U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Incident Qualifications and Certification System (IQCS)
Bureau/Office: Bureau of Land Management, National Interagency Fire Center
Date: 10/03/2017
Point of Contact:
Name: Suzanne S. Wachter
Title: BLM Associate Privacy Officer
Email: swachter@blm.gov
Phone: (202) 912-7178
Address: 20 M Street SE, Washington DC 20003

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Incident Qualifications and Certification System (IQCS) Major Application (MA) is an interagency application that tracks training and certifications for emergency incident responders. This application represents an emergency incident community of Federal agencies including: the Department of Defense (DOD), the United States Department of Agriculture (USDA) Forest Service, the Department of the Interior (DOI) and all of its bureaus and offices, Federally recognized Tribes and Alaska Natives, State Foresters' Representatives, and other cooperating entities such as the Nature Conservancy and the Army Corps of Engineers (USACE). These entities utilize IQCS to document training and experience of

emergency incident responders who may be assigned to an incident allowing management to identify qualified responders to fill emergency incident assignments in a safe and efficient manner.

The IQCS is a system of record for the National Wildfire Coordinating Group (NWCG) and the DOI Incident Position Qualification Guide job codes and job criteria. Fundamental business processes and functions include:

- Repository management of incident (e.g., wildland fire and all hazards) positions performance standards, and their respective qualification and certification requirements.

- Training management, including course/offering descriptions, learning objectives, pre-course requirements, class schedules, student registration, and class participation information.

- Workforce analysis that accurately reports in a timely manner the disposition, status, and deficiencies of positions throughout the incident response community.

- Tracking of personnel information related to an individual's qualification and certification currency, and history that includes such information as positions held, position performance, training, physical fitness status, and external warrants.

C. What is the legal authority?

The creation and the maintenance of this system are authorized in accordance with provisions of

- Public Lands: 43 U.S.C. 1811e
- Reciprocal Fire Protection Agreements: 42 U.S.C. 1856a
- Fire Prevention and Control Act: 15 U.S.C. 2201
- Government Organization and Employees Training: 5 U.S.C. 4118
- General Authority to Employ: 5 U.S.C. 3101
- Planning for Fire Protection: 16 U.S.C. 551C
- Public Lands DOI Duties of the Secretary: 43 U.S.C. 1457
- Department of the Interior All-Hazards Incident Staffing: Emergency Management Policy Bulletin 2011-1

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

010-04-01-02-01-0420-00-104-008; Incident Qualifications and Certification System (IQCS)

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
None	**N/A**	No	**N/A**

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

This system is covered by the BLM-40, Incident Qualification and Certification System (IQCS), 73 FR 6996, February 6, 2008, which may be viewed at https://www.doi.gov/privacy/blm_notices.

This BLM-40 SORN covers DOI personnel and is currently being revised to provide updated content for the system and incorporate new Federal government-wide requirements in accordance with OMB Circular A-108. Other Federal agencies utilizing IQCS to track training and certifications for their emergency responder personnel must meet requirements under the Privacy Act and OMB A-108, including publication of a system of records notice, notification, access and amendment procedures, and addressing complaints.

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Personal Cell Telephone Number
☒ Birth Date
☒ Personal Email Address
☒ Home Telephone Number
☒ Employment Information
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*
Official address and phone number; physical clearance status; pertinent education history related to qualifications; work history; qualifications and certifications; pertinent work or skills experience; licenses and certificates held; training completed; and test scores. Information such as birth date, personal email address, personal home phone number, and personal cell phone number are voluntarily provided and not required by the system. Social Security numbers were removed from this system as part of the DOI efforts to eliminate the unnecessary use and collection of Social Security numbers and other privacy sensitive information. BLM has also taken action to eliminate or reduce the use of birth dates where possible.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency
☒ Tribal agency
☒ Local agency
☒ DOI records
☐ Third party source
☒ State agency
☒ Other: *Describe*
Cooperating entities with emergency incident qualifications covered in the system.

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☒ Email
☒ Face-to-Face Contact
☐ Web site
☐ Fax
☒ Telephone Interview
☒ Information Shared Between Systems
☒ Other: *Describe*
Information is entered directly into the application by account managers or manually imported from other qualification systems as a responder record. How the account managers gather the information from the responders varies. IQCS is not the system of record for the data that the account managers maintain on the responders, only the information when it is input into the system is DOI information.

The information shared with other systems consists of emergency responder name, unit identification, certifications and qualifications and is utilized to dispatch qualified personnel as needed for disasters, wildland fires, etc.

D. What is the intended use of the PII collected?

The IQCS is an information system that tracks training and certifications for emergency incident responders. The typical emergency incidents for which the information is used are wildland fires, human caused disasters, and weather related incidents such as hurricanes, floods, or tornados. Fundamental high level business processes and functions include:

- Training management that includes items like student registration and class participation information.
- Workforce analysis that accurately reports in a timely manner the disposition, status and deficiencies of positions throughout the incident response community.
- Tracking of emergency incident responder information related to an individual's qualification and certification currency and history that includes positions, position performance, training, physical fitness status, and external warrants.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

Data on emergency responders is shared within the BLM either through reports such as the emergency responder qualification card or reports containing analytics of numbers of employees qualified in specific positions or numbers of employees requiring specific training courses.

To support BLM management officials in managing an incident by insuring that only qualified personnel are assigned to wildland fires, prescribed fires, natural disasters, and terrorist acts, in positions that they are qualified to perform; thus reducing the potential for loss of property or life due to having unqualified personnel assigned to incident positions.

To support home unit (employing unit) coordinators updating the database with information about training course completion, task book completion, qualifications obtained, and positions that individuals are no longer qualified to perform.

The IQCS database contains elements that require review under the Privacy Act (PA) disclosure requirements at 5 U.S.C. 552a (b) and the Freedom of Information Act (FOIA), 5 U.S.C. 552, before any information will be released. Rules of Behavior documentation is in accordance with BLM policy and is available from the specific project files. Applicable Privacy Act warning statements are placed on all information printouts from the system.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

Data on emergency responders is shared within the Bureaus / Offices either through reports such as the emergency responder qualification card or reports containing analytics of numbers of employees qualified in specific positions or numbers of employees requiring specific training courses.

To support Bureaus/Offices management officials in managing an incident by insuring that only qualified personnel are assigned to wildland fires, prescribed fires, natural disasters, and terrorist acts, in positions that they are qualified to perform; thus reducing the potential for loss of property or life due to having unqualified personnel assigned to incident positions.

To support home unit (employing unit) coordinators updating the database with information about training course completion, task book completion, qualifications obtained, and positions that individuals are no longer qualified to perform.

The IQCS database contains elements that require review under the Privacy Act (PA) disclosure requirements at 5 U.S.C. 552a (b) and the Freedom of Information Act (FOIA), 5 U.S.C. 552, before any information will be released. Rules of Behavior documentation is in accordance with BLM policy and is available from the specific project files. Applicable Privacy Act warning statements are placed on all information printouts from the system.

Since each cooperating agency has access to the records of their personnel contained in the system, any requests for that information is the responsibility of the agency to which the data in question belongs.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

Emergency responders' PII is not shared with other Federal agencies, except for authorized purposes outlined in the published routines uses in BLM-40, Incident Qualification and Certification System (IQCS) system of records notice, such as investigations related to falsifying training qualifications. Each participating Federal agency maintains their own portion of the information within IQCS. The only information provided is whether an individual is qualified for the position.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

Each participating tribe maintains their own portion of the information within IQCS. The only information provided is whether an individual is qualified for the position.

Information may also be shared with tribes as authorized and described in the routine uses contained in the BLM-40, Incident Qualification and Certification System (IQCS) system of records notice.

☒ Contractor: *Describe the contractor and how the data will be used.*

Contractors perform maintenance on the system and provide customer support. The data is used as part of the routine operations and maintenance to validate system performance or to verify the identity of the account manager for customer support.

Information may be shared with contractors as authorized and described in the routine uses contained in the BLM-40, Incident Qualification and Certification System (IQCS) system of records notice.

☐ Other Third Party Sources: *Describe the third party source and how the data will be used.*

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

The provision of information is voluntary. Account and training managers input responders' information into the system. The only requirement for the individual emergency incident responder to have a record is for the responder's name and employing organization. In order for the individual to be considered as qualified for a position, pertinent training and experience information must be provided. The individual responder has the option to not provide personal data. If information is not provided the responder will be ineligible for dispatch as an emergency responder.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ Privacy Act Statement: *Describe each applicable format.*

☒ Privacy Notice: *Describe each applicable format.*

Notice is also provided through the publication of this privacy impact assessment and the BLM-40, Incident Qualification and Certification System (IQCS) system of records notice, which may be viewed at https://www.gpo.gov/fdsys/pkg/FR-2008-02-06/html/E8-2136.htm.

☐ Other: *Describe each applicable format.*

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

The system contains search fields for retrieving data by unique emergency responder identifier (EMPLID) created by the system, an emergency responder's organization, or an individual's last name.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

An end user may represent many roles in the local organization. These roles define what type of reports can be accessed. For example:

The roles of Training Officer or Training Coordinator can produce training course rosters, training course completion status and historical training session information.

The role of Account Manager can produce the qualified position card, training, experience and position reports for the individual. Master History reports are often printed for the individual's personal use.

The role of Supervisor can produce training, experience, and position reports useful during an Incident Responders Development Plan (IRDP) session. The role can also produce reports useful for workforce analysis.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

The data verification and quality control process documents the accuracy of data through a comparison to the source data. The IQCS end-user will ensure that the data from non-DOI records is accurate during the initial input, e.g., training records are accompanied with a signed certificate from the Course Coordinator or Instructor.

B. How will data be checked for completeness?

The IQCS end-user will request supplemental documentation from the incident responder (as required) to ensure the completeness of the initial data input, e.g., National Wildfire Coordinating Group (NWCG) Position Task Book (PTB) is the physical artifact that documents the acquired skills for an emergency incident position. It contains evaluations of the individual responder by incident supervisors and the final certification by management.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Emergency incident responder experience data will be the responsibility of the local IQCS end-user to verify as needed. Business requirements data, used by the application to measure the assignment of a position to an emergency incident responder, is updated as the business changes and continues to mature. Updates from other systems of record are completed as they are received. These updates are received in flat-files or as automated updates. Those updates that are received by flat file are verified with the system of record and entered by the IQCS national staff.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

DOI bureaus and offices follow guidance on permanent and temporary records disposition issued by the National Archives Records Administration (NARA). The BLM Records Retention schedule is DAA-0049-2013-0001, Incident Qualification and Certification System, which consists of one temporary disposition item.

The IQCS contains the emergency response experience and qualification records of emergency responders. After five years of inactivity on a responder record, the record is identified to be in an archive status and will continue to be maintained at the agency. The record can be reactivated as needed in IQCS. Extant records are to be migrated to any new qualifications system upon IQCS System decommission. Delete any records in archive status that are inactive for 25 consecutive years.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Temporary records are disposed of in accordance with DAA-0049-2013-0001 and BLM policy. Destruction of eligible temporary records is documented on BLM Form 1270-4, Documentation of Records Destruction for On-Site and Federal Records Center (FRC) Disposals, and must be coordinated with the State/Center/WO Records Administrator or Records Manager and appropriate records custodian.

Approved disposition methods for electronic records include deleting, degaussing or erasing, in accordance with NARA Guidelines and 384 Departmental Manual 1.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a minimal privacy risk due to the type and volume of personal information maintained in the system. IQCS tracks training and certifications for emergency incident responders for wildland fires, human caused disasters, and weather related incidents such as hurricanes, floods, or tornados. Information collected and used is limited to the minimum required to perform the purpose and functions

of the system. To mitigate privacy risk, BLM removed Social Security numbers from this system, and has taken action to eliminate or reduce the use of birth dates where possible.

IQCS is classified as moderate for FISMA and has all of the required system security documentation and a current Authority to Operate (ATO). In accordance with OMB Circulars A-123 and A-130, IQCS has controls in place to prevent the misuse of the data by those having access to the data. Such security measures and controls consist of: passwords, user identification, IP addresses, database permissions and software controls. All employees including contractors must meet the requirements for protecting Privacy Act information.

Business rules and guidelines, as well as rules of behavior, have been established to prevent inadvertent disclosure to individuals not authorized to use the system or those who do not have a direct "need to know" certain information contained in the system. All end-users have an individual password and ID that is issued by the IQCS application steward. All new users will receive training on the use of the system. All DOI employees must complete mandatory privacy, security and records management training annually, and acknowledge the DOI Rules of Behavior.

The IQCS SSP describes the practice of audit trails. Audit trails maintain a record of system activity and user activity including invalid logon attempts and access to data via User ID, IP Address, etc. Audit trails are also captured within the system to determine who has added, deleted or changed the data within the system. Any qualification over-rides require that the account manager document the reasoning and the login name with date and time is added by the system.

Accounts are reviewed annually to ensure that only authorized personnel have systems logins. Additionally, any account that is inactive for more than one year is automatically suspended. All personnel accessing the system must acknowledge the rules of behavior prior to each login.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The information collected is the minimum necessary to ensure that emergency responders have the necessary training before they are dispatched in response to emergencies to ensure that federal emergency response requirements are being met and standards maintained.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*

☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*

☒ No

E. How will the new data be verified for relevance and accuracy?

No new data will be derived.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☒ Other: *Describe*
Database Managers and Security Management Personnel.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access to pages and therefore responder data is on a "need-to-know" basis and is controlled by the assignment of a role and department security row. A role is a collection of data fields to add, modify, retrieve, and delete responder information. It can be assigned singularly or tailored by layering several distinct roles to meet many different local business models. Example roles are: Account Manager, Training Officer, and Certifying Official.

A department security row represents a responder's organization. A department security row is configured to match business requirements by identifying the organization(s) to access. Example department security rows are: Grand Canyon National Park, Tonto National Forest, and Fort Apache Agency. The combination of role and department security allows the IQCS end user to access the responders within the organization(s) of the department security row and perform the defined actions as provided by the assigned role.

The assignment of a role and department security row to an individual is authorized through an agency administrator familiar with business requirements and local personnel. Procedures to require an account are documented in IQCS account request standard operating procedure (SOP) based on the BLM Security Controls for Access to IT Systems and Applications Standard Operating Procedures.

The criteria, procedures, controls, and responsibilities regarding access are documented in the business rules and guidelines and rules of behavior and comply with the intent of the Computer Security Act of 1987 [Public Law 100-235] for standards and guidelines on security and privacy.

Access to data is limited to authorized personnel whose official duties require such access and is on a "need-to-know" basis implemented by the IQCS role-based and department security row application.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

The contract is a standard maintenance contract that contains the required Privacy Act FAR clauses for IT systems.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

The IQCS monitors account managers, training managers, and other individuals who use the system through audit trails. Audit trails maintain a record of system activity and user activity including invalid logon attempts and access to data via User ID, IP Address, etc.

Audit trails are also captured within the system to determine who has added, deleted or changed the data within the system. Any qualification over-rides require that the account manager document the reasoning and the login name with date and time is added by the system.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

Audit trails maintain a record of system activity and user activity including invalid logon attempts and access to data via User ID, IP Address, etc.

Audit trails are also captured within the system to determine who has added, deleted or changed the data within the system. Any qualification over-rides require that the account manager document the reasoning and the login name with date and time is added by the system.

M. What controls will be used to prevent unauthorized monitoring?

Formal rules of behavior are provided to the user and accepted by his or her signature prior to gaining access. These rules delineate the responsibilities and expectations for all individuals using the IQCS program. Additionally, a warning banner and notification of monitoring is present to all end-users of the system and must be accepted prior to each and every login attempt. Non-compliance of these rules will be enforced through sanctions commensurate with the level of infraction.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☒ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges

☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☒ Other. *Describe*
Account managers can only see the data on the emergency responders that they have in their organization. The IQCS system administrators and programmers can see all of the records, but they have to use VPN to access the application and use their PIV card to authenticate for the VPN. The Interagency account managers can access the application through the web and are not required to use VPN or use their PIV card.

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Assistant Director, National Interagency Fire Center, is the IQCS Information System Owner and the official responsible for oversight and management of the IQCS security controls and the protection of agency information processed and stored in the IQCS application. The Information System Owner and IQCS Privacy Act System Manager, in collaboration with the BLM Senior Management Team, are responsible for ensuring adequate safeguards are implemented to protect individual privacy in

compliance with Federal laws and policies for the data managed, used, and stored in the IQCS application. These officials, DOI bureau and office emergency response officials, and authorized IQCS personnel are responsible for protecting individual privacy for the information collected, maintained, and used in the system, and for meeting the requirements of the Privacy Act, in consultation with DOI Privacy officials.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The IQCS Information System Owner is responsible for oversight and management of the IQCS security and privacy controls, and for ensuring to the greatest possible extent that agency data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of agency PII is reported to DOI-CIRC within one hour of discovery in accordance with Federal policy and established DOI procedures. Each participating entity is responsible for ensuring the proper use of the system and their data as agreed within the applicable Memorandums of Understanding (MOUs).