



United States Department of the Interior

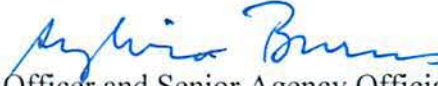
OFFICE OF THE SECRETARY

Washington, DC 20240

NOV 09 2016

OCIO DIRECTIVE 2016-003

To: Heads of Bureaus and Offices
Associate Chief Information Officers

From: Sylvia Burns 
Chief Information Officer and Senior Agency Official for Privacy

Subject: Department of the Interior Mobile Applications Privacy Policy

1. Purpose. The dramatic growth of mobile solutions to support the mission of the Department of the Interior (DOI) creates privacy risk and presents challenges for protecting individual privacy and the security of DOI information and information systems. This policy establishes privacy roles, responsibilities, and requirements for the development and management of Mobile Applications intended for use by DOI employees and/or the public.

2. Scope. This policy applies to all DOI bureaus and offices, their supporting organizations, and contractors for Mobile Applications that are developed by, on behalf of, or in coordination with DOI.

3. Definitions.

- a. DOI Mobile Application. A native software application that is developed by, on behalf of, or in coordination with DOI for use on a mobile device (e.g., phone or tablet) by DOI employees and/or the public. Hybrid mobile applications used or developed with native application are also included within the scope of this policy.
- b. Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- c. Information System Lifecycle. All phases in the useful life of an information system, including planning, acquiring, operating, maintaining, and disposing.
- d. Location Information. The ability of a mobile device to know a user's current location and/or location history as determined by Global Positioning System (GPS) and/or other methods.
- e. Metadata. The information stored as the description of a unique piece of data and all the properties associated with it. Metadata identifies, describes, explains, and provides content, context, structure and classifications pertaining to an organization's data and enables effective discovery, retrieval, usage, and management of data. For example,

mobile device metadata may include the time and duration of all phone calls made from a particular mobile device, the mobile device IDs of the mobile devices involved in the phone calls, and the locations of each participant when the phone calls occurred.

- f. **Mobile Device ID.** A unique serial number that is specific to a mobile device. These numbers vary in permanence, but typically a device has at least one permanent number. These numbers are used for various purposes, such as for security and fraud detection and remembering user preferences. Combining a unique device identifier with other information, such as location data, can allow the phone to be used as a tracking device.

- g. **Personally Identifiable Information (PII).** Any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. For example, such information may include a name, username, Social Security number, date and place of birth, phone number, home address, email address, credit card number, account number, driver's license number, vehicle license number, photograph, biometric identifier (e.g., facial recognition, fingerprint), educational information, financial information, medical information, criminal or employment information, or any information created specifically to identify or authenticate an individual (e.g., a random generated number). Sensitive PII is PII which, if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some types of PII, such as Social Security numbers, credit card numbers, and biometric identifiers, are always sensitive and must be safeguarded against unauthorized disclosure. Some types of PII may become sensitive PII when maintained or combined with other types of PII or identifying information about the individual. The context surrounding the use of PII is also important to determine whether it is sensitive PII. For example, a list of employee names by itself may not be considered sensitive PII, but a list of employees who received poor performance ratings is sensitive PII.

- h. **Privacy Act Statement.** A disclosure statement provided to an individual when PII is directly collected for a Privacy Act system of records. The Privacy Act Statement provides the legal authority and purpose for the collection, the routine uses of the information and who will have access to the information, and discloses whether providing the information is voluntary or mandatory, and any consequences for not providing the information. The Privacy Act Statement may be provided on a form, in a separate handout, read to the individual, or prominently posted.

- i. **Privacy Notice.** A notice that informs individuals of activities that may have privacy implications, and discloses some or all the ways PII may be gathered, used, managed and disclosed. A Privacy Notice is provided when PII is present or collected but may not necessarily be maintained in a Privacy Act system. The Privacy Notice has the same requirements as a Privacy Act Statement and must include the authority and purpose for collecting information, the uses of information, any sharing or dissemination of

information, and the consequences of not providing information. A Privacy Notice may also be called a Privacy Act Statement.

- j. Privacy Control. The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.
- k. Privacy Impact Assessment (PIA). An analysis and a formal document detailing the process and the outcome of the analysis that is required whenever an information technology (IT) system, technology, program, project, information collection, or other activity involves the use of PII, has privacy implications, or otherwise impacts individual privacy. A PIA is a tool that analyzes privacy risk and describes what information DOI is collecting, why the information is being collected, how the information is used, stored, and shared, how the information may be accessed, how the information is protected from unauthorized use or disclosure, and how long information is retained.
- l. Program Manager. The responsible agency official who is uniquely empowered to make final scope-of-work, capital investment, and performance acceptability decisions.
- m. Security Control. The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.
- n. System Manager. The individual identified in a Privacy Act system of records notice who is responsible for the operation and maintenance of the system of records to which the system of records notice pertains.
- o. System Owner. The official responsible for the overall procurement, development, integration, modification, or operation and maintenance of information systems. The System Owner implements the information resources management requirements such as privacy, security, and records.
- p. System of Records Notice (SORN). The statement providing the public notice of the existence and character of a group of any records under the control of any agency in which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires that this notice be published in the *Federal Register* upon establishment or substantive revision of a system of records, and establishes what information about the system must be included.
- q. User. Individual using a DOI Mobile Application.

4. Responsibilities. Each DOI bureau and office shall establish its own privacy procedures and practices for the implementation of this policy, which shall conform to and incorporate the following Departmental requirements.

- a. The Senior Agency Official for Privacy (SAOP) is the official with overall authority and responsibility for implementing and managing an agency-wide governance and privacy program, and overseeing data protection and compliance activities in alignment with Federal privacy laws, regulations, and policies. The SAOP is responsible for:
 - (i) Formulating and implementing privacy policies, procedures, and standards to ensure full compliance with Federal privacy laws and policies relating to the protection of information privacy;
 - (ii) Overseeing, coordinating, and facilitating DOI's privacy compliance activities;
 - (iii) Establishing privacy requirements in the risk management framework in accordance with Office of Management and Budget (OMB) policy and National Institute of Standards and Technology (NIST) guidelines; and
 - (iv) Conducting assessments and periodic reviews to identify deficiencies and manage privacy risk, and approving the selection of privacy controls to mitigate privacy risk related to the collection, use, processing, storage, maintenance, disclosure or disposal of PII.

- b. The Departmental Privacy Officer (DPO) carries out the privacy functions delegated by the SAOP, and is responsible for managing an agency-wide privacy program to carry out administrative, management and compliance activities to ensure compliance with Federal privacy laws, regulations and policies. The DPO is responsible for:
 - (i) Providing guidance and working with Departmental, bureau and office officials to ensure that use of DOI Mobile Applications complies with DOI privacy policies;
 - (ii) Conducting assessments of privacy controls, and reviewing and approving privacy impact assessments and compliance documentation submitted by bureaus and offices for DOI Mobile Applications, as appropriate;
 - (iii) Coordinating with System Owners, Program Managers, System Managers, developers, and legal counsel, as appropriate, to complete privacy compliance reviews and documentation for proposed DOI Mobile Applications;
 - (iv) Performing periodic privacy compliance reviews of DOI Mobile Applications to ascertain compliance with DOI privacy policy; and
 - (v) Reporting issues and status of oversight activities to the SAOP as necessary to

ensure compliance with Federal laws and mandates.

- c. Associate Privacy Officers (APOs) are responsible for managing bureau or office privacy programs in alignment with the DOI Privacy Program, and overseeing privacy activities for their respective organizations to ensure compliance with Federal privacy laws, regulations, policies, and Departmental privacy policy and standards. The APOs are responsible for:
 - (i) Serving as the primary contact between the DPO and the bureau or office on privacy program activities, including the conduct of privacy assessments on the official use of mobile applications;
 - (ii) Providing guidance to System Owners, Program Managers, System Managers, and developers on the privacy policy for the use of mobile applications, and collaborating to ensure privacy requirements are met and controls are implemented to safeguard PII;
 - (iii) Coordinating and overseeing privacy assessments on mobile applications and ensuring their use complies with Federal requirements and DOI privacy policies;
 - (iv) Performing periodic privacy reviews of mobile applications to ensure ongoing compliance with DOI privacy policy; and
 - (v) Reporting status of privacy activities for mobile applications to the DPO as needed to ensure privacy protections and requirements are implemented.

- d. System Owners, Program Managers, and System Managers are agency officials who are responsible for making decisions on the procurement, development, integration, modification, or operation and maintenance of information systems; the collection or maintenance of Privacy Act system of records; or information resources management requirements such as privacy, security, and records. Roles and responsibilities for these officials may vary depending on the specific application and are also outlined in other DOI privacy and security policies. See definitions in Section 3 above, as well as the DOI PIA Guide, DOI Privacy Control Standards, DOI Security Control Standards, and NIST Special Publication (SP) 800-53. System Owners, Program Managers, and System Managers, as appropriate, are responsible for:
 - (i) Coordinating with APOs to ensure that privacy risks are identified, evaluated and appropriately addressed, and privacy compliance documentation is completed when proposing, developing, implementing, or changing DOI Mobile Applications;
 - (ii) Engaging and coordinating with appropriate bureau/office and Office of the Chief Information Officer (OCIO) officials to ensure all applicable information

assurance requirements and processes are completed when proposing, developing, implementing, or changing DOI Mobile Applications;

- (iii) Monitoring the design, deployment, operation, and retirement of DOI Mobile Applications to ensure that collection and use of PII is limited to what is authorized and described in the privacy compliance documentation;
 - (iv) Collaborating with APOs and Associate Chief Information Security Officers (ACISOs) to establish administrative, technical, and physical controls for storing and safeguarding PII consistent with DOI privacy, security, and records management requirements to ensure the protection of PII from unauthorized access, disclosure, or destruction as it relates to DOI Mobile Applications;
 - (v) Meeting the requirements of the Privacy Act for any collection or maintenance of information from individuals, including publication of notices, and maintaining and updating required privacy documentation as necessary for the development and use of DOI Mobile Applications during the entire information system lifecycle; and
 - (vi) Ensuring the development and use of DOI Mobile Applications complies with all Federal laws, regulations, OMB mandates, NIST guidelines and DOI policy.
- e. Associate Chief Information Officers (ACIOs) are officials responsible for overseeing privacy and security programs, and IT resources for their respective bureau or office, and working with the SAOP, DPO, APOs and ACISOs to issue policy, implement procedures, and ensure information management and assurance activities are in compliance with Federal laws, regulations, and policies. ACIOs are responsible for:
- (i) Implementing and overseeing vetting and assessment procedures for the development, management and approval of mobile applications for their respective organizations;
 - (ii) Engaging with appropriate OCIO officials to ensure all applicable information assurance requirements and processes are completed when proposing, developing, implementing, or changing DOI Mobile Applications; and
 - (iii) Overseeing the assessment and approval process to ensure that privacy risks are identified, evaluated and appropriately addressed, and privacy compliance documentation is completed for development of DOI Mobile Applications for their respective organizations prior to deployment.
- f. Associate Chief Information Security Officers are responsible for the oversight of bureau or office information security programs and establishing security policy and procedures

to manage the security state of organizational information systems through the security authorization processes. ACISOs are responsible for:

- (i) Collaborating with privacy officials to implement safeguards to protect PII collected, created, processed, or maintained from the use of DOI Mobile Applications from loss, theft, misuse, unauthorized access, destruction, unauthorized modifications or disclosure;
- (ii) Serving as the primary information security contact for the bureau or office on security program activities, including requirements for security control assessments for the official use of DOI Mobile Applications;
- (iii) Providing guidance on security controls, procedural requirements and remediation to System Owners, Program Managers, System Managers, and developers for the development and use of DOI Mobile Applications; and
- (iv) Engaging with appropriate officials to ensure applicable information assurance requirements and processes are completed for the development and of DOI Mobile Applications.

5. Minimum Privacy Requirements for DOI Mobile Applications. The use of Mobile Applications raises distinct privacy implications that must be addressed prior to deployment. Location data, pictures, contact, passwords, and credit card numbers are just a few examples of the sensitive data that may be collected and transmitted through a Mobile Application. Mobile Applications are subject to all the same Federal laws, regulations, policies and standards as other applications developed and managed by DOI. This includes all privacy and security requirements, such as privacy impact assessments, publication of Privacy Act notices, and security authorization where applicable. Any development, deployment, or use of DOI Mobile Applications must meet the requirements of the Privacy Act of 1974; E-Government Act of 2002; Federal Information Security Modernization Act (FISMA) of 2014; the Paperwork Reduction Act of 1995; OMB Circular A-130, OMB M-03-22, and other related OMB policies; DOI Privacy Act regulations at 43 CFR Part 2, Subpart K; 383 Departmental Manual chapters 1-13; DOI PIA Guide; DOI Privacy Control Standards; DOI Security Controls Standards; and other applicable laws, regulations, policies and standards. The policies detailed below provide the baseline privacy requirements for DOI Mobile Applications. Additional privacy protections may be necessary depending on the purpose and capabilities of each mobile application.

a. Provide Notice

- (i) **Application-Specific Privacy Notice.** Each DOI Mobile Application must have a Privacy Notice that is easily accessible to users through the commercial application store before installation, as well as within the application itself after installation. The Privacy Notice should be application-specific and cannot merely reference the official DOI website Privacy Policy. The Privacy Notice should

briefly describe the application's information practices to include the collection, use, sharing, disclosure, and retention of PII. The Privacy Notice should also address redress procedures, application security, and the Children's Online Privacy Protection Act (COPPA) (when applicable). These requirements are detailed in Section 208 of the E-Government Act of 2002, OMB Circular A-130, OMB M-03-22, and NIST SP 800-53.

- (ii) **Privacy Act Statement.** If a DOI Mobile Application is collecting PII from users for a Privacy Act system, then a Privacy Act Statement must be provided at the point of collection in accordance with the Privacy Act of 1974. This Privacy Act Statement may be provided through a pop-up notification on the DOI Mobile Application screen where PII is collected or via other approved mechanism in consultation with the APO. This requirement applies when collecting information from both Federal employees and members of the public. These requirements are detailed in the Privacy Act, 5 U.S.C. 552a(e)(3), Section 208 of the E-Government Act of 2002, OMB Circular A-130, OMB M-03-22, and NIST SP 800-53. The Privacy Act Statement must include:
 - (a) The legal authority that authorizes the collection of PII;
 - (b) The principal purpose(s) for which the information is collected and intended to be used;
 - (c) The routine uses for the PII;
 - (d) With whom the PII will be shared;
 - (e) The applicable System of Records Notice(s); and
 - (f) Whether the provision of information is mandatory or voluntary, and any consequences or effects on the individual for not providing the requested information.
- (iii) **Contextual Notice.** DOI Mobile Applications deliver direct, contextual, self-contained notices about the uses of information through the mobile platform. Therefore, these notices should be:
 - (a) Provided upon each update to the mobile application to specifically identify any changes to the uses of information from previous versions of the application;
 - (b) Provided as "just-in-time" disclosures and obtain users' affirmative express consent before DOI Mobile Applications access sensitive content or other tools and applications on the mobile device for the first time (e.g.,

location services); and

- (c) Provided with independent opt-out features so that users may customize the mobile application's features (e.g., opting out of location-based services while still choosing to utilize other application services), where appropriate.

b. Limit the Collection and/or Use of Sensitive Content

- (i) DOI Mobile Application features cannot collect and/or use PII unless the collection is authorized and directly needed to achieve a DOI mission purpose;
- (ii) If the collection and/or use of PII is directly necessary to achieve a DOI mission purpose, the collection and/or use of the information must be documented and justified in the mobile application's PIA;
- (iii) Any collection, use and maintenance of PII must be kept to the minimum necessary to achieve the DOI mission in accordance with DOI privacy policy, OCIO Directive 2007-005, *Departmental Strategy to Safeguard Personally Identifiable Information and Reduce the Collection and Uses of Social Security Numbers*, and Federal law, policy and standards; and
- (iv) The collection, use and maintenance of sensitive PII must have specific legal authority, be maintained in secure DOI systems with adequate controls to safeguard the PII, be included in the bureau or office PII inventory, have been assessed by the APO for adequacy, and meet any necessary procedural requirements and approvals by the SAOP.

c. Establish Guidelines for User Submitted Information

- (i) Where feasible, use forms and check boxes to limit data collection and minimize data entry errors;
- (ii) Before allowing a user to submit information to DOI, provide a "review before sending" function that allows users to correct or opt-out of sending their information to the Department;
- (iii) Use prompts to obtain user consent for the collection, use and disclosure of PII, and for each update that affects these PII activities;
- (iv) Unless necessary to achieve a DOI mission purpose, limit the ability of users to post information within the application that other users may access or view. This limits the potential for users to share PII unnecessarily; and

- (v) Mask characters for sensitive data in page displays.

d. Ensure Mobile Application Privacy and Security

- (i) Establish a vetting process to evaluate the privacy and security of mobile applications in accordance with Federal policy, NIST SP 800-163, *Vetting the Security of Mobile Applications*, and related policies and standards. This vetting process should include privacy and security assessments, testing for vulnerabilities, and a process for the ACIO and approving officials to evaluate the assessments and results of the testing for conformance with Federal and DOI requirements prior to approval and deployment of mobile applications;
- (ii) Engage with bureau/office privacy and security officials, and the OCIO as necessary, early and throughout development to ensure the security and privacy requirements are met, risk is appropriately identified and mitigated, and adequate controls are implemented to safeguard user PII and the DOI environment;
- (iii) If users submit information through a DOI Mobile Application, ensure that information is encrypted in transit and immediately transferred to a protected DOI system that is compliant with Federal law and DOI policy;
- (iv) Any sensitive data transferred or stored must be protected by encryption methods that meet Federal requirements, Federal Information Processing Standard (FIPS) 140-2 and approved DOI practices for cryptographic protection of Federal information;
- (v) Sensitive content that a DOI Mobile Application accesses or uses for the benefit of the user, but that DOI does not need to collect (e.g., location information), should be locally stored within the mobile application or mobile device. This information should not be transmitted to or shared with DOI;
- (vi) Ensure PII is used only for authorized purposes and is protected during each stage of the information lifecycle; and
- (vii) Establish rules of behavior and clarify roles and responsibilities within the organization for the vetting process and the development and use of mobile applications.

6. DOI Mobile Application Development.

- a. System Owners, Program Managers, and System Managers must notify their APO before engaging in the development of a DOI Mobile Application.
- b. APOs engage with System Owners, Program Managers, System Managers, and

developers to ensure privacy controls are implemented and safeguards are integrated into the development and use of the DOI Mobile Application.

- c. Before deployment, the DOI Mobile Application goes through a compliance review process that includes privacy, security, information collection clearance, records management, and legal as necessary to address specific issues related to the use of the mobile application and any collection of information from the public. Program officials and developers are responsible for contacting these officials for consultation on additional requirements. For example, a legal review for compliance with COPPA must be conducted if a mobile application engages with children; or the bureau/office Information Collection Clearance Officer must be contacted for a review for any necessary OMB approvals for a survey or collection of information from ten or more members of the public.
- d. Bureau/office privacy and security officials engaged in the vetting or compliance review process will conduct appropriate assessments and meet procedural requirements to ensure compliance with Federal and DOI requirements, and provide results and recommendations to System Owners, Program Managers, or System Managers.
- e. Before deployment, System Owners, Program Managers, and System Managers must collaborate with APOs to complete a PIA, Application-Specific Privacy Notice, and Privacy Act Statement (if necessary) for the DOI Mobile Application. In accordance with the DOI PIA Guide, the PIA must (1) document a general description of the proposed use; (2) identify the legal authorities for the proposed use; (3) describe what PII, if any, is collected, from whom PII is collected, and how the PII is used; and (4) analyze any privacy risk and the privacy and security controls implemented to mitigate that risk.
- f. Before deployment, the DOI Mobile Application's PIA, Application-Specific Privacy Notice, and Privacy Act Statement (if necessary) must be reviewed and approved by the APO. Approval should be based on a determination whether the DOI Mobile Application contains appropriate privacy safeguards, meets DOI security requirements to protect user PII and the DOI environment, and whether a new or updated PIA, SORN, or other documentation is required.
- g. The APO determines whether the necessary documentation is complete and the DOI Mobile Application contains appropriate privacy and security protections, and contacts the DPO for any required Departmental privacy approvals prior to the release and deployment of the DOI Mobile Application.
- h. DOI Mobile Applications go through the compliance review process any time there is a change made to the DOI Mobile Application that affects or potentially affects the user PII or handling of data, consistent with the PIA review cycle and privacy continuous monitoring program. Existing DOI Mobile Applications, which were developed before

the implementation of this policy, must complete the compliance review cycle within six months of this policy's issue date.

- i. System Owners, Program Managers, System Managers, and APOs promptly provide results pertaining to particular DOI Mobile Applications to the DPO upon request for evaluation to ensure that DOI Mobile Applications meet Federal and DOI privacy requirements and continue to contain appropriate privacy protections.

7. Retention and Disposal of PII. System Owners, Program Managers and System Managers, as appropriate, must maintain PII collected or created through the use of DOI Mobile Applications in accordance with approved records retention schedules, applicable system of records notices as appropriate, and Departmental privacy policy for the retention, minimization and disposal of PII. Privacy controls shall be implemented to ensure only minimum PII is collected as legally authorized, relevant and necessary to accomplish the DOI mission. Procedures must be established to protect PII during the entire information lifecycle regardless of media, and to delete, erase, or destroy PII when no longer needed to reduce privacy risk in alignment with records retention requirements. System Owners, Program Managers and System Managers are responsible for ensuring program staff, contractors, and partners adhere to these requirements and applicable records retention schedules, and that methods for disposal of PII are approved and secure in accordance with records retention schedules, 384 Departmental Manual 1, guidelines issued by the National Archives and Records Administration, and DOI privacy policy.

8. Privacy Compliance Reviews. The DPO, in collaboration with APOs, may conduct privacy compliance reviews of DOI Mobile Applications periodically to assess compliance with DOI privacy policy and standards.

9. Privacy Contact. For questions and comments on this policy, please contact the DOI Privacy Office at 202-208-1605. Please contact the appropriate bureau or office APO for questions related to specific privacy procedures and practices for the implementation of this policy.

10. Effective Date. This Directive is effective upon signature.

cc: Elizabeth Klein, Acting Principal Deputy Assistant Secretary, Policy, Management & Budget
Elena Gonzalez, Deputy Assistant Secretary, Technology, Information and Business Services
Departmental Privacy Officer
Chief Information Security Officer
Departmental Records Officer
Departmental Information Collection Clearance Officer

Departmental Section 508 Coordinator
Office of the Solicitor
Office of Inspector General
Associate Chief Information Officers
Associate Privacy Officers
Associate Chief Information Security Officers
Bureau and Office Records Officers
Bureau and Office Information Collection Clearance Officers
Bureau and Office Section 508 Coordinators