PRIVACY IMPACT ASSESSMENT (PIA)

For the

USMC Fire and Emergency Services Marine Corps Fire Incident Records System (MCFIRS)
Department of the Navy - 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: DADMS: MFC-06-0131857
- ☐ **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: M11320-1

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.

10 U.S.C. 5013, Secretary of Navy
10 U.S.C. 5041, Headquarters, Marine Corps
DoDI 6055.06, DoD Fire and Emergency Services (F&ES) Program
Marine Corps Order 11000.11B, Marine Corps Fire Protection and Emergency Services Program
E.O. 9397 (SSN), as amended.
Health Insurance Portability and Accountability Act (HIPPA)

Department of Defense (DOD) and Marine Corps policy for Fire Protection and Emergency Services require reporting of all emergency and non-emergency incident responses to the National Fire Incident Reporting System (NFIRS). These policy documents further require maintenance of personnel records, training records, equipment inventories, fire prevention inspection reports, and other mission related administrative information, in order to plan, program, budget for and execute the Fire and Emergency Services (F&ES) program effectively.

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 MCFIRS is to provide an electronic records management and reporting system to support emergency response mission and manage day-to-day operations of the USMC Fire and Emergency Services. MCFIRS is designed to organize large volumes of critical information related to data required under the National Fire Incident Reporting System (NFIRS), mission related information regarding personnel, risk response and prevention demographics, apparatus and equipment inventory, fire prevention & inspections, risk management, maintenance, fire hydrants, scheduling, training, and other operational activities. This information is crucial in dispatching emergency apparatus, establishing command at an emergency incident, and running the day-to-day operations of a fire & emergency services organization. The ability to handle large volumes of information directly affects the mission capability of emergency personnel to save lives, reduce property damage and protect the environment. MCFIRS provides real-time information that can be simultaneously shared among different fire and emergency medical services, supervisors, and leadership. In addition, MCFIRS provides an avenue to analyze and respond to Installation Command and HQMC data calls, increases the efficiency and effectiveness of operations, and allows USMC F&ES to meet legal requirements.

MCFIRS will utilize a commercial off-the-shelf product, Emergency Reporting Fire EMS Records Management System from Reporting Systems, Inc.(RSI); DBA Emergency Reporting, www.emergencyreporting.com.

The Emergency Reporting Fire EMS Records Management System is a web based IT subscription service that can be accessed using an internet connection. It leaves no cookies, has no executable files and leaves no footprint on any computer after logging off the web-site.

MCFIRS is separated into two types of users.

• General Users - Use MCFIRS to enter data throughout the different modules. Their ability to access the different modules, run reports, view information, and edit are controlled by fire department administrators.

• Administrators - Have complete control over who can login, control passwords, access modules, define user fields, and limit the ability of each user's privileges in a module to input, view, edit, print, and run reports.

If a user is not given access to a module then the module will not show up when the user logs on.

The concept of operations (CONOPS) of MCFIRS is to access the Emergency Reporting web-site using computers that are connected to the Navy Marine Corps Intranet Network (NMCI) via a web browser. Once at the web-site the user will provide a user name and strong password. Once a user logs in they will access one of 17 modules to dispatch emergency Fire & EMS apparatus to emergency incidents, create Fire & EMS reports, or input data that supports the overall operations of the organization.

PII elements collected are: Name, SSN, Driver's License, Gender, Race, DOB, Personal Cell Phone, Home Phone, Personal Email, Home Address, Medical Information, Employment Information, Military Records, Emergency Contact, Education Information.

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

MCFIRS is subject to a range of generic threats applicable to most government information systems processing PII and other sensitive unclassified information. A potential threat exists to the confidentiality and integrity of the information processed, stored, and transmitted by the system. A potential threat also exists regarding the availability of MCFIRS impacting the execution of the Marine Corps Fire and Emergency Services mission. Potential threats are from natural, environmental, and human sources.

Natural disasters and damage can result from fire, water, wind, and electrical sources. Environmental threats include loss of power or air conditioning. Human threats are from those who would target this system for espionage, criminal activity, unlawful use, denial of service, or malicious harm. Threats from external or internal agents include espionage services, terrorists, hackers, and vandals. Any of these threats could potentially lead to loss of PII.

Statistical analysis of computer-related incidents indicate that the greatest threat to the system is from a trusted agent who has access to the system.

The most likely incident involves an authorized user who accidentally or inadvertently commits or omits some action that damages or compromises the system, one of its components, or information that is processed, stored, or transmitted by the system.

The next most likely incident involves an authorized user who takes deliberate action to damage the system, one of its components, or system data for personal gain or vengeful reasons. Such a person could also engage in espionage, other criminal activity, exploitation, or theft of the assets of the system for personal gain, an example of this would be identity theft.

There is the threat of co-option of users with authorized access to the system, contractor support personnel, or USMC F&ES personnel with physical access to the system components, arising from the motivation of financial gain.

There is the threat posed by disgruntled employees, especially those who are to be terminated for cause.

There is a threat posed by users of the system who negligently or inadvertently fail to follow security requirements for the handling and labeling of system output or media, or the rules against the introduction of authorization software or data.

There is the threat arising from the failure of authorized users to employ proper procedures for the entry or manipulation of system data arising due to failure of users to be properly trained in the use and operation of the system.

Insider threats can be manifested in the following ways:

- The unauthorized reading, copy, or disclosure of PII or sensitive but unclassified information.
- The execution of denial of services attacks.
- The introduction of viruses, worms, or other malicious software into the system.
- The destruction or corruption of data (intentional or unintentional).
- The exposure of PII or sensitive but unclassified data to compromise through the improper labeling or handling of printed output.
- The improper labeling or handling of storage media resulting in the compromise of PII or sensitive but unclassified information.

In order to address these risks the USMC F&ES Department will control access to MCFIRS, restrict module access levels, provide password control for data entry, restrict user defined fields, and provide means to validate entries where possible. A member account sign-up form must be completed and sent to the Administrator for approval. The Administrator will approve all requests for member accounts on a need to know basis.

PII data is displayed on workstation monitors. To avoid compromise, workstation machines will time out and monitors will go dark when periods of inactivity are exceeded. This keeps unattended workstations from being left for long periods with data exposed.

Encryption devices (e.g. software or hardware) will be used whenever PII or sensitive but unclassified information is transmitted between the NMCI network and other networks outside of the boundary. Any information considered to be sensitive will be encrypted during transmission. Secure Socket Layer (SSL) encryption is required on MCFIRS.

Initial and periodic security training and awareness will be provided to users of MCFIRS. The goal of the training is to promote the proper and consistent application by users of the basic security features and procedures to provide the necessary protection for sensitive but unclassified information and equipment. Training shall include instructions on the proper handling and safeguarding of sensitive equipment and information.

The Information Assurance Officer (IAO) shall ensure all personnel are trained in the proper response to compromise or possible compromise of PII and other sensitive information in accordance with DoD 8570.01 Information Assurance Workforce Improvement Program.

Reporting Systems, Inc. (RSI), DBA Emergency Reporting will provide MCFIRS IT service and support, maintain all software and hardware, and provide updates and backups meeting DoD security Standards.

RSI shall ensure appropriate security and privacy of all data transmitted to the website in compliance with HIPAA regulations and all other applicable federal, state and/or local rules, regulations and/or laws.

RSI shall maintain the Website and store the Agency's data at the Bellingham Fibercloud Data Center. If RSI utilizes another data center in the future, it shall meet or exceed the accessibility, reliability, and security standards of the Fibercloud Data Center.

RSI shall provide the Website to be accessible by current browser technology (Internet Explorer 5.5) as standardized by the W3C (World Wide Web Consortium).

RSI shall provide at least daily data backups to guard against data loss in the event of catastrophic system failure.

RSI shall maintain all data submitted on the Website for a period of eight years (96 months) from the time of submission by the Agency. Data older than eight years shall be archived and removed from the servers, but may be reloaded if the data is needed.

Emergency Reporting received a System Security Authorization Agreement (SSAA) 28 July 2006 (MCAS Cherry Point) in accordance with DoD Instruction (DoDI) 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), the then current standard process for determining the products and procedures in place accomplish the requirements for Information Assurance and support.

Concurrent with the preparation of this PIA, USMC F&ES is submitting MCFIRS for certification and accreditation with the USMC through the DoD Information Assurance Certification and Accreditation Process (DIACAP). The DIACAP package was reviewed and Authority to Operate was granted on DATE
(please note that this PIA will be updated to include the date ATO was granted).

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 USMC F&ES Departments
- HQMC
- United States Navy - Naval Safety Center

☒ **Other DoD Components.**

Specify.
- United States Air Force
- DoD Fire Training Academy

☒ **Other Federal Agencies.**

Specify.
- United Stated Fire Administration
- National Fire Academy
- The Federal Emergency Management Agency
- National Fire Incident Reporting System
- National Emergency Medical Services Information System

☒ **State and Local Agencies.**

Specify.

- States of Arizona, California, Georgia, North Carolina, South Carolina, Virginia, and Washington
- Local agencies participating in mutual aid response and/or training with USMC F&ES

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Reporting Systems, Inc.(RSI); DBA Emergency Reporting, www.emergencyreporting.com is the contractor for MCFIRS. The following language is provided in the contract to safeguard PII.

All data transmitted to the website shall remain the property of the USMC F&ES. Retransmission of this data to the State of Washington and FEMA is authorized. Modifying, deleting or other modifications of submitted data by RSI is prohibited. Scientific research that is based on broad data trends is authorized, but no Agency specific data must be visible to any third parties.

RSI agrees to keep confidential information disclosed to it by USMC F&ES in accordance herewith, and to protect the confidentiality thereof in the same manner it protects the confidentiality of similar information and data of its own. at all times exercising at least a reasonable degree of care in the protection of confidential information.

☒ **Other** (e.g., commercial providers, colleges).

Specify.

- Educational Institutions
- Commercial providers of Fire and Emergency Services training
- International Fire Service Accreditation Congress (IFSAC)
- National Board on Fire Service Professional Qualifications (PROBOARD)

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.

When PII is collected from individuals on the scene of emergency incidents the information is obtained voluntarily within the scope of the provision of emergency services.

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

Individuals employed by USMC F&ES Departments do not have an opportunity to object to the collection of their PII in MCFIRS. PII is required as a condition of employment for administrative, promotional and training and certification activities. While PII must be collected, individuals are able to correct erroneous information resident within MCFIRS. PII for USMC F&ES personnel is manually entered by supervisors and system administrators upon employment. Erroneous information can be corrected by notifying the Installation system administrator through the appropriate chain of command.

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.

When PII is collected from individuals on the scene of emergency incidents the information is obtained voluntarily within the scope of the provision of emergency services. Individuals can deny treatment and services and withhold consent to provide PII at that time.

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

PII from USMC F&ES employees resident in MCFIRS is used to provide personnel and administrative services for the individual and USMC F&ES Department and program. If a USMC F&ES employee were given the opportunity to exclude their PII from MCFIRS, it would prevent them from being considered for assignment or promotion and would not allow for the verification of credentials to allow for continued employment with USMC F&ES.

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 of 1974 (PL 93-579) requires that individuals be informed of the authority which allows the solicitation of the information and whether disclosure of such information is mandatory or voluntary; the principal purpose for which the information is intended to be used; the routine uses which may be made of the information gathered; and the effects, if any, of not providing all or any part of the requested information. In accordance with these and other requirements a Privacy Advisory alerts users of MCFIRS that they are entering into a records/data collection that is governed by rules established under the Privacy Act (5 U.S.C. 552a)/PL 93-579 and notifies them that they are only authorized to use information within the collection for "official use" only, and that they may not share/ disseminate the information unless specifically authorized, and that civil/criminaly penalties apply for any unauthorized sharing/dissemination of data maintained within the collection.

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.