ADAMS ML091660040

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **Kathryn Greene, Director, Office of Administration**	
Name of System: **Integrated Personnel Security System (IPSS)**	
Date RFPSB received PIA for review: **June 12, 2009**	Date RFPSB completed PIA review: **June 15, 2009**
Noted Issues: The RFPSB received an e-mail request from ADM/DFS on 6/12/2009 to update the points of contact listed in the IPSS PIA (ML071690125): Business Project Manager - Andrew Pretzello changed to Darlene Fenton, telephone number 301-415-7050 Executive Sponsor - Timothy Hagan changed to Kathryn Greene, telephone number 301-492-3500 Last Page - First block - Timothy F. Hagan changed to Kathryn O. Greene, Director, Office of Administration	
Russell A. Nichols, Chief Records and FOIA/Privacy Services Branch Information and Records Services Division Office of Information Services	Signature/Date: ***/RA/ 06/15/2009***
Copies of this PIA will be provided to: *James Shields, Acting Director* *Business Process Improvement and Applications Division* *Office of Information Services* *Paul Ricketts* *Senior IT Security Officer (SITSO)* *FISMA Compliance and Oversight Team* *Computer Security Office*	

U.S. Nuclear Regulatory Commission

Revised
Privacy Impact Assessment

(*Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collections requirements, and record management requirements.)*

for the

Integrated Personnel Security System (IPSS)

Date: June 07, 2007

A. GENERAL SYSTEM INFORMATION

1. Provide brief description of the system:

   The IPSS tracks and manages the personnel security (security clearances, investigative and access authorizations data) and badging data associated with the issuance of permanent and temporary badges; drug program data associated with applicant drug testing and employee random drug testing; incoming and outgoing classified visit data; and facility clearance data associated with contractor companies that must have a facility clearance.

2. What agency function does it support?

   IPSS supports Personnel and Facilities Security functions for the Office of Administration, Division of Facilities and Security (ADM/DFS).

3. Describe any modules or subsystems, where relevant, and their functions.

   There are no separate modules in IPSS.

4. Points of Contact:

Project Manager	Office/Division/Branch	Telephone
Karen Cudd	**ADM/DFS/FSB**	**301-415-6554**
Business Project Manager	Office/Division/Branch	Telephone
Darlene Fenton	**ADM/DFS/FSB**	**301-415-7050**
Technical Project Manager	Office/Division/Branch	Telephone

Karen Cudd	**ADM/DFS/FSB**	**301-415-6554**
Executive Sponsor	Office/Division/Branch	Telephone
Kathryn Greene	**ADM/OD**	**301-492-3500**

5. Does this Privacy Impact Assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. ___ New System ___ Modify Existing System __X__ Other (Explain)

This PIA supports updating the older PIA from 2005 to allow for the Security Categorization of IPSS to be approved.

b. If modifying an existing system, has a PIA been prepared before?

Yes

(1) If yes, provide the date approved and ADAMS accession number.

October 27, 2005 ML052920257

B. INFORMATION COLLECTED AND MAINTAINED

(These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.)

1. **INFORMATION ABOUT INDIVIDUALS**

a. Does this system maintain information about individuals?

Yes.

(1) If yes, what group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public) is the information about?

Federal employees, Federal contractors, licensees, consultants, foreign nationals, and employment applicants.

b. What information is being maintained in the system about individuals (describe in detail)?

Demographic data, personal identification, and security clearance/access approval information, to include but not limited to: name, social security number, date and place of birth, identity verification information, credential (badging) information and drug testing information.

c. Is the information being collected from the subject individuals?

No, the information is collected from e-QIP and/or standard government forms used for personnel security.

(1) If yes, what information is being collected from the individuals?

d. Will the information be collected from 10 or more individuals who are **not** Federal employees?

No, the information is collected from e-QIP and/or standard government forms used for personnel security.

(1) If yes, does the information collection have OMB approval?

(a) If yes, indicate the OMB approval number:

e. Is the information being collected from internal files, databases, or systems?

Yes.

(1) If yes, identify the files/databases/systems and the information being collected.

The information is pulled from the official agency records on investigations, clearances, drug testing, and credentialing maintained in paper as part of the Personnel and Facility Security Program.

f. Is the information being collected from an external source(s)?

No.

(1) If yes, what is the source(s) and what type of information is being collected?

N/A

g. How will this information be verified as current, accurate, and complete?

Signature page acts as the certification from the individual that the information they submit as part of their investigation is current, accurate, and complete. OPM and/or NRC then conducts a thorough review to ensure completeness and accuracy.

h. How will the information be collected (e.g. form, data transfer)?

Information is manually entered into IPSS.

I. What legal authority authorizes the collection of this information?

Executive Order 10450 is the legal authority.

j. What is the purpose for collecting this information?

To track and manage the official agency records on investigations, clearances, drug testing, and credentialing that are maintained in paper in the TWFN 6th floor vault as part of its Personnel and Facility Security Program.

2. **INFORMATION NOT ABOUT INDIVIDUALS**

a. What type of information will be maintained in this system (describe in detail)?

N/A

b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

N/A

c. What is the purpose for collecting this information?

N/A

C. USES OF SYSTEM AND INFORMATION

(These questions will identify the use of the information and the accuracy of the data being used.)

1. Describe all uses made of the information.

The information is used for reporting, statistics, forecasting, history tracking, etc.

2. Is the use of the information both relevant and necessary for the purpose for which the system is designed?

Yes.

3. Who will ensure the proper use of the information?

The Office of Administration management staff ensures proper use of the information.

4. Are the data elements described in detail and documented?

   Yes.

   a. If yes, what is the name of the document that contains this information and where is it located?

      The IPSS Data Dictionary and User's Guide contains this information and is located in Rational and maintained by Lockheed Martin Information Technology (LMIT) as part of the operations and maintenance contract for the NRC.

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

   No.

   a. If yes, how will aggregated data be maintained, filed, and utilized?

      N/A

   b. How will aggregated data be validated for relevance and accuracy?

      N/A

   c. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

      N/A

6. How will the information be *retrieved* from the system (be specific)?

   Information about an individual is retrieved by name or social security number. Information is also retrieved via integrated Crystal Reports or adhoc reports.

7. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

   No.

   a. If yes, explain.

      (1) What controls will be used to prevent unauthorized monitoring?

8. Describe the report(s) that will be produced from this system.

There are over 75 specific reports and an adhoc capability available from the existing systems. Reports are run on an as needed basis.

a. What are the reports used for?

Reports will be used for security information, budgetary purposes, resource planning, and quality control purposes.

b. Who has access to these reports?

The Personnel and Facilities Security Branch staff, the System Administrator and ADM IT Coordinator.

D. RECORDS RETENTION AND DISPOSAL

*(These questions are intended to establish whether the information contained in this system has been scheduled, or if a determination has been made that a general record schedule can be applied to the information contained in this system. Reference NUREG-0910, "*NRC Comprehensive Records Disposition Schedule*.")*

1. Has a retention schedule for this system been approved by the National Archives and Records Administration (NARA)?

   Yes.
   a. If yes, list the disposition schedule.

2. Is there a General Records Schedule (GRS) that applies to information in this system?

   Yes.

   a. If yes, list the disposition schedule.

3. If you answered no to questions 1 and 2, complete NRC Form 637, NRC Electronic Information System Records Scheduling Survey, and submit it with this PIA.

E. ACCESS TO DATA

1. INTERNAL ACCESS

a. What organizations (offices) will have access to the information in the system?

ADM/DFS/PSB, ADM/DFS/FSB, and a few positions with a need-to-know basis (view-only in only a few screens) will have access to IPSS. The Office Director of ADM determines who is allowed read-only access.

(1) For what purpose?

For reporting, statistics, forecasting, history tracking, etc

(2) Will access be limited?

Yes, limited by roles and responsibilities.

b. Will other systems share or have access to information in the system?

No other systems directly interface with IPSS.

c. How will information be transmitted or disclosed?

N/A

d. What controls will prevent the misuse (e.g., unauthorized browsing) of information by those having access?

Users of IPSS have at least a 145b or an IT-II access authorization. IPSS has an audit trail to track modifications to the data. IPSS requires a user id and password to access the role-based system and the roles are set by least-privilege. Before an individual can gain access to the system, the ADM/DFS/FSB Branch Chief must approve the access and then an integrity statement is signed.

e. Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes.

(1) If yes, where?

IPSS User's Guide located in Rational and maintained by Lockheed Martin Information Technology (LMIT) as part of the operations and maintenance contract for the NRC.

2. **EXTERNAL ACCESS**

a. Will external agencies/organizations/public share or have access to the information in this system?

No external agencies have direct access to the information in IPSS. However, a flat file is produced monthly to verify security clearances with OPM's Clearance Verification System (CVS).

(1) If yes, who.

OPM.

b. What information will be shared/disclosed and for what purpose?

The information uploaded into the secure portal at OPM's CVS includes the social security number, last name, active clearance level, and date and city and state/country of birth.

c. How will this information be transmitted/disclosed?

This information is uploaded electronically to the secure portal within OPM. The transmission is secured with 128-bit encryption.

F. TECHNICAL ACCESS AND SECURITY

1. Describe security controls used to limit access to the system (e.g., passwords). Explain.

IPSS uses a user id and encrypted password to access the system. The password must be reset every 90 days. IPSS automatically locks a user's access after 3 unsuccessful tries and the user is also logged out of the system after 15 minutes of inactivity.

2. Will the system be accessed or operated at more than one location (site)?

No. IPSS is only used at Headquarters.

a. If yes, how will consistent use be maintained at all sites?

3. Which user group(s) (e.g., system administrators, project manager, etc.) have access to the system?

IPSS Administrator
Security Manager
Senior Adjudicator
Adjudicator
Processor
Badge Manager
Badge Guard
Station Guard

Drug Manager
Drug Tester
View Only

4. Will a record of their access to the system be captured?

   Yes.

   a. If yes, what will be collected?

      The date and time of the last login is captured. Certain fields are also captured in an audit log as the data is modified.

5. Will contractors have access to the system?

   Yes.

   a. If yes, for what purpose?

      The Processor role is handled by an ADM/DFS/PSB contract and has limited rights. The NRC guards have access with limited rights. These contractors are limited to specific roles in the system.

      The Processor role processes the Standard Forms as well as updating investigation and clearance information. The Station Guard role has viewing capability as well as the issuance of temporary badges. The Badge Guard has the rights to add and modify badging information as well as the inherited rights of the Station Guard.

      - Ensure that the following Federal Acquisition Regulation (FAR) clauses are referenced in all contracts/agreements/purchase order where a contractor has access to a Privacy Act system of records to ensure that the wording of the agency contracts/agreements/purchase order make the provisions of the Privacy Act binding on the contractor and his or her employees:

        - 52.224-1 Privacy Act Notification.

        - 52.224-2 Privacy Act.

6. What auditing measures and technical safeguards are in place to prevent misuse of data?

   An audit log tracks modifications to certain data fields within IPSS.

7. Are the data secured in accordance with FISMA requirements?

   The last full Certification and Accreditation was completed October 2003.

a. If yes, when was Certification and Accreditation last completed?

The last full Certification and Accreditation was completed and approved October 2003. This PIA is part of the IPSS security categorization that is currently in the approval process.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OIS/IRSD/RFPSB Staff)

System Name: Integrated Personnel Security System (IPSS)

Submitting Office: Office of Administration (ADM)

A. PRIVACY ACT APPLICABILITY REVIEW

___ Privacy Act is not applicable.

_X_ Privacy Act is applicable.

___ Privacy Act is applicable. Creates a new system of records. FOIA/PA Team will take the lead to prepare the system notice.

___ Privacy Act is applicable. Currently covered under System of Records, NRC- . Modification to the system notice is required. FOIA/PA Team will take the lead to prepare the following changes:

Comments:

The three categories of information maintained in the IPSS are covered under three separate systems of records, NRC-35, "Drug Testing Program Records," NRC-39, "Personnel Security Files and Associated Records," and NRC-40, "Facility Security Access Control Records," with each having separate access authorization levels based on information type, need-to-know, roles and responsibilities. For example, someone with access to an individual's security clearance/access approval information may not have access to an individual's drug testing information. No modification to the system notices are required. **IPSS contains personally identifiable information (PII)**.

Reviewer's Name	Title	Date
Sandra S. Northern	Privacy Program Officer	June 25, 2007

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

___ No OMB clearance is needed.

___ OMB clearance is needed.

_X_ Currently has OMB Clearance. Clearance No. 3206-0005

Comments:

The information collected for the Integrated Personnel Security System (IPSS) is collected on forms SF-85, SF-85P, and SF-86 and is covered by the Office of Personnel Management's OMB Clearance number 3206-0005.

Reviewer's Name	Title	Date
Christopher J. Colburn	Senior Analyst	June 28, 2007

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

_X_ Additional information is needed to complete assessment.

___ Needs to be scheduled.

___ Existing records retention and disposition schedule covers the system - no modifications needed.

___ Records retention and disposition schedule must be modified to reflect the following:

Comments:

RASS has reviewed the schedules that ADM provided for the IPSS, and they seem to be appropriate. However, RASS has questions regarding how these dispositions will be implemented by the IPSS system. The schedules identified have a variety of retention periods and different triggering events that drive the disposition (see examples below).

GRS 1-36 b Destroy when employee separates from a testing designated position
GRS 1-36 c Destroy when 3 years old
GRS 1-36 e Destroy when employee leaves agency or 3 years old whichever is later

GRS 18-22 a Destroy upon notification of death of employee or not later than 5 years after separation or transfer of employee or 5 years after contract relationship expires, whichever is applicable.
GRS 18-22 b Destroy in accordance with investigating agency instructions
GRS 18-22 c Destroy with related case file.

GRS 18-24 a Destroy 5 years after close of case
GRS 18-24 b Destroy 2 years after completion of final action

RASS requested that ADM provide information on how the IPSS system implements these differing schedules to the different collections of information that are captured in the system. RASS asked ADM the following questions. Does IPSS maintain information on the death of employees that triggers an action to implement a process to destroy the records? Does it maintain records of when an employee leaves the agency? Are date frames of material capture maintained for disposition purposes? Are there any processes included in the system that are

intended to manage the information from a recordkeeping perspective? RASS also requested that ADM provide any information on these processes so that RASS can determine that there are appropriate controls in place to apply the schedules that you have identified.

ADM responded that they would defer RASS' questions to Sandie Schoenmann as she is responsible for these files as DFS/PSB Branch Chief. IPSS requires the functionality to destroy records at certain times. ADM believes the IPSS database is fully normalized and is very complex for record deletion because of the table connections and the paper records stored in the vault are still the official agency records for personnel security.

Reviewer's Name	Title	Date
Jeffrey Bartlett	Records Management Analyst	June 27, 2007

D. BRANCH CHIEF REVIEW AND CONCURRENCE

___ This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.

_X_ This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

/RA/ Date **07/02/2007**

Margaret A. Janney, Chief
Records and FOIA/Privacy Services Branch
Information and Records Services Division
Office of Information Services

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **Timothy F. Hagan, Director, Office of Administration**	
Name of System: **Integrated Personnel Security System (IPSS)**	
Date RFPSB received PIA for review: **June 14, 2007**	Date RFPSB completed PIA review: **July 02, 2007**
Noted Issues: IPSS contains personally identifiable information (PII). Information in IPSS is covered by Privacy Act systems of records: - NRC-35, "Drug Testing Program Records" - NRC-39, "Personnel Security Files and Associated Records" - NRC-40, "Facility Security Access Control Records" IPSS contains information collections covered by OMB Clearance number 3206-0005. RASS has questions regarding how records dispositions will be implemented by the IPSS system. ADM deferred responses to Sandie Schoenmann as she is responsible for these files as DFS/PSB Branch Chief.	
Margaret A. Janney, Chief Records and FOIA/Privacy Services Branch Office of Information Services	Signature/Date: ***/RA/*** **07/02/2007**
Copies of this PIA will be provided to: *James C. Corbett, Director* *Business Process Improvement and Applications Division* *Office of Information Services* *Kathy L. Lyons-Burke, CISSP* *Senior IT Security Officer (SITSO)/Chief Information Security Officer (CISO)* *Office of Information Services*	