PRIVACY IMPACT ASSESSMENT (PIA)

For the

INNOPORT FAX SOLUTION FOR DOD STOP LOSS MANDATE
United States Marine Corps (USMC)

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 M01040-2 and NM05000-2

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.

1. Executive Order 9397 of 23 November 1943, allows a federal department to utilize social security numbers as account numbers for individual persons;

2.Title 10 USC, Part I, Chapter 506, Section 5041, in that, the Commandant of the Marine Corps will prepare for such employment of the Marine Corps, and for such recruiting, organizing, supplying, equipping (including research and development), training, servicing, mobilizing, demobilizing, administering, and maintaining of the Marine Corps;

3. Title 10 USC 5013, in that the Secretary of the Navy is responsible for, and has the authority necessary to conduct, all affairs of the Department of the Navy, including the following functions: recruiting, organizing, supplying, equipping (including research and development), training, servicing, mobilizing, demobilizing, administering (including the morale and welfare of personnel and maintaining.;

4. SECNAV MEMO - Retroactive Stop Loss Special Pay Compensation, September 23, 2009

5. Public Law 110-329, Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009.

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.

Stop Loss was implemented by the Department of Defense as a means to maintain Subject Matter Experts (SME) and Service Personnel strength to meet new mission requirements caused by the Operations in Iraq and Afghanistan. The March 19th, 2009 Office of the Under Secretary for Defense Memorandum, "Retroactive Stop Loss Special Pay Compensation," mandates that stop loss eligible personnel should be notified that there is a potential for Retroactive Stop Loss Pay, reflect the estimated number of eligible months and the projected special pay amount. The memo also requires evidentiary documents be provided for recordkeeping. Lastly, the memo directs secretaries to establish claim and appellate procedures, websites, points of contact for assistance or other outreach mechanisms to inform and expedite claims. On September 23, 2009, the Secretary of the Navy mandated that the United States Marines Corps provide a mechanism for reimbursement. In order to meet the short time lines of this mandate, the United States Marine Corps chose to utilize Innoport, a third-party company located in King of Prussia, Pennsylvania that provides Secure Fax Capability.

Innoport will provide the following service for the Marine Corps:

(1) Centralized toll-free fax lines that will allow Service Members world-wide to fax their DD-214 (This form proves Service Members eligibility for this entitlement).
(2) Upon Innoport receiving the fax, it is encrypted and submitted via e-mail address owned and controlled by the Marine Corps.
(3) USMC Personnel Administrators will process the forms for reimbursement to the Marine.

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

There is always a risk associated with the handling and transmission of this type of PII data. Service Members will have to find fax machines that may be public (for example, a fax machine at an office supply store). This public environment raises the possibility of a Service Member leaving a copy of their documents behind accidentally. Further, while Innoport's solution provides confidentiality to the document, there is still a risk of data corruption. The confidentiality risk of the data is mitigated largely through Innoport's service offerings (described below). Ensuring that Service Members maintain the original copies of their paperwork for recordkeeping is executed through proper training and messaging. In the event that the transmitted document becomes corrupt, the individual may resubmit their paperwork upon notification.

Another potential privacy risk involves sending a large amount of Marine Corps information through a third-party service provider. While the information will not remain on Innoport's servers longer than 2 days, based on a service agreement signed with the Marine Corps and Innoport. While the temporary storage of Marine Corps information poses a privacy risk, this risk is mitigated by the encryption of the data received by Innoport. No unencrypted data will reside on the Innoport serves.

The following is a description of the Server provided by Innoport:
Secure fax service from Innoport preserves confidentiality of fax documents and gives clients, customers, patients, and health care professionals secure means of communication.
Innoport offers several secure fax solutions, including PDF delivery with 128-bit encryption as well as File Transfer Protocol over Secure Socket Layer (FTPS) fax delivery.
Innoport's fax to e-mail service already eliminates mishandling of faxes off shared fax machines through direct delivery to a private e-mail address. With the advantage of PDF fax encryption, this provides an added layer of security by password-protecting fax documents. Encrypted faxes may only be viewed by supplying the proper password. the Marine Corps has full control on creating and changing the password at anytime for the encrypted

faxes arriving to the Marine Corps e-mail account.

For secure fax sending, Innoport presents web fax service for uploading the files to be faxed through a secure web site. This secure fax solution offers assurance that the contents of the fax transmissions are safeguarded as it passes throughout the Innoport network.

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. Manpower & Reserve Affairs Stop Loss Cell (Marsh Center Personnel)

☐ **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. Innoport Secure Fax Solution.

Contractors have access to privacy data and are bound to the Privacy Act by the terms of the contract. Contractors sign a Non Disclosure Agreement (NDA) to assure confidentiality between the contractor and government to protect any type of confidential and proprietary information. Specific language in the contract is described as:

Security measures shall be taken to satisfy the security requirements in accordance with the Marine Corps System Security Plan. Data/information shall be protected from an Information Systems Security (INFOSEC) perspective. The contractor shall apply security considerations to software design and management.

Only contractors who have a valid need to know and a favorably adjudicated background investigation are permitted to have access to the system. During the course of routine system maintenance contractors may be exposed to PII. Users are DoD employees or authorized contractors supporting the DoD.

☐ **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.

(2) If "No," state the reason why individuals cannot object.

All Marines have been directed to submit stop loss paper work as required by the OUSD and SECNAV Memorandums. The Marine Corps has stipulated the only means of submitting this information is through the Innoport secure fax service, website, or direct delivery. Marines are required to submit this information for purposes of pay and proper military recordkeeping.

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.

PII must be collected to support this Initiative. If an individual were given the opportunity to withhold their consent, they would not receive reimbursement for stop loss.

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 Innoport solution does not provide a Privacy Act Statement, Advisory, or other form of notification to the individual. The forms required for Stop Loss Pay do, however, provide a Privacy Act Statement to the individual marine.

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.