U.S. Department of the Interior Privacy Impact Assessment (PIA)

Draft sample of a PIA. Submitted as part of the Glacier National Park Camera System for Monitoring Logan Pass

Sophie Brochu, Matthew Catuccio, Ava Chadbourne, Philip Heney, Harish Suresh

2023

This sample privacy impact assessment was filled out for the proof-of-concept system that Worcester Polytechnic Institute student, created for the Logan Pass parking monitoring project. This form was filled out to the best of our ability as students who are not experts in federal privacy law. This draft version of the PIA form can be used as a reference to understand how to answer various questions but should not be submitted in its current state. For further guidance, the Department of the Interior PIA guide can be found here: https://www.doi.gov/sites/doi.gov/files/uploads/DOI-PIA-Guide-09-30-2014.pdf

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: Glacier National Park Logan Pass Monitoring System
Bureau/Office: National Park Service, Glacier National Park, IT
Point of Contact:
Note: Name and contact information of person filing the PIA

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on:

- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers

☒ All

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

B. What is the purpose of the system?

Visitation in Glacier National Park has increased dramatically since 2016, leading to severe overcrowding in parking lots such as Logan Pass. The Visitor Use Management (VUM) team at Glacier National Park seeks to address this problem by learning about how and when parking lots fill and driver and vehicle patterns in parking lots. One method the park is interested in trying to utilize is u ng cameras to track cars entering and leaving the parking lot. Because of the use of wildlife cameras, the monitoring system has

the potential to take images of car license plates and faces of visitors and employees. While collecting these forms of PII is not the intent of this system, a surveillance camera-based system will inherently collect them along with images of cars.

C. What is the legal authority?

The Electronic Freedom of Information Act (FOIA) Amendments of 1996, The Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995, National Parks Omnibus Management Act of 1998, Section 104, Executive order 13011 of July 16, 1996, "Federal Information Technology."

D. Why is this PIA being completed or modified?

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

E. Is this information system registered in CSAM?

☐ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*
☒ No

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

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Image capturing process	Collects images of cars exiting and entering	Yes	Images of cars can contain license plates and potentially faces of visitors.
Image processing	Process images to determine how many cars are exiting and entering at a time	Yes	The software needs to go through each image, which can contain license plates and the faces of visitors and staff. PII is not being extracted from the

			images and stored. The images are still stored on the SD card throughout this process. Once this process is completed, images are then deleted from the card.

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)*

☒ No

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

☐ Yes: *Describe*
Guide states: "If information is collected from the public, contact you Bureau Information Collection Clearance Officer to determine whether you need to obtain OMB approval"
☒ No

Section 2. Summary of System Data

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

☐ Name
☐ Personal Cell Telephone Number
☐ Personal Email Address
☐ Mailing/Home Address
☒ Other: *Specify the PII collected.* This monitoring system can collect images of license plates, make and model of vehicles, and the faces and bodies of visitors, employees, and volunteers.

This information (images) is gathered by game cameras, which are motion-detection surveillance cameras. After the images are processed, they will be deleted and the data is stored as a list of numbers of cars entering and exiting the parking lot, along with the time that the vehicles entered and exited.

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

☐ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☐ DOI records
☐ Third party source
☐ State agency
☒ Other: *Describe* The PII is created within the image collection system itself. The system takes images which is the source of the PII.

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

☐ Paper Format
☐ Email
☐ Face-to-Face Contact
☐ Web site
☐ Fax
☐ Telephone Interview
☐ Information Shared Between Systems
☒ Other: *Describe*

Motion detecting trail cameras collect and store the images on SD cards.

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

Images are intended to be used to count the number of cars entering and exiting the parking lot. This information can further be used to inform management and visitors of parking patterns at Logan Pass. For management, the information can be used to schedule staff and inform management strategies.

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

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.* Glacier National Park will be the only office that has access to the PII. The Visitor Use Management team will process any information gathered through this system. Collection of the SD cards may be completed by Visitor Service Assistants and other associated staff members.

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

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

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

☒ Contractor: *Describe the contractor and how the data will be used.*
The Visitor Use Management team hires independent contractors who may have access to this information. The information will be used in the same method as the VUM team. The images would be used for collecting data on cars entering and exiting the lot.

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

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

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

☒ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*
The system uses cameras in a public setting. Because the system is constantly collecting images, there is no way to opt out.

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

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

☐ Privacy Notice: *Describe each applicable format.*

☐ Other: *Describe each applicable format.*

☒ None

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

Personal information is not intended to be retrieved from this system. The data will be collected from the camera which requires a key to open the lock. The keys are only owned by the VUM team.

I. Will reports be produced on individuals?

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

☒ No

Section 3. Attributes of System Data

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

The vehicle monitoring system is not designed to use or store information about visitors after the images have been processed. Because storage of personal information is not the intended purpose, the information does not need to be checked for accuracy.

B. How will data be checked for completeness?

The vehicle monitoring system is not designed to use or store information about visitors after the images have been processed. Because storage of personal information is not the intended purpose, the information does not need to be checked for completeness.

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

Because the system is not using or storing information about individuals, the information will not need to be checked to determine if it is current.

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

Data in this system will be stored for no longer than one month. SD cards in the cameras will be collected every two weeks, and the images will be analyzed within 48 hours of the SD cards being collected. After images are analyzed, they will be deleted off the SD cards. Images should not be retained on any personal devices for any period of time.

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

After images are analyzed, they will be deleted off the SD card. SD cards have no memory or trash can, so once they are deleted, they cannot be found again.

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.

The collection of data using cameras in public has some security risks. The cameras are visible to the public and within reach, so if desired, they could possibly be vandalized, and the SD cards could potentially be stolen.

The collection of the SD cards has some risks as well. One of the major risks is a collector dropping or losing an SD card. While there is a procedure for safekeeping the SD cards, it is possible for an SD card to be misplaced or lost.

The image analysis has minimal risks. The major risk would be malware installed on the computer of a VUM team member. The system does not use the internet so there are minimal risks with the information getting leaked.

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 system is designed to understand parking lot dynamics at Glacier National Park. Many solutions that do not infringe on privacy have been explored and have not worked or been feasible.

☐ No

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

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

☒ No

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

☐ Yes: *Explanation*

☒ No

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

☐ Yes: *Explanation*

☒ No

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

The system does not derive new data or create previously unavailable data about an individual through data aggregation.

F. Are the data or the processes being consolidated?

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

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

☒ No, data or processes are not being consolidated.

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

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
Other: *Describe*

Software and hardware developers will need access to the system to improve it. The VUM team will be the only other group who will have access to the data once it is analyzed.

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

Users will have access to the data on a need-to-know basis. Access will be restricted to the VUM team and any developers that are hired.

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

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

The VUM team has worked with students from WPI to help create a proof of concept of this system. In order to make the analysis software stronger, it is expected that there will be contact with contractors or other students in the future.

☐ No

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

☒ Yes. *Explanation*
The system uses Artificial Intelligence along with cameras to monitor cars entering and exiting the parking lot.

☐ No

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

☒ Yes. *Explanation*

The images captured from the cameras have the potential to include images with identifying features along with the time they were captured. While this data cannot be collected in real time, it can be used to monitor past behaviors.
☐ No

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

Information regarding the location of an individual and behaviors of an individual can be extrapolated from the images collected from the cameras.

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

The system will be stored on government computers and will not be available to the public. The data will not be available on the internet, and neither will information regarding the system used. Only authorized users will have access to the analysis system as well as the stored data.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☐ Security Guards
☒ Key Guards
☐ Locked File Cabinets
☐ Secured Facility
☐ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☐ Locked Offices
☒ Other. *Describe*

The cameras that are collecting images are locked using a padlock and locked to the mount using a cable lock. Both locks need a key to be unlocked. Identification badges are needed to access the government computers that have the analysis software and datasets stored.

(2) Technical Controls. Indicate all that apply.

☒ Password
☐ Firewall
☐ Encryption
☒ User Identification
☐ Biometrics
☐ Intrusion Detection System (IDS)
☐ Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☒ Other. *Describe*

The data storage and information is stored on government computers that require PIV cards and passwords to access. If the data is stored on a shared drive, a password will be necessary to login to an account that has access to this information.

(3) Administrative Controls. Indicate all that apply.

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

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

The VUM team is responsible for the safe use and handling of the data. The VUM team is collecting the information and therefore it is their responsibility to ensure the privacy rights of the public and employees are not violated.

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

The VUM team is responsible for assuring proper use of the data and reporting any compromise to the safe storage and proper use of the information. This team is responsible for the collection and analysis of all information and is therefore responsible for keeping the information safe and reporting if anything goes wrong with the collection or storage of this data.

For more information: https://www.doi.gov/sites/doi.gov/files/uploads/DOI-PIA-Guide-09-30-2014.pdf