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: United States Park Police Pre-Employment Suitability Determination Process
Bureau/Office: National Park Service / United States Park Police
Date:
Point of Contact:
Name: Richard Pope
Title: Commander, Training Branch
Email: Richard_Pope@nps.gov
Phone: 202-610-3529
Address: 1100 Ohio Dr SW Washigton DC 20024

Section 1. General System Information

A. Is a full PIA required?

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

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

B. What is the purpose of the system?

The purpose of the system is to provide the United States Park Police with information to determine suitability of a potential candidate for the purpose of employment as a Police officer with the United States Park Police.

The United States Park Police only collects information that is necessary to assess the suitability of candidates during the pre-employment suitability determination process to determine if they meet the qualifications and standards required to become federal law enforcement officers with the United Stated Park Police.

C. What is the legal authority?

U.S.C. Title 54, 5 U.S.C. 3301, 3302, 3307, 3309, 3313, and Executive Order 9397

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?
The completed PIA, associated system of records notice(s), and any other supporting artifacts must be entered into the CSAM system for each registered system or application.

☐ 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.*
NONE	NONE	N/A	N/A

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

☒ Yes:

OPM/GOVT–5 Recruiting, Examining, and Placement Records

☐ No

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

☒ Yes: OMB Control # 1024-0245
☐ No

Section 2. Summary of System Data

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

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

☐ Other: *Specify the PII collected.*

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 United States Park Police Pre-Employment Suitability Determination Process System collects personal information from individuals that apply for employment and have been identified as candidates for employment. Additional information on candidates is collected through other federal, state and local government systems and through third party sources such as credit bureaus.

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*

The United States Park Police Pre-Employment Suitability Determination Process System collects personal information from individuals that apply for employment and have been identified as candidates for employment. Additional information on candidates is collected through other federal, state and local government systems and through third party sources such as credit bureaus. This information is collected via electronic systems available to this law enforcement agency.

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

The information collected will be used to review an individual qualifications for employment in connection with the pre-employment qualification determination phase of the United States Park Police application process.

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.*

The information is used within the Department of Interior's Office of Law Enforcement and Security (OLES), Personnel Security Office to receive an initial waiver for security clearances. This waiver is granted by the Director of OLES in order to hire candidates and assign them to the Federal Law Enforcement Training Center (FLETC). This process is essential due to a long-standing backlog of clearance investigations within the Office of Personnel Management. The backlog does not allow the United States Park Police to meet FLETC's class registration deadlines due to policy compliance which designates security clearance levels of candidates prior to attending FLETC.

☐ 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.*

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOI as a routine use pursuant to 5 U.S.C. 552a(b)(3) to other Federal agencies as described under the routine uses for the system of records notice "OPM/GOVT–5 Recruiting, Examining, and Placement Records" when the disclosure is compatible with the purpose for which the records were compiled.

☐ 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.*

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

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOI as a routine use pursuant to 5 U.S.C. 552a(b)(3) to other third party sources as described under the routine uses for the system of records notice "OPM/GOVT–5 Recruiting, Examining, and Placement Records" when the disclosure is compatible with the purpose for which the records were compiled.

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.*

Individuals may decline to provide information. They are informed that this will impede the ability to properly determine their suitability for employment and they may be removed from the process.

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

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

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

A privacy act statement is provided on all the forms used to collect the information.

☐ 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.).

Records in this system can be retrieved by name and date of birth. If records are similar at this level other data such as abbreviated SSN and other personal identifiers may be used.

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?

Information will be cross checked with the information supplied by the applicant; then confirmed in a follow up interview of applicant.

B. How will data be checked for completeness?

Information in these records is reviewed and confirmed by a law enforcement official with the individual who supplies the information during a personal interview.

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

Information is entered by the individual and is only as current as that provided by the correspondent.

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

At NPS, the records are subject to the NPS Management and Accountability Records Schedule; records are destroyed 7 years after closure. The information is maintained for cross comparison in out years due to applicants applying multiple times for this position. Temporary records that have met their retention period are approved for destruction. Approved destruction methods for temporary records include shredding or pulping paper records, and erasing or degaussing electronic records in accordance with 384 Departmental Manual 1 and National Archives and Records Administration (NARA) guidelines.

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

At NPS, the records are subject to the NPS Management and Accountability Records Schedule; records are destroyed 7 years after closure. The information is maintained for cross comparison in out years due to applicants applying multiple times for this position. Temporary records that have met their retention period are approved for destruction. Approved destruction methods for temporary records include shredding or pulping paper records, and erasing or degaussing electronic records in accordance with 384 Departmental Manual 1 and National Archives and Records Administration (NARA) guidelines.

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.

Privacy risks to the individual is minimized by the implementation of security and privacy controls. The records contained in this system are safeguarded in accordance with 43 CFR 2.226 and other applicable security rules and policies. Access to records in the United States Park Police System is limited to authorized personnel whose official duties require such access. Paper records are secured in file cabinets in areas which are locked during non-duty hours. Information is maintained in locked file cabinets within locked offices which are located in facilities which are staffed by law enforcement 24 hours a day 7 days a week or in an alarmed facility with other physical security measures when not occupied by law enforcement.

All authorized users are trained and required to follow established internal security protocols and must complete all security, privacy, and records management training and sign the DOI Rules of Behavior.

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 collection allows for the most efficient and effective way for the United States Park Police to screen and process thousands of applicants for a small number of positions. The information allows us to properly determine a candidate's suitability for employment as a federal law enforcement officer.

☐ 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: The information will be transferred to the individuals United States Park Police Personnel Security file upon hiring by the United States Park Police.

☐ No

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

☒ Yes: The information will be used to determine suitability for hire as a federal law enforcement officer.

☐ No

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

Confirmation through other government law enforcement systems and through individual interviews.

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*

Personnel assigned to determining the suitability of a candidate for employment would be granted access to paper files (collection) submitted by the applicant. The information within the paper files (collection) is available on a need to know basis and would only confirm what was submitted by the applicant.

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

Access to data in the system based on the least privilege access and for an official need to know.

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?*

☒ No

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

☐ Yes. *Explanation*

☒ No

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

☐ Yes. *Explanation*

☒ No

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

N/A

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

The roles per individual are assigned locally by the Commander, Training Branch. Access to these records is only granted to those persons within the United States Park Police, or others who are specifically authorized by the United States Park Police. Access levels and permission levels have been established and assigned only to those persons who have a need to know the information in order to carry out their official duties.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

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

(2) Technical Controls. Indicate all that apply.

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

(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 Commander, Training Branch, United States Park Police and the United States Park Police Records Manager will be responsible for the records and administrative functions required by the collection.

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 Commander, Training Branch, United States Park Police and the United States Park Police Records Manager and the official responsible for oversight and management of the security and privacy controls and for ensuring to the greatest possible extent that agency data is properly managed and that all access to agency data has been granted in a secure and auditable manner.