stovepiped" development of logistics IT systems. GCSS-MC Enterprise Non-Secure Internet Protocol Router Network (NIPRNET) is the primary Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) web accessible, controlled unclassified, logistics portal and processing area for GCSS-MC. It is comprised of those business process capabilities necessary to achieve the requirements outlined in the GCSS-MC/Logistics Chain Management (LCM) Block 1 Capability Development Document (CDD), including Demand Management, Maintenance Management, Inventory Management, Distribution Management, Order Management, Request Management, Warehouse Management, Procurement Management, Asset Management, Task Organization, Customer Management, and Sourcing Management.

The personal information collected about individuals within GCSS-MC Enterprise NIPRNET relates solely to identification and authentication of users accessing the system. This information includes Names, Dates of Birth and Social Security Numbers (SSN) for the purpose of validating the need-to-know of individuals requesting access to GCSS-MC components during the Self-Registration (provisioning) process and the identification and authentication of existing users. This Personally Identifiable Information (PII) is not retrievable in anyway by users and there is no designed functionality for retrieving user information based on a unique identifier. Employment information (MOS, unit, etc.) is also collected and stored via a system interface with the Marine Corps Total Force System (MCTFS), the United States Marine Corps (USMC) authoritative source. This employment data received from MCTFS is refreshed every six months.

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

Privacy risks considered were: (1) unauthorized access to the server and associated database and (2) disclosure of an individual's sensitive information to individuals without a valid need-to-know.

1) The risk of unauthorized access to the server and associated database is addressed to safeguard privacy in multiple layers and reduce the possibility of unauthorized access and reduce the impact if compromised by an attacker. Physical access to GCSS-MC servers and associated databases is controlled via a Defense Information System Agency (DISA) Defense Enterprise Computing Center (DECC) hosting environment. The Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) controls which are negotiated with or inherited from the hosting enclave are enumerated in the GCSS-MC System Security Authorization Agreement (SSAA), Appendix F. Logical access to GCSS-MC Personally Identifiable Information (PII) is not available to the system administrators at the DISA DECC.

System Administrative access to GCSS-MC applications exists for Security and Administrative users from security hardened machines located in the GCSS-MC Operations Center (GOC). Physical access to the GOC is controlled via Proximity card at building access and two separately controlled cipher lock doors. User name and passwords needed to boot machines are held and controlled by GCSS-MC Information Assurance (IA) staff. User name and passwords needed for GOC machine operating system logon is closely controlled and is given to those with a minimum Interim Secret security clearance on a need-to-know basis. Once booted and logged on, a GOC user will connect with the out of band network using a hosting enclave provided user name and password. This is all controlled via the System Authorization Access Request (SAAR) process for system access. Front-end users will access the system from the NIPRNET via a DoD-approved web browser capable of Secure Socket Layer (SSL) v3 or Transport Layer Security (TLS) v1. Front end users will have minimal access to PII consisting only of employment data restricted in scope to only users in their hierarchy, as outlined in GCSS-MC BR.110, "Design Security Profiles".

2) The risk of disclosure of an individual's sensitive information to individuals without a need-to-know is addressed to safeguard privacy by ensuring that sensitive information is only disclosed to individuals with a need-to-know.

This is accomplished by ensuring that sensitive information is limited to the greatest extent possible by any front-end users of the application. Most PII (SSN, Date of Birth, etc) in the GCSS-MC is used exclusively for Identification and Authentication. Other PII (employment data) is used in a limited scope for manpower and utilization purposes. Database Administrators (DBAs) may have the ability to gain access to all PII in the database during user account maintenance, however DBA access is gained in a controlled environment (GOC) and is controlled by the Information Assurance Manager to those with: (1) a valid need-to-know, (2) a minimum of an Interim Secret security clearance, and (3) documented, detailed plans of system work to be performed. Again, employment data may be accessed by a user's administrative hierarchy within GCSS-MC for determining allocation of resources in accordance with the GCSS-MC Role-Based Access Control (RBAC) mechanisms.

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.

During the User Self-Registration process, individuals will be provided with a Privacy Act Statement which states the purpose of privacy act information collection. If a user objects to the collection of their PII, they may disagree with the Privacy Act Statement prior to entering any information by clicking the 'Disagree' button on the Privacy Act Statement page. They will then be directed out of the Self-Registration process and to the Marines.com web site. Disagreeing with the Privacy Act Statement will result in the user not completing the Self-Registration process.

(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.

During User Self-Registration, individuals will be provided with the Privacy Act Statement prior to entering any user information. At this time, individuals can give or withhold their consent by clicking on either the 'I agree' or 'I disagree' buttons on the Privacy Act Statement page.

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

Not Applicable

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.

The Privacy Act Statement is provided to all users who Self-Register to use the system. In order for user to Self-Register they must agree to the Privacy Act Statement, otherwise they will not be granted access. Below is the draft GCSS-MC Privacy Act Statement. If the production version of the PAS changes from the message below, this PIA will be updated accordingly:

* Authority: Title 10 US Code 5013, Secretary of the Navy; Title 10 US Code 5041, Headquarters, Marine Corps; Deputy Secretary of Defense, "Department of Defense Reform Initiative Directive #54-Logistics Transformation Plans", 23 March 2000; ALMAR 006/04, "Marine Corps Logistics Modernization," 2 February 2004; GCSS-MC, "Capability Development Document," 22 December 2005, Requirements 1004.2, 1004.4, 1004.5, and 1004.6.

* Principal Purpose: This information will be used to verify the identity of eligible users of the Global Combat Support System-Marine Corps/Logistics Chain Management Block 1 (GCSS-MC/LCM Block 1) system.

* Routine Uses: None.

* Disclosure: Voluntary. However, failure to provide the requested information will result in denial of access to the GCSS-MC/LCM Block 1 system.

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.