

**Department of the Interior Privacy Impact Assessment Name of Project: National Park Service General Support System (NPS GSS) Bureau: National Park Service Project's Unique ID: WAN DOI-NPS-**

**G-002** Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- Bureau/office IT Security Manager
- Bureau/office Privacy Act Officer
- DOI OCIO IT Portfolio Division
- DOI Privacy Act Officer

**Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division.**

**Also refer to the signature approval page at the end of this document.**

**A. CONTACT INFORMATION:**

**Who is the Bureau/Office Privacy Act Officer who reviewed this document?** (Name, organization, and contact information).

Felix A. Uribe  
Privacy Officer  
Bureau Chief of Information Security Office  
1201 Eye St. NW, Washington, DC 20005  
Telephone: 202-354-6925  
Email: felix\_uribe@nps.gov

**B. SYSTEM APPLICATION/GENERAL INFORMATION:**

**1) Does this system contain any information about individuals?** No

The NPS One GSS consists of the entire local area network structure in WASO, regions, parks and other centers, wherever their location. It includes desktops, servers and all other ancillary equipment appended to or

communicating with the infrastructure. It includes enterprise software resident on the GSS, such as the operating system, anti-virus software, firmware, and office automation products that support other applications. It also includes Personal Digital Assistant (PDAs) and any other device that communicates with the GSS.

The NPS One GSS currently supports three major applications: Facility Management Software System (FMSS), Point of Sale System (POSS), and Accounting Operations Center General Support System (AOC GSS). Each of these applications may contain information about individuals which will be described in each of their own PIA.

**a. Is this information identifiable to the individual<sup>1</sup>?**

(If there is **NO** information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed).

Not Applicable.

**b. Is the information about individual members of the public?**

(If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).

Not Applicable.

**c. Is the information about employees?**

(If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

Not Applicable.

---

<sup>1</sup> “Identifiable Form” - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

**C. DATA in the SYSTEM:**

**1) What categories of individuals are covered in the system?**

Not Applicable.

**2) What are the sources of the information in the system?**

**a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?**

Not Applicable.

**b. What Federal agencies are providing data for use in the system?**

Not Applicable.

**c. What Tribal, State and local agencies are providing data for use in the system?**

Not Applicable.

**d. From what other third party sources will data be collected?**

Not Applicable.

**e. What information will be collected from the employee and the public?**

Not Applicable.

**3) Accuracy, Timeliness, and Reliability**

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

Not Applicable.

- b. How will data be checked for completeness?**

Not Applicable.

- c. Is the data current?** What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Not Applicable.

- d. Are the data elements described in detail and documented?** If yes, what is the name of the document?

Not Applicable.

**D. ATTRIBUTES OF THE DATA:**

- 1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

Not Applicable.

- 2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

Not Applicable.

- 3) Will the new data be placed in the individual's record?**

Not Applicable.

- 4) Can the system make determinations about employees/public that would not be possible without the new data?**

Not Applicable.

- 5) How will the new data be verified for relevance and accuracy?**

Not Applicable.

- 6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

Not Applicable.

- 7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.**

Not Applicable.

**8) How will the data be retrieved?** Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Not Applicable.

**9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

Not Applicable.

**10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)**

Not Applicable.

**E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:**

**1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

Not Applicable.

**2) What are the retention periods of data in this system?**

Not Applicable.

- 3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

Not Applicable.

- 4) Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

Not Applicable.

- 5) How does the use of this technology affect public/employee privacy?**

Not Applicable.

- 6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

Not Applicable.

- 7) What kinds of information are collected as a function of the monitoring of individuals?**

Not Applicable.

- 8) What controls will be used to prevent unauthorized monitoring?**

Not Applicable.

**9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

Not Applicable.

**10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

Not Applicable.

**F. ACCESS TO DATA:**

**1) Who will have access to the data in the system?** (E.g., contractors, users, managers, system administrators, developers, tribes, other)

Not Applicable.

**2) How is access to the data by a user determined?** Are criteria, procedures, controls, and responsibilities regarding access documented?

Not Applicable.

**3) Will users have access to all data on the system or will the user's access be restricted? Explain.**

Not Applicable.

**4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** (Please list processes and training materials)

Not Applicable.

- 5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**

Not Applicable.

- 6) Do other systems share data or have access to the data in the system? If yes, explain.**

Not Applicable.

- 7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

Not Applicable.

- 8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**

Not Applicable.

- 9) How will the data be used by the other agency?**

Not Applicable.

- 10) Who is responsible for assuring proper use of the data?**

Not Applicable.