Privacy Impact Assessment (PIA) for the

Selective Service System

General Support Network (GSN)

April 22, 2024

Section 1: Introduction
The Selective Service System (SSS) 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.

Name of Project: General Support Network (GSN) System

Point of Contact Information:

1. **Who is the Authorizing Official?**
   Name: Scott Jones
   Title: Chief Information Officer
   Phone: (703) 605-4128
   Email: Scott.Jones@sss.gov

2. **Who is the system owner?**
   Name: Daniel Mira
   Title: Deputy Chief Information Officer
   Phone: (703) 605-4027
   Email: Daniel.Mira@sss.gov

3. **Who is the system manager**?
   Name: Perry Chaplin
   Title: Sr. System Administrator/IT Specialist
   Phone: (703) 605-4131
   Email: Perry.Chaplin@sss.gov

4. **Who is the Information Systems Security Officer who prepared this document?**
   Name: Charles Plummer
   Title: Information System Security Officer
   Phone: (703) 605-4082
   Email: CPlummer@sss.gov

5. **Who is the Information Systems Security Manager who reviewed this document?**
   Name: Jonathan Kimball
   Title: Information System Security Manager
   Phone: (703) 605-4123
   Email: Jonathan.Kimball@sss.gov

6. **Who is the Privacy Act Officer?**
   Name: Jonathan Kimball
   Title: Information System Security Manager
   Phone: (703) 605-4123
   Email: Daniel.Mira@sss.gov

Section 2: Information Collection, Sharing, and Protection

A. What is the purpose of the system?

The GSN is a General Support System (GSS) used to support the security of Selective Service System (SSS) information systems. The GSN primarily consists of SSS organization-wide "enterprise" security controls, external network communications infrastructure, workstations, servers, and printers. The GSN provides normal network functionality such as internet access, word processing, e-mail services, and wide area communications. The GSN includes the underlying infrastructure that supports major applications, as well as oversight and support of administrative and minor applications within SSS.

B. What is the legal authority?

Section 10(b)(3), Military Selective Service Act (50 U.S.C. App. 460(b)(3)) provides the authority for the GSN SSS to collect information on Individuals that are males over the age of 18 who have registered with the Selective Service System including SSS employees.

C. 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*

D. Is this information system registered in CSAM?

☒ Yes: System Name: General Support Network
☐ No

E. What information will be collected?

In the table below, indicate the types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3) using these designations:

A. SSS Employees, Contractors, and Detailees
B. Other Federal Government Personnel
C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs)
D. Members of the Public - Non-USPERs

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, or stored	(3) The information relates to	(4) Comments
Name	X	A	The data is used for identification and authentication of approved users, in telework agreements, and beneficiary forms.
Date of birth or age	X	A	The data is used for identification and authentication of approved users.
Place of birth	X	A	The data is used for identification and authentication of approved users.
Gender	X	A	The data is used for identification and authentication of approved users.
Race, ethnicity, or citizenship	X	A	The data is used for identification and authentication of approved users.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A	The data is used for identification and authentication of approved users.
Tax Identification Number (TIN)			
Driver's license	X	A	Only stored temporarily with I9 forms before upload to DOI IBC Electronic Official Personnel Folder (EOPF) system.
Alien registration number			
Passport number	X	A	Only stored temporarily with I9 forms before upload to DOI IBC EOPF system.
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	A	The data is captured in telework agreements and beneficiary forms.
Personal e-mail address	X	A	The data is captured in telework agreements and beneficiary forms.
Personal phone number	X	A	The data is captured in telework agreements and beneficiary forms.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Education records			
Military status or other information	X	A	Sometimes temporarily store SF-15 forms before upload to DOI IBC EOPF.
Employment status, history, or similar information			
Legal documents			
Device identifiers, e.g., mobile devices			
Foreign activities			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, or stored	(3) The information relates to	(4) Comments
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A	Stored on one HR user's laptop as temporary solution while researching options. Need to keep these for 5 years
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	A	The data is used for identification and authentication of approved users.
- **Video containing biometric data**			
- **Fingerprints**	X	A	The data is used for identification and authentication of approved users.
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	The data is used for identification and authentication of approved users.
- **User passwords/codes**	X	A	The data is used for identification and authentication of approved users.
- **IP address**	X	A	The data is used for identification and authentication of approved users.
- **Date/time of access**	X	A	The data is used for identification and authentication of approved users.
- **Queries run**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			

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

☒ Paper Format

☒ Email: Basic information required to establish a user account in the system is collected via PDF forms and submitted via email.

☐ Face-to-Face Contact

☐ Web site

☒ Fax

☒ Telephone Interview
☐ Information Shared Between Systems. *Describe*
☐ Other: *Describe*

G. What is the intended use of the PII collected?
GSN uses PII for appropriate identification of approved users who need to be able to access GSN as employees, contractors, or detailees.

H. With whom will the PII be shared, both within SSS and outside SSS? Indicate all that apply.
☒ Within the Bureau/Office:
☐ Other Bureaus/Offices:
☒ Other Federal Agencies: SSS uses DOI IBC as its HR Line of Business (LOB)
☐ Tribal, State or Local Agencies:
☐ Contractor:
☐ Other Third-Party Sources:

I. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?
☒ Yes: PII is used in/by the system for identification and authentication. Users can decline to provide PII and not work in support of SSS.
☐ No:

J. 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: Users are provided with account management forms containing privacy notices.
☐ Other: *Describe each applicable format.*
☐ None

K. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).
Data is not retrieved by individual identifiers as GSN is an IT system implemented to provide basic compute, network, and end-user services for the Agency, not for the express purpose of collecting, storing, transmitting, or processing information on individuals.

L. Will reports be produced on individuals?
☐ Yes: *What will be the use of these reports? Who will have access to them?*
☒ No

Section 2: Privacy Threshold Analysis

A. Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

☐ Yes, this IS a system of records as defined in the Privacy Act of 1974.

☒ No, this IS NOT a system of records as defined in the Privacy Act of 1974.

B. 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

NOTE: If the answer to 2.A and 2.B is No, then there is no SORN required for the system.

Section 3: Attributes of System Data

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

All of the data is sourced from SSS records.

B. How will data be checked for completeness?

All of the data is sourced from SSS records. Forms (I9, telework, etc) are required to be completed in their entirety for business purposes.

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

I9 forms are only kept temporarily and collected only at the time of hiring. Updates are not required. Telework agreements are updated when employees move or renewed when telework policies change.

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

This is not a system of records.

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

SSS adheres to the General Records Schedule (GRS) 5.6, which is available on Sharepoint.

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.

GSN is not a system of records and minimal PII is stored in the system. Most is in systems hosted externally such as the DOI IBC EOPF. The type of PII stored within telework agreements and other such files retained in GSN is typically non-sensitive.

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: *This is not a system of records. The incidental storage of PII is in alignment with the purpose for which it was designed.*

☐ 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: This is not a system of records. The question is N/A.

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

☐ Yes: *Explanation*

☒ No: This is not a system of records. The question is N/A.

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

☐ Yes: *Explanation*

☒ No: This is not a system of records. The question is N/A.

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

This is not a system of records.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated.

☐ Yes, processes are 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

☐ Contractors

☐ Developers

☐ System Administrator

☐ Other: *Describe*

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

Access to files and data is restricted based on role and responsibilities of users within SSS.

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. All users, including contractors, are subject to the same training, access agreements, and monitoring to protect SSS data.

☐ No

J. Is the system using technologies in ways that the SSS has not previously employed?

☐ 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?

None- N/A.

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

None- N/A.

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
☐ Cyber Awareness Challenge
☒ Identifying and Safeguarding PII
☒ Phishing Awareness
☐ Insider Threat Awareness
☐ Privacy Act - PII Rules of Behavior
☐ General Information Technology Security Program Rules of Behavior
☒ **GSN** System Rules of Behavior
☒ 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.

Daniel Mira, Senior Agency Official for Privacy (SAOP)
Jonathan Kimball, Privacy Act Officer

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?

Ruben Ramos, Chief Information Security Officer
Charles Plummer, Information System Security Officer
Jonathan Kimball, Information System Security Manager

Section 5. Review and Approval

PIAs for Bureau or Office level systems must be signed by the designated Information System Owner, Information System Security Officer, and Bureau Privacy Officer, and approved by the Bureau Assistant Director for Information Resources as the Reviewing Official. Department-wide PIAs must be signed by the designated Information System Owner, Information System Security Officer, and Departmental Privacy Officer, and approved by the SSS Chief Information Officer/Senior Agency Official for Privacy as the Reviewing Official.

DANIEL MIRA

Digitally signed by DANIEL MIRA
Date: 2024.09.25 16:32:21 -04'00'

Daniel Mira
System Owner

Date

Charles Plummer

Digitally signed by Charles Plummer
Date: 2024.09.23 12:32:11 -04'00'

Charles Plummer
Information System Security Officer (ISSO)

Date

JONATHAN KIMBALL

Digitally signed by JONATHAN KIMBALL
Date: 2024.09.23 12:27:10 -04'00'

Jonathan Kimball
Privacy Act Officer

Date