



U.S. Department of the Interior PRIVACY IMPACT ASSESSMENT

Introduction:

The Department of the Interior (DOI) requires the DI-4001 Privacy Impact Assessments (PIA) form to be conducted and maintained for all IT systems that collect, maintain, use, or share personally identifiable information (PII), whether the system is new, undergoing significant modification, or already in operation as well as electronic collections under the Paperwork Reduction Act. The PIA is a critical tool for evaluating privacy risks, documenting safeguards, ensuring compliance with the E-Government Act of 2002 (Section 208) and OMB Guidance. This form must be completed electronically and submitted to the Department Privacy Office for review and determination via our [Privacy Office Support Request Page](#). For further guidance, consult the [DOI PIA Guide](#).

System Information

System or Project Name:	Internet Quarters Management Information System
System or Project Acronym:	iQMIS
Date submitted for review:	August 25, 2025
System Operational Status:	Operational

Point of Contact

Name:	Adrienne Brooks-Hill
Title:	Associate Privacy Officer
Office:	Office of the Secretary
Phone:	202-208-1605
E-mail:	DOI_Privacy@ios.doi.gov

Section 1: System Overview

1. What triggered this PIA? (Check one)

- | | |
|--|---|
| ☐ New System | ☐ Significant Modification |
| ☐ New Electronic Collection | ☒ Other: Describe below |

This system's last risk assessment was conducted on June 13, 2018.

2. What is the purpose of the system or project?

The Internet Quarters Management Information System (iQMIS) is a centralized web-based system used to set rental rates for employees or tenants living in government-owned housing, in accordance with Federal regulations in OMB Circular A-45, *Rental and Construction of Government Housing*. The iQMIS application produces rent calculations and tenant rental agreement documents as requested by the customers. iQMIS is offered as a shared service to assist Department of the Interior (DOI) bureaus/offices and Federal agency customers meet regulatory requirements. The purpose of iQMIS is to:

- Set a rental rate for each Federal housing unit and tenant in compliance with OMB Circular A-45;
- Document the occupancy of each unit by employees/tenants;
- Print lease agreements and other occupancy documents;
- Provide rent payment forms/documents for the agency to collect rents;
- Transmit payroll actions to the DOI Federal Personnel and Payroll System (FPPS) for DOI, Department of Transportation (DOT) and International Boundary and Water Commission (IBWC) employees;
- Transmit estimates of rent revenues to the DOI Financial and Business Management System (FBMS) for DOI rental units; and
- Produce housing inventory, housing utilization, rent revenue estimates and other reports for agency property managers.

There are numerous DOI bureaus/offices and Federal agency customers using iQMIS for employee housing. The DOI bureaus and offices using iQMIS include Bureau of Indian Affairs, Bureau of Land Management, Bureau of Reclamation, National Park Service, U.S. Fish and Wildlife Service, and U.S. Geological Survey. Other Federal agencies and offices include U.S. Forest Service, Indian Health Service, Customs & Border Protection, Federal Aviation Administration, and Veterans Administration.

3. Is the system registered in BisonGRC?

- ☒ Yes: If applicable What is the project's UII code?
☐ No: Explain why this is not either done or required.

UII code is 010-000001756, iQMIS System Security & Privacy Plan.

4. What legal authorities authorize the collection and use of data in this system or project?

The legal requirement to charge employees and other occupants rent for Federal housing is provided in 5 U.S.C. 5911, Quarters and Facilities: Employees in the United States. The requirements specifying the amount of rent to be charged are identified in the OMB Circular A-45, *Rental and Construction of Government Housing*, and OMB Circular A-25, *User Fees*.

5. Does the system or project require a published Privacy Act System of Records Notice (SORN)?

- ☐ Yes: If yes, list the applicable citations below.
☒ No

iQMIS is not a system of records because records cannot be retrieved by an individual's name or other unique identifier. Users retrieve records by housing installation name and housing unit number. Rent collected from the employee/tenant through payroll deduction actions are processed through the DOI Federal Personnel and Payroll System (FPPS), which is maintained under the DOI-85: Payroll, Attendance, Retirement and Leave Records system of records notice, 83 FR 34156 (July 19, 2018). This SORN may be viewed at <https://www.doi.gov/privacy/sorn>.

6. Does this project involve an information collection that requires OMB approval under the Paperwork Reduction Act?

- ☒ Yes

☐ No

The legal requirement to charge employees and other occupants rent for Federal housing is provided in 5 U.S.C. 5911, Quarters and Facilities: Employees in the United States. The requirement specifying the amount of rent to be charged and methods of rent collection are identified in OMB Circular A-45, *Rental and Construction of Government Housing*, and OMB Circular A-25, *User Fees*. The IBC Quarters Program also has approval from the Office of Management and Budget, under its Paperwork Reduction Act procedures, to collect private rental market data from members of the public to set rental rates under OMB Control Number 1084-0033 (for iQMIS Form OS-2000 and OS-2001). This OMB approval expires 2-28-2026 and is renewed every three years.

7. List all minor applications or subsystems that are hosted on this system and covered under this PIA.

None

Section 2: Data Description and Use

1. What categories of PII and sensitive data types will the system collect, use, or store? Check all that apply.

- | | | |
|--|---|---|
| ☒ Name (full, first or last) | ☒ Home telephone number | ☒ Employment or resume info |
| ☐ Aliases/nickname | ☐ Personal Email | ☒ Full or Truncated SSN |
| ☐ Driver's license | ☒ Mailing or home address | ☐ Physical characteristics |
| ☐ Citizenship | ☐ Religious preference | ☐ Biometrics or facial recognition |
| ☐ Legal Status | ☐ Mother's maiden name | ☐ Vehicle information |
| ☐ Sex | ☐ Marital status | ☐ Passport information |
| ☐ Race or ethnicity | ☐ Spouse Information | ☐ Travel information |
| ☐ Date of birth | ☐ Child or family information | ☐ Parent's name |
| ☐ Place of birth | ☐ Emergency contact info | ☐ Credit card number |
| ☒ Personal cell phone number | ☐ Financial information | ☐ Nationality |
| ☐ Tribal or other ID number | ☐ Education information | ☐ Disability Information |
| ☐ Military records | ☒ Other: Describe below | |

For employees/tenants living in Federal housing, iQMIS users may request PII from the employee/tenant directly, the employee's hiring manager, or an Administrative Officer to ensure the payment of rent. For example, an individual's SSN or the last 4 of the SSN are required to process a payroll deduction for rent. Mailing address is required to process a Bill of Collection for rent.

For members of the public who complete the OS-2001 and OS-2000 forms, iQMIS collects the name, address and phone number of the private rental unit agent, manager, owner, or tenant as well as the name and address of mobile home communities. Business address and phone numbers and community names and addresses are publicly available. Last name, home address and phone are optional. Members of the public may complete the form and provide only with their first name.

2. What is the source for the PII collected? Check all that apply.

- ☒ Individual ☒ DOI Records

- ☒ Federal Agency
- ☒ Tribal Agency
- ☒ Local Agency

- ☐ Third Party Records
- ☐ State Agency
- ☐ Other: *Describe Below*

3. How will the information be collected? Check all that apply.

- ☒ Paper Format
- ☒ Email
- ☒ Face-to-Fact Contact
- ☒ Website

- ☐ Fax
- ☒ Telephone Interview
- ☒ Shared Between Systems: *Describe*
- ☐ Other: *Describe*

PII is collected by iQMIS Users from employees/tenants or their supervisors. This data may be collected face-to-face, by telephone, or by email. The data is entered into the iQMIS system using a web form. Once saved, the data is stored in database tables. All iQMIS data is encrypted in transit and at rest. PII is also shared through electronic files, sent between iQMIS and FPPS for rent payment purposes.

PII from members of the public on the OS-2000 or OS-2001 form is collected by telephone, email or web page, compiled in the contractor's database, and then uploaded to the iQMIS application as a contract deliverable. Once uploaded, the data is stored in database tables. All iQMIS data is encrypted in transit and at rest.

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

For employees/tenants, PII is necessary for rent collection purposes. Specific business and payroll processes are determined by each agency, according to their unique requirements. SSNs are used to collect rent from the employee/tenant through payroll deduction actions and are only collected for that purpose. Mailing addresses and personal phone numbers may be necessary to create a Bill for Collection. Emails, phone numbers and addresses may also be used to provide written and electronic communications with the employee/tenant on their rent, their lease, and other housing-related issues, for example, to provide a notice of inspection or to provide a notice of rent change.

For private rental market data, PII is collected for follow-up questions, to verify data provided on OS-2000 or OS-2001, and for Paperwork Reduction Act purposes. The PRA requires that a sample of respondents be taken to determine the time required to complete the government's information request. iQMIS staff contact several private rental market owners via email every 3 years during the OMB's renewal process.

5. How does this project limit the collection and use of PII to only what is necessary?

This system limits its collection and use of PII by only asking for the necessary information to generate a Bill for Collection, for those tenants who cannot pay rent through payroll deductions, and to what is needed to rent Federal housing under 5 U.S.C. 5911, Quarters and Facilities: Employees in the United States.

Section 3: Data Sharing and Individual Rights

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

- ☒ **Within the Bureau/Office:** Describe how the data will be used below.
- ☐ **Tribal, State or Local Agencies:** Describe how the data will be used below.
- ☒ **Other Bureaus/Offices:** Describe how the data will be used below.
- ☒ **Contractor:** Describe how the data will be used below.
- ☒ **Other Federal Agencies:** Describe the federal agency and how the data will be used
- ☐ **Other Third-Party Sources:** Describe how the data will be used below.

Within the Bureau/Office: For employees, PII may be shared by the IBC Quarters Program Office with other IBC offices for payroll or accounting purposes. Specifically, the IBC Payroll Operations Branch and IBC Debt Management Branch may require individual tenant names and SSN to assist with payroll deduction and rent issues. SSNs are only transmitted verbally or by Secure Transport -- never by email or paper. PII is also shared through electronic files, sent between iQMIS and FPPS for rent payment purposes under strict security and privacy controls. All parties involved have a specific role in the rent payment process and are a designated shared service provider.

The Bureau of Indian Affairs (BIA) and the Bureau of Indian Education (BIE) allow some tribal organizations have housing that it owns. In turn, BIA or BIE permits these organizations to use iQMIS to set rental rates to comply with OMB Circular A-45, *Rental and Construction of Government Housing*. If the tribal organizations have taken control of the housing, they may or may not use iQMIS for rent setting as it would no longer need to comply with A-45, because it would not be government provided housing

For tenants who cannot pay through payroll deduction, PII may be shared by the individual agency/bureau personnel with their accounting offices for Bill of Collection purposes.

Other Bureaus/Offices: PII from one bureau/office is not typically shared with another bureau/office. However, a bureau may need to share PII with their shared service provider (IBC Payroll Operations Branch and the IBC Debt Management Branch), such as names and SSN, to assist with payroll deduction and rent issues. SSNs are only transmitted verbally or by Secure Transport -- never by email. PII is also shared electronically between iQMIS and FPPS for rent payment purposes under strict security and privacy controls. All parties involved have a specific role in the rent payment process.

Each bureau owns their own iQMIS data and has a unique business process which prescribes how it will be used within their organization. They may share that data internally with their bureau's Human Resources personnel or with accounting personnel responsible for entering Bills of Collection into the accounting system. All personnel using employee/tenant PII have a "need to know" and a responsibility to secure the rent payment within their bureau/office process. These communications are conducted within their bureau/office, by email, face-to-face or via telephone.

Contractor: For the private rental market data, PII is not shared with anyone, and is visible only to the contractor who collected it and the iQMIS System Managers/Program Manager. Contractors collecting rental market data are the only ones who will see PII for what they collected. They do not see any tenant information or PII for individuals entered into iQMIS.

Other Federal Agencies: The Department of Health and Human Services, Indian Health Service (IHS) allows some tribal organizations have housing that it owns. In turn, IHS permits these organizations to use iQMIS to set rental rates to comply with A-45. If the tribal organizations have taken control of the housing, they may or may not use

iQMIS for rent setting as it would no longer need to comply with A-45, because it would not be government provided housing.

2. Does this system have an MOU/MOA/ISA with other Federal Agencies or State/Local/Tribal Agencies with which it shares information?

- ☐ Yes
☒ No

iQMIS does not require an MOU, since it does not connect to external systems or agencies. All connections are within DOI.

3. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII? If not, what steps are in place to ensure individuals are aware of how their information is being used?

- ☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*
☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

Individuals entered in iQMIS have chosen to live in government housing at their work site, which is voluntary. Others occupy housing as a condition of employment but voluntarily accept this condition when applying for the Federal position. Occupancy of Federal housing requires a contractual agreement (a lease) and the individual's agreement to pay rent for the housing provided. The opportunity to decline or consent to specific use of PII occurs upon position acceptance or exercising the option of accepting Federal housing.

For bureaus/agencies that also use FPPS, employee name and SSN are required for collection of rent by payroll deduction. If an employee declines to provide their SSN to their housing manager, the employee may be denied housing because payment cannot be arranged without the SSN. If an employee refuses to provide their PII, other sources, such as the hiring manager or bureau/agency Administrative Officer, may be contacted for employee information.

For non-employees, their name and mailing address are required to establish the Bill of Collection. If the non-employees decline to provide their address, they will be denied housing since payment cannot be arranged in the accounting system without a billing address.

For private rental market data collected through OS-2000 and OS-2001, the property agent, manager, owner, or tenant may decline to provide their last name, address, or phone upon form completion. Only a first name is required on the OS-2000 and OS-2001 for processing.

4. How does the project provide notice to individuals prior to the collection of information? Check all that apply.

- ☒ Privacy Act Statement: ☐ Other: *Describe Below*
☒ Privacy Notice: ☐ None: *Example - law enforcement cases.*

For private rental market data, the OS-2000 and OS-2001 forms describe the purpose of the data, an estimate of

burden, the right to decline, and have a Privacy Act Statement.

Privacy notice is provided through the publication of this privacy impact analysis. Notice regarding the FPPS and DOI employee payroll processes, deductions and sharing are provided through the publication of the FPPS PIA and the DOI-85, Payroll, Attendance, Retirement, and Leave Records, system of records notice, 83 FR 34156 (July 19, 2018). This SORN may be viewed at <https://www.doi.gov/privacy/sorn>.

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

Users of iQMIS retrieve data based on housing unit numbers they are authorized to manage. iQMIS users cannot search for or retrieve data based on an individual name, SSN or other personal identifier. However, individual tenant information is stored as a related record within each housing unit record and is not searchable. iQMIS reports can be used to print employee/tenant's names. To find a specific tenant, the iQMIS user must know the tenant's current and previous housing unit number.

A System Manager may search based on communities and individual units for private rental market data. System Managers cannot search for or retrieve an individual name or other personal identifier.

6. Will reports be produced on individuals, whose PII is contained in this system? If yes, who has access and what is the purpose of these reports?

- ☒ Yes: Describe the use of these reports and who will have access to them.
☐ No

The iQMIS system provides reports to help bureaus/offices and agencies with housing management and rent payment functions. All users have access to reports, which they may also provide to their supervisors and managers.

Housing Unit reports provide information on whether a unit is occupied or vacant. These reports list the current tenant by name but do not include any other personal identifiers. Some examples of reports where the tenant's name appears include:

- Current Tenant Assignments
- Rent by Tenant
- Rent Change by Tenant
- Rent Payment Method
- Tenant Occupation & Rent Payment Method

The iQMIS system also produces lease agreements and payroll deduction/payment forms for individual employees/tenants that may include PII such as name. The processes are unique to each bureau/office and agency. The employee's/tenant's name will print on lease documents, but address or SSN is only printed on relevant documents to collect their rent payment through payroll (non-DOI agencies only, if entered by user), Bill for Collection, or internal account transfer. These documents may be provided to payroll or accounting personnel to ensure rent collection.

For private rental market data, no reports are produced that display the property manager, agent, owner, or tenant.

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

iQMIS has internal validation that checks for completeness of data, but iQMIS cannot and does not verify accuracy. Individuals directly provide the data found in iQMIS through submission of either OS-2000 or OS-2001 forms or upon position acceptance. Each agency designates the appropriate iQMIS user who is responsible for accuracy, typically an on-site employee responsible for housing management. Each agency is the owner of their data and is responsible for monitoring and ensuring its accuracy.

For the DOI bureaus and other agencies that use FPPS, iQMIS can confirm SSNs entered by users and confirm the correct name (see Section 2, question C above.) This verification allows the system to detect inaccurate SSNs, ensures the tenant is actively employed, and ensures that rent is not charged to the wrong employee.

For private rental market data, iQMIS relies on the data provider and the contractor to ensure accuracy.

Section 4: Data Management and Retention

1. What is the retention period for the data and under what records schedule?

Bureaus and agencies using iQMIS are responsible for retaining their own signed lease agreements and property inventory changes, in accordance with applicable agency records retention schedules or General Records Schedules (GRS) approved by the National Archives and Records Administration (NARA). iQMIS users are responsible for properly filing and retaining housing-related documents for 3 years after employee/tenant departure, in accordance with GRS 5.4, Item 080, Housing rental and lease records. These records are temporary and destroyed three years after lease termination, lapse, reassignment, rejection of application, cancellation of lease, or conclusion of litigation.

For private rental market data, records regarding rent formulation and program management are maintained by the IBC Quarters Program Office under the Departmental Records Schedule (DRS) - 1, Administrative Records, Long-Term Financial and Acquisition Records, which has been approved by NARA (DAA-0048-2013-0001-0011). These records are temporary. The program is required to keep its rent-setting methodology and private rental market survey documentation for 6 years after cutoff. These records include private rental market data collected from the general public (managers/agents/landlords/tenants) through the OS-2000 and OS-2001 forms and stored in iQMIS.

2. What measures are in place to validate the accuracy and completeness of data received from external sources?

iQMIS has internal validation that checks for completeness of data (for example, SSN field must be 9 digits) and required fields for completeness. Data changes cannot be saved unless mandatory fields are complete. Users are warned if this occurs and are provided with an opportunity to correct the issue and save the record again. Each user is ultimately responsible for its completeness, and each agency is responsible for monitoring and ensuring the completeness of their data.

For private rental market data, the contractor ensures completeness. The contractor enters all required information into iQMIS, such as square footage, number of bedrooms and bathrooms. Incomplete data is identified during the market data analysis by iQMIS staff.

3. Does the project include logging capabilities to record and monitor access to PII?

- ☒ Yes
☐ No

Audit logs are reviewed on a regular basis and any suspected attempts at unauthorized access or scanning of the system are reported immediately to IT Security. The system conducts normal auditing of system user access and user activities within the system. Each housing/tenant record audit trail displayed on a web page reflects changes to a field, including date changed, the user who made the change, the field changed, the old value and the new value. Each user record audit trail (for system and security managers only) documents a user's last login date, plus user scope, role or contact changes made by a Security Manager.

Section 5. Privacy Risks and Mitigation Strategies

1. What privacy risks are associated with the collection, use, retention, and disclosure of PII, and how are they mitigated at each stage of the information lifecycle?

There is a risk to privacy due to the volume and sensitivity of PII in the system. iQMIS is a FISMA moderate system based upon the type and sensitivity of data and requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive data contained in the system. Privacy risks are mitigated by controls implemented in the system. iQMIS is an accredited Federal application that is protected by various physical, technical, and administrative security controls, including continuous monitoring for security threats.

Upon collection, use, retention and processing, there is a risk that PII could be accessed or used by unauthorized personnel. This risk occurs at the local level by agencies collecting PII through face-to-face interviews, email or telephone, and is mitigated through privacy and security training, local controls, and by limiting access to PII. Individual users are responsible for protecting any privacy data in the paper form. Authorized iQMIS users are responsible for following their bureau/office and agency property management controls. Contractors receive access approval in writing from a bureau/agency Supervisor and a second-level manager. Contractors must agree in writing to the iQMIS Rules of Behavior. They complete an initial and annual privacy, security, and records management training, provided by the contracting bureau/agency. A contractor's ability to change data is specified on the authorization, based on their responsibilities for housing management and designated system Role (see Section 4, question H.) Record access is limited in iQMIS to the specific housing installation(s) they manage.

Access controls are implemented to ensure that users are authorized to access the iQMIS system using the principle of least privilege and separation of duties. Authorized iQMIS users are responsible for bureau/office and agency property management controls, which require the collection of PII of occupants of government housing. Users are authorized by management in writing as having a responsibility in the rent payment and payroll deduction process, and to communicate with occupants on housing-related issues.

Access to records in the system is limited to authorized personnel who have a need to know in the performance of their official duties, and each user's access is restricted to only the functions and data necessary to perform that individual's job responsibilities. Once entered by the user and saved, SSNs are not visible in the iQMIS application. Processes are unique to each agency. A payroll electronic record, or a printed Payroll Deduction Form, is used to initiate the rent payment, change the rent payment, or stop the rent payment after departure. All data, including SSNs, are encrypted in transit and at rest in the database. An audit trail provides the identity of each entity accessing the system, the time and date of access (including activities performed using a system administrator's identification), and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts at unauthorized access or scanning of the system are reported immediately to IT Security. Only authorized users with valid HSPD-12 PIV Card or FIPS USB security key will be able to access the system. As federal employees, all iQMIS users are required to complete initial and annual privacy, security, and records management training, and sign Rules of Behavior. It is the responsibility of their bureau/office and agency employer to provide privacy training.

There is a risk that information may be used outside the scope of the purpose for which it was collected. This risk is mitigated by limiting access to the system to only those personnel who have an official need to perform their job duties and ensuring employees complete initial and annual privacy, security, and records management training, and sign Rules of Behavior. Agency payroll and accounting personnel have a business requirement to view and access PII to perform their official duties. PII is only disclosed to the authorized iQMIS user who is responsible for assigning housing, printing the employee/tenant lease, and collecting rent.

Employee SSN and other PII may be collected and entered into iQMIS by authorized housing personnel. iQMIS masks the SSN displayed on the screen using asterisks to ensure only authorized users can view the SSN. Individual users are responsible for protecting any privacy data in the paper form. SSN and other PII may be disclosed to payroll/accounting personnel for rent payment actions on a need-to-know basis. Payroll actions for nine (9) iQMIS customer agencies are automated through a file interface to FPPS. Transmission of files between iQMIS and FPPS is tightly controlled, and both systems are accredited Federal applications. PII is used only for internal payroll and accounting purposes, which is not shared outside the Department unless authorized.

There is a risk that individuals may not have adequate privacy notice. This risk is mitigated by the publication of this PIA, and the related INTERIOR/DOI-85: Payroll, Attendance, Retirement and Leave Records system of records notice for payroll processes. This SORN may be viewed at <https://www.doi.gov/privacy/sorn>.

There is a risk that information may be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The data collected and stored has intentionally been limited to the minimal amount of data needed to assign housing, manage employee/tenant lease, collect rent, and manage government housing program reporting and meeting Federal requirements. Records are maintained in accordance with records schedules that were approved by NARA. Users also are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act.

2. Does the system generate new data or inferences through aggregation or analytics that may influence decisions or individual records? If so, how are those data verified, used, and protected?

- ☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*
- ☒ No

Not applicable.

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

- ☐ Yes: *Provide explanation below*
☒ No

Not applicable.

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

- ☐ Yes: *Provide explanation below*
☒ No

Not applicable.

5. How will the new data be verified for relevance and accuracy? Enter N/A if new data is not derived or created.

Not applicable. The system does not derive new data or create previously unavailable data about an individual.

Section 6: Automated Decision-Making and AI Risk Management

1. Does the system use AI, machine learning, or have a non-operational AI Component?

- ☐ Yes
☒ No, *Proceed to Section 7.*

2. How are models validated for fairness, accuracy, and transparency?

Not applicable

3. Are individuals notified of AI-based decisions that affect them?

- ☐ Yes
☐ No

Not applicable

4. Are safeguards in place to prevent bias or unintended consequences?

- ☐ Yes
☐ No

Not applicable

5. Are models periodically reviewed or retrained to ensure ongoing reliability?

- ☐ Yes
☐ No

Not applicable

6. Is federated learning used for privacy-preserving model training?

- ☐ Yes
☐ No

Not applicable

Section 7: Security and Access Controls

1. Who will have access to project data and how is access determined, authorized, and restricted? Check all that apply and respond in the space below.

- | | |
|---|--|
| ☒ Users | ☒ System Administrator |
| ☒ Contractors | ☐ Other: <i>Describe below</i> |
| ☒ Developers | |

Users receive approval for access in writing from their bureau/agency Supervisor and a second-level manager. Users must agree, in writing, to the iQMIS Rules of Behavior. As federal employees, they complete initial and annual privacy, security, and records management trainings, provided by their own bureau/agency. Users must have a government-issued HSPD-12 PIV card or a FIPS USB security key to access iQMIS. A User's ability to change data is specified on their authorization form, based on their responsibilities for housing management and designated system Role (see Section 4, question H.) Record access is limited in iQMIS to the specific housing installation(s) they manage. Remote access is not authorized.

Contractors receive approval for access, in writing, from a bureau/agency Supervisor and a second-level manager. Contractors must agree, in writing, to the iQMIS Rules of Behavior. They complete an initial and annual privacy, security, and records management training, provided by the contracting bureau/agency. A contractor's ability to change data is specified on the authorization, based on their responsibilities for housing management and designated system role (see Section 4, question H). Record access is limited in iQMIS to the specific housing installation(s) they manage.

Developers and System Administrators are internal IBC Quarters Program employees with responsibilities to operate and maintain the iQMIS system and program its functionality and security features. Developers receive access approval in writing from their IBC Supervisor and a second-level manager. Users must agree in writing to the iQMIS Rules of Behavior. They complete initial and annual privacy, security, and records management trainings. A Developer can view or change any data in the system, in addition to having complete authority over program functions. Developers do not normally change data but may do so to resolve an issue.

System Managers are internal IBC Quarters Program employees with responsibilities to operate and maintain

the iQMIS system, enter rent algorithms, and provide Help Desk services to users. System Managers receive access approval in writing from their IBC Supervisor and a second-level Manager. Users must agree in writing to the iQMIS Rules of Behavior. They complete initial and annual privacy, security, and records management trainings. To assist with issues and problems, they have access to all data in the system. System Managers do not normally change data but may do so to resolve an issue.

Database Administrators are DOI OCIO employees with responsibilities to operate and maintain the Oracle database tables that iQMIS utilizes for data storage. All data, including SSNs, are encrypted in the Oracle tables. Database Administrators do not change data, although they have the capability to do so.

The DOI/OCIO backs up all IBC server files, including iQMIS, using replication. All data, including SSNs, are encrypted in the Oracle tables. OCIO hosting services are provided under an annual Inter Agency Agreement with the IBC's iQMIS Office.

Bureau/Agency payroll and accounting personnel have a business requirement to collect rent from the employee/tenant. They do so through iQMIS files and printed documents, some of which contain PII. Additionally, Bureau/Agency Management have a business requirement to manage their housing. iQMIS produces spreadsheets and reports containing housing, tenant and rent data, but no PII is reported.

2. What data protection policies apply to cloud-based PII storage?

Not applicable. iQMIS does not use cloud storage; data is stored on premises.

3. How does the system monitor and detect unauthorized access, use, or exfiltration of PII?

Controls outlined in the iQMIS System Security Plan that adhere to the standards outlined in the National Institute of Standards and Technology (NIST) SP 800-53, Recommended Security and Privacy Controls for Federal Information Systems, are in place to prevent unauthorized monitoring. These controls include the use of role-based training, encryption, and maintaining data in secured facilities. iQMIS assigns roles based on the principles of least privilege and performs due diligence toward ensuring that separation of duties is in place.

Routine scans of the network are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any iQMIS assets. iQMIS IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system, the time and date of access (including activities performed using a system administrator's identification), and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts at unauthorized access or scanning of the system are reported immediately to IT Security.

4. Does the project include any monitoring of user activity or tracking of individuals? If so, what controls ensure the appropriate use of this capability by authorized personnel?

☒ Yes: describe what controls ensure authorized and appropriate use of this capability.

☐ No

Controls outlined in the iQMIS System Security Plan that adhere to the standards outlined in the National

Institute of Standards and Technology (NIST) SP 800-53, Recommended Security and Privacy Controls for Federal Information Systems, are in place to prevent unauthorized monitoring. These controls include the use of role-based training, encryption, and maintaining data in secured facilities. iQMIS assigns roles based on the principles of least privilege and performs due diligence toward ensuring that separation of duties is in place.

Routine scans of the network are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any iQMIS assets. iQMIS IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system, the time and date of access (including activities performed using a system administrator's identification), and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts at unauthorized access or scanning of the system are reported immediately to IT Security.

5. Will contractors be involved in the following project activities? Check all that apply.

- ☐ Design
- ☐ Development
- ☐ Maintenance

The contractor is **not** involved with any of the above. The contractor is only authorized to collect data per the contract that does contain Privacy Act requirements.

6. What physical, technical, and administrative controls are implemented to protect PII? Check all that apply.

Physical Controls

- | | |
|--|--|
| ☒ Security Guards | ☒ Cipher Locks |
| ☒ Key Guards | ☒ Identification Badges |
| ☒ Locked File Cabinets | ☐ Safes |
| ☒ Secured Facility | ☐ Combination Lock |
| ☐ Closed Circuit Television | ☒ Other: <i>Describe Below</i> |

Locked Offices

Technical Controls

- | | |
|--|--|
| ☒ Password | ☒ Intrusion Detection Systems (IDS) |
| ☒ Firewall | ☒ Virtual Private Network (VPN) |
| ☒ Encryption | ☒ Public Key Infrastructure (PKI) Certificates |
| ☒ User Identification | ☐ Biometrics |
| ☒ Other: <i>Describe Below</i> | |

Personal Identity Verification (PIV) Card; Federal Information Processing Standards (FIPS) Universal Serial Bus (USB) security key for two-factor authentication (non-governmental users only).

Administrative Controls

- | | |
|--|---|
| ☒ Periodic Security Audits | ☒ Methods to Ensure Only Authorized Personnel Have Access |
| ☒ Backups Secured Off-site | ☒ Encryption of Backups Containing Sensitive Data |
| ☒ Rules of Behavior | ☒ Mandatory Security, Records and Privacy Training |
| ☒ Role-Based Training | ☒ Regular Monitoring of Users' Security Practices |
| ☐ Other: <i>Describe Below</i> | |

7. What processes are in place for individuals to file a Privacy Act complaint relating to the project?

The Privacy Act Statement on all forms states that providing the information requested is voluntary. However, an individual may file a Privacy Act request to seek records about themselves, request amendment or correction of records. The DOI procedures for filing a Privacy Act complaint are found at the following website, <https://www.doi.gov/privacy/privacy-civil-liberties..>

8. What processes are in place for individuals to access their information?

An individual may file a Privacy Act request to seek records about themselves, request amendment or correction of records. The DOI procedures for filing Privacy Act requests are found at the following website, <https://www.doi.gov/privacy/privacy-act-requests.>

9. What processes are in place to allow the subject individual to correct inaccurate or erroneous information?

An individual may file a Privacy Act request to seek records about themselves, request amendment or correction of records. The DOI procedures for filing Privacy Act requests are found at the following website, <https://www.doi.gov/privacy/privacy-act-requests.>

10. 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?

Each iQMIS user is responsible for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of their employee's/tenant's privacy protected data to their own bureau/agency in accordance with their procedures. Per the iQMIS Rules of Behavior, iQMIS Users must also "Notify the iQMIS Help Desk and appropriate bureau/agency IT personnel immediately of any security events or incidents that might threaten or negatively impact the integrity or availability of iQMIS. The bureau/agency will ensure that policy and procedures are in place such that apparent security violations are to be investigated, and remedial action taken."

The iQMIS Information System Owner is responsible for operational oversight and management of the system's security and privacy controls and ensuring to the greatest possible extent that agency data is properly managed and that all access to data has been granted in a secure and auditable manner. The iQMIS Information System Owner, Information System Security Officer, and authorized users are responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, the customer agency and appropriate DOI officials in accordance with Federal policy and established DOI procedures. Each customer agency is responsible for the management of their data and reporting of any potential loss, compromise, unauthorized access, or disclosure of data resulting from their activities or

management of the data.

Section 8: Incident Response and Review

1. In the event of a privacy breach, what steps will be taken to mitigate harm, notify affected individuals, and report to oversight agencies?

Loss, compromise, unauthorized disclosure, or unauthorized access of PII is considered a "security incident". The ISO and all authorized users must report to DOI Cyber Incident Report Council (DOI-CIRC) within one hour of discovery. BFGA will follow incident response procedures mentioned in the DOI Privacy Breach Response Plan. Those procedures consist of:

1. Immediate Reporting within one (1) hour of discovery;
2. Containment and mitigation to prevent further loss;
3. Risk Assessment to determine the scope and nature of the breach;
4. Notification, if required;
5. Oversight reporting, if required; and
6. Remediation and prevention to prevent recurrence.

2. How often will this PIA be reviewed and updated to reflect changes in privacy risks or system operations?

This PIA will be reviewed periodically in accordance with the system's continuous monitoring plan and updated to reflect when major changes occur to the system's technology, data, or operations that could affect privacy risks.