



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				Date	
MaaS360 Cloud Services				09-30-2015	
Bureau/Office			Bureau/Office Contact Title		
Office of the Chief Information Officer			Departmental Privacy Officer		
Point of Contact Email	First Name	M.I.	Last Name	Phone	
Teri_Barnett@ios.doi.gov	Teri		Barnett	(202) 208-1605	
Address Line 1					
1849 C Street NW					
Address Line 2					
Mail Stop 5547 MIB					
City			State/Territory		Zip
Washington			District of Columbia		20240

Section 1. General System Information

A. Is a full PIA required?

Yes

Yes, information is collected from or maintained on

Federal personnel and/or Federal contractors

B. What is the purpose of the system?

MaaS360 Cloud Services (MaaS360) is a major application that provides the Department of the Interior (DOI) with a consolidated cloud-based management platform for all of its mobile devices (iOS, Android, Windows) operated within the DOI environment. MaaS360 simplifies the management process by providing a consolidated portal environment for Bureau and Offices to monitor and manage the configuration, inventory, and security settings across their mobile devices. MaaS360 provides the ability to push patches and update configurations on user devices without impacting the user or to

have the device physically present. Other than the MaaS360 client application which is loaded on each device, the system does not impact the user experience and is transparent to users of DOI's mobile devices.

C. What is the legal authority?

Federal and DOI requirements require that Agencies manage their mobile device inventories, to include configuration management, asset management, and security configurations.

Departmental Regulations, 5 U.S.C. 301; The Paperwork Reduction Act, 44 U.S.C. Chapter 35; The Clinger-Cohen Act, 40 U.S.C. 11101, et seq.; Federal Information Security Modernization Act of 2014, 44 U.S.C. 3541 et seq.; OMB Circular A-130, Management of Federal Information Resources; Executive Order 13571, "Streamlining Service Delivery and Improving Customer Service," April 11, 2011; and Presidential Memorandum, "Building a 21st Century Digital Government," May 23, 2012.

D. Why is this PIA being completed or modified?

Existing Information System under Periodic Review

E. Is this information system registered in CSAM?

Yes

Enter the UII Code and the System Security Plan (SSP) Name

010-000000698; MaaS360 Cloud Services

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	Describe
None	None	No	

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)

DOI-47, HSPD12: Logical Security Files, 72 FR 11040, March 12, 2007

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

No

Section 2. Summary of System Data

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

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Religious Preference | <input type="checkbox"/> Social Security Number (SSN) |
| <input type="checkbox"/> Citizenship | <input type="checkbox"/> Security Clearance | <input type="checkbox"/> Personal Cell Telephone Number |
| <input type="checkbox"/> Gender | <input type="checkbox"/> Spouse Information | <input type="checkbox"/> Tribal or Other ID Number |
| <input type="checkbox"/> Birth Date | <input type="checkbox"/> Financial Information | <input type="checkbox"/> Personal Email Address |
| <input type="checkbox"/> Group Affiliation | <input type="checkbox"/> Medical Information | <input type="checkbox"/> Mother's Maiden Name |
| <input type="checkbox"/> Marital Status | <input type="checkbox"/> Disability Information | <input type="checkbox"/> Home Telephone Number |
| <input type="checkbox"/> Biometrics | <input type="checkbox"/> Credit Card Number | <input type="checkbox"/> Child or Dependent Information |
| <input type="checkbox"/> Other Names Used | <input type="checkbox"/> Law Enforcement | <input type="checkbox"/> Employment Information |
| <input type="checkbox"/> Truncated SSN | <input type="checkbox"/> Education Information | <input type="checkbox"/> Military Status/Service |
| <input type="checkbox"/> Legal Status | <input type="checkbox"/> Emergency Contact | <input type="checkbox"/> Mailing/Home Address |
| <input type="checkbox"/> Place of Birth | <input type="checkbox"/> Driver's License | |
| <input checked="" type="checkbox"/> Other | <input type="checkbox"/> Race/Ethnicity | |

Specify the PII collected.

User/Administrator work email addresses, Work Phone number, user name of device owner.

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

- | | | | |
|--|--|---|---|
| <input checked="" type="checkbox"/> Individual | <input type="checkbox"/> Tribal agency | <input checked="" type="checkbox"/> DOI records | <input type="checkbox"/> State agency |
| <input type="checkbox"/> Federal agency | <input type="checkbox"/> Local agency | <input type="checkbox"/> Third party source | <input checked="" type="checkbox"/> Other |

Describe

DOI System - BisonConnect. Individuals request mobile devices as part of their request they provide their name (first, last), which also constitutes their username. Once the device is enrolled it will synchronize information between the device and DOI's email system, BisonConnect, which includes their business contact information.

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

- | | | | |
|---|---|---|--|
| <input type="checkbox"/> Paper Format | <input type="checkbox"/> Face-to-Face Contact | <input type="checkbox"/> Fax | <input type="checkbox"/> Telephone Interview |
| <input checked="" type="checkbox"/> Email | <input type="checkbox"/> Web Site | <input checked="" type="checkbox"/> Other | <input checked="" type="checkbox"/> Information Shared Between Systems |

Describe

DOI policy requires that all mobile devices operated within the DOI environment are enrolled and managed by MaaS360. Users may request a device through email or a bureau/office form, or may be issued a device from their organization depending on each bureau/office internal process. Once a device is issued to a user, it is enrolled into MaaS360 and receives the default security configuration policy. MaaS360 regularly queries the device to validate that the configuration is still implemented and will provide a complete inventory of the device settings, including installed applications, configuration settings, hardware settings, and patch status.

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

PII collected generally includes work-related information such as the user's official email address, which may include the user's First Initial and Last Name or First Name and Last Name. This information is used to identify to whom the device is assigned, and manage and secure mobile devices in accordance with Departmental policies.

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 or office and how the data will be used.

MaaS360 is a Department-wide application. Each Bureau/Office Mobile Device Manager (MDM) administrator has access only to their bureau/office Portal and has the ability to review and manage accounts and devices assigned to their respective bureau/office.

- Other Bureaus/Offices

- Other Federal Agencies
- Tribal, State or Local Agencies
- Contractor
- Other Third Party Sources

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.

Users voluntarily provide their user name and official email address when they make a request for a government-issued mobile device, as well as consent to use of that information to issue and manage the device. User names are used to identify to whom the device has been issued. Users may not consent to uses of their information as user name and official address are required to manage and associate mobile devices issued to the user. For example, if a user refuses to provide a user name when upon request then the user will not be issued a mail-enabled smart phone. Each bureau/office has internal procedures, forms and Rules of Behavior that cover the requirements and management of government-issued equipment so there are numerous methods that users may receive notice and opportunity to consent when requesting devices or equipment.

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

- Privacy Act Statement Privacy Notice Other None

Describe each applicable format.

Individuals are provided notice on how their information is managed through this privacy impact assessment and publication of the DOI-47, HSPD12: Logical Security Files, 72 FR 11040, March 12, 2007.

Each bureau/office has their own internal procedures, forms that cover requirements and management of government-issued equipment. These processes and forms may include bureau specific notice on the policies and requirements for acceptable use, expectation of privacy, and use of information collected for issuance and use of government-issued equipment. All employees are notified via Departmental policy, mandatory security awareness training, DOI Rules of Behavior and the DOI Warning Banner that employee use of government-issued equipment and the DOI network is subject to monitoring and information provided from individuals may be monitored to ensure the authorized use and security of DOI information and assets.

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

Data regarding the devices is manually generated through the MaaS360 portal. Data can be retrieved using many different criteria such as Device Name, Username, E-mail Address, Device type, Manufacturer, Model, Operating System, IMEI/MEID, Installed Date, Last Reported, Device ID, Platform Name, Mailbox Managed, and Managed status.

I. Will reports be produced on individuals?

No

Section 3. Attributes of System Data

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

Not applicable since data is not collected from sources other than DOI.

B. How will data be checked for completeness?

Not applicable since there is not a need to check for data completeness.

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

Once the device is registered in MaaS360 the information is synchronized continuously between the device and the

MaaS360 portal. As long as the user has an assigned device the information is current. In the event of termination, retirement or transferring to another job the device will be wiped and all information removed from MaaS360 in accordance with policy and records retention requirements. Each bureau/office has established processes and procedures for the removal of accounts and devices.

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

MaaS360 program records are maintained under the DOI Departmental Records Schedule 1 – Administrative bucket (DAA-0048-2013-0001-0013), which has been approved by the National Archives and Records Administration (NARA). These administrative and information technology records map to 1.4A1 Information Technology – System Maintenance and Use Records, and have a temporary disposition. Records are cut off when superseded or obsolete, and destroyed three years after cut-off. Some records may be maintained under DOI bureaus and offices records retention schedules and will be retained in accordance with those schedules as appropriate.

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

Data is maintained in the system as long as the user has the assigned device. Users who separate, retire, or are terminated will have their devices wiped using the MaaS360 console. All user data is removed from both the device and portal at that time in accordance with Departmental policy and records retention requirements. Each Bureau/Office has created individual processes and procedures for disposing of the data.

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 as the information maintained in the system is user name and official email address for the purpose of managing and securing mobile devices in accordance with Federal and Departmental security requirements.

MaaS360 is a cloud-based software as a service mobile device management (MDM) application that operates outside the DOI Assessment and Authorization boundary. MaaS360 is hosted in the cloud and managed by Fiberlink (www.fiberlink.com) with some administrative functions being performed by DOI administrative staff through a consolidated web-based portal. MaaS360 provides the ability to monitor devices and remotely wipe the device for security reasons. There are no physical components included in DOI's portion of the MaaS360 authorization boundary; controls consist of management and oversight capabilities. The administrative functions include user, device configuration, and security settings. The only interaction between MaaS360 and DOI is the validation of user devices and the enrollment into MaaS360 by administrators.

As the service provider, Fiberlink is responsible for the management and operation of the Cloud System as a Service (SaaS) managing the system configuration and ensuring that the appropriate security controls are implemented. As the cloud service provider Fiberlink administrators have access to all data contained within the cloud environment. Fiberlink administrators have undergone background investigations and per contract have no ownership to DOI data stored within the system.

DOI has the means to evaluate control descriptions, documentation, test results, and vulnerabilities that are identified. DOI devices are enrolled in the MDM solution to provide management and oversight of the devices. Communications between devices and the user interface to the management portal are encrypted using a FIPS 140-2 validated OpenSSL encryption module. DOI completed a System Security Plan to assesses the security controls for MaaS360 as part of the security authorization, and to meet requirements under the Federal Information Security Modernization Act of 2014 and National Institute of Standards and Technology (NIST). Continuous monitoring is conducted in conjunction by both the Fiberlink and DOI security team, and assessments are performed annually, and penetration testing and in-depth monitoring are conducted to ensure compliance with all vulnerability mitigation procedures. Also, the MaaS360 Information System Security Officer reviews the system security plan annually or when needed to ensure that the system maintains compliance with security requirements.

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 maintained is necessary to properly manage and secure government-issued mobile devices in accordance with Departmental policy.

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

No

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

No

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

No

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

Not applicable since the system does not derive new data.

F. Are the data or the processes being consolidated?

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

Developers

System Administrator

Contractors

Other

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

Device users do not have access to the MaaS360 console or system. System Administrators have access and their access is based on least privileges as required for official duties.

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?

Fiberlink is the contractor responsible for maintaining the system. MaaS360 is a cloud service and DOI only has limited access to the configuration and administration of the service. The DIAR (Department of the Interior) Clause 1452.224-1 "Privacy Act Notification (July 1996) (DEVIATION) is included in the contract. The contract is expected to be re-competed and will include appropriate Federal Acquisition Regulations (FAR) Clauses and privacy and security provisions to safeguard data.

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

No

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

No

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

Not applicable since information is not being collected as a function of monitoring individuals.

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

Device criteria is monitored, individual user activity is not monitored within the system. However, controls in place to

prevent unauthorized activity include access controls, least privileges, mandatory security and privacy training, DOI Rules of Behavior, and security audits to ensure compliance with Departmental security policy.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

- | | | | |
|---|--|---|--|
| <input checked="" type="checkbox"/> Security Guards | <input checked="" type="checkbox"/> Secured Facility | <input checked="" type="checkbox"/> Identification Badges | <input type="checkbox"/> Combination Locks |
| <input type="checkbox"/> Key Cards | <input type="checkbox"/> Closed Circuit Television | <input type="checkbox"/> Safes | <input checked="" type="checkbox"/> Locked Offices |
| <input type="checkbox"/> Locked File Cabinets | <input type="checkbox"/> Cipher Locks | <input type="checkbox"/> Other | |

(2) Technical Controls. Indicate all that apply.

- | | |
|---|---|
| <input checked="" type="checkbox"/> Password | <input checked="" type="checkbox"/> Intrusion Detection System (IDS) |
| <input checked="" type="checkbox"/> Firewall | <input type="checkbox"/> Virtual Private Network (VPN) |
| <input checked="" type="checkbox"/> Encryption | <input type="checkbox"/> Public Key Infrastructure (PKI) Certificates |
| <input checked="" type="checkbox"/> User Identification | <input type="checkbox"/> Personal Identity Verification (PIV) Card |
| <input type="checkbox"/> Biometrics | |
| <input type="checkbox"/> Other | |

(3) Administrative Controls. Indicate all that apply.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Periodic Security Audits | <input type="checkbox"/> Regular Monitoring of Users' Security Practices |
| <input type="checkbox"/> Backups Secured Off-site | <input checked="" type="checkbox"/> Methods to Ensure Only Authorized Personnel Have Access to PII |
| <input checked="" type="checkbox"/> Rules of Behavior | <input type="checkbox"/> Encryption of Backups Containing Sensitive Data |
| <input checked="" type="checkbox"/> Role-Based Training | <input checked="" type="checkbox"/> Mandatory Security, Privacy and Records Management Training |
| <input checked="" type="checkbox"/> Other | |

Describe

MaaS360 is a System as a Service (SAAS) provided by Fiberlink and has been evaluated against the requirements established by FedRAMP and is continuously monitored by the vendor as well as DOI security personnel for potential lapses in security.

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.

Fiberlink as the Cloud Service Provider is responsible under contract for maintaining the security and privacy of information contained within the system in accordance with FISMA, NIST Standards, and Privacy Act requirements. The MaaS360 system owner is responsible for protecting the privacy of individuals for this application and for addressing Privacy Act requests or complaints in consultation with the Privacy Officer. Procedures for submitting Privacy Act requests or complaints are outlined in DOI Privacy Act Regulations at 43 CFR Part 2, Subpart K available at <http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=43:1.1.1.1.2>, and in the published Privacy Act system of records notice, DOI-47, HSPD12: Logical Security Files.

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?

Contractors and system administrators with access to the data are responsible for reporting the loss, compromise, unauthorized disclosure or unauthorized access of data. This responsibility is described in DOI security and privacy policies, mandatory IT security and privacy training, and DOI Rules of Behavior. The System Owner is responsible for ensuring proper use of the data and the requirements for reporting incidents.