ADAMS ML080800457

U.S. Nuclear Regulatory Commission

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

Criminal History Check (CHC) System

Date prepared by sponsoring office: March 17, 2008

A. GENERAL SYSTEM INFORMATION

1. Provide brief description of the system:

   The Criminal History Check (CHC) system was put in place to serve as a third-party service for the licensee fingerprint checks of individuals granted unescorted access to a nuclear power facility or access to safeguards information by power reactor licensees. The system is funded by reimbursable funds paid for by the requesting licensee. Fingerprints are either paper-based or electronic and are sent to the Facilities Security Branch, Division of Facilities Security, Office of Administration (FSB/DFS/ADM) for processing between the U.S. Nuclear Regulatory Commission (NRC) and the Federal Bureau of Investigation (FBI). The results of the fingerprint checks are then sent back to the requesting licensee from the NRC.

2. What agency function does it support?

   This system supports the safety and security of NRC controlled facilities and information.

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

   Not applicable.

4. Points of Contact:

Project Manager	**Office/Division/Branch**	**Telephone**
Doreen Turner	ADM/DFS/FSB	301-415-6511
Business Project Manager	**Office/Division/Branch**	**Telephone**

Andrew Pretzello	ADM/DFS/FSB	301-415-7404
Technical Project Manager	**Office/Division/Branch**	**Telephone**
Doreen Turner	ADM/DFS/FSB	301-415-6511
Executive Sponsor	**Office/Division/Branch**	**Telephone**
Timothy Hagan	ADM/OD	301-415-6222

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)

      No changes are being made to the system at this time.

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

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

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?

      Licensees.

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

      The information being maintained includes demographic information such as name, social security number, date of birth, and address.

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

      Yes.

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

The information being collected includes demographic information, name, social security number, date of birth, and address.

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

Yes.

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

(a) If yes, indicate the OMB approval number: 3150-0002.

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

No.

f. Is the information being collected from external sources?

Yes.

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

The licensees collect the fingerprints and demographic information from the individuals and send it to the NRC. The NRC then acts as a pass-through and sends the information to the FBI.

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

The licensees verify the information before it is sent to the NRC and the Federal Bureau of Investigation (FBI) verifies the information before it is returned to the NRC.

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

The licensees either mail the paper fingerprint cards or send the fingerprint data via the NRC's Electronic Information Exchange (EIE) server. The electronic fingerprint submission is saved to an encrypted USB flash drive. The data from the USB flash drive is then loaded into the CHC system and the paper fingerprint cards are scanned into the CHC system. All data is then transmitted to the FBI.

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

Title 10 CFR Part 73.57

j. What is the purpose for collecting this information?

NRC collects this information because licensees are not able to have direct contact with the FBI system, and to ensure the trustworthiness of individuals with unescorted access at nuclear power plants, fuel cycle facilities, and others as required by NRC regulation.

2. **INFORMATION NOT ABOUT INDIVIDUALS**

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

The information being maintained includes licensee site information.

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

The source of the information is from licensees.

c. What is the purpose for collecting this information?

The licensee site information allows the CHC program personnel to contact the licensee sites, as necessary to resolve issues.

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 by the FBI to perform criminal history checks. The results are sent from the FBI back to the NRC and the NRC transmits the results to the licensee.

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 licensees in charge of this process for their location and the NRC CHC Project Manager will ensure the 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 data elements are described in two manuals, *"AltaScan Store and Forward Manager Report Application*" and "*CD-Import Application*," located in the secure CHC system room, T-6 G4.

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?

Not applicable.

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

Not applicable.

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

Not applicable.

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

The information is retrieved from the system by the AltaScan Store and Forward software by transaction control number, social security number, or name.

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?

Not applicable.

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

The reports that are produced from the CHC system include a submission search report to verify submissions to the FBI, a response search report to verify responses back from the FBI; a demographic search report to search on transaction control numbers, names, social security numbers, or a date range; a daily statistics report; a monthly statistics report; a resend status report to retry a

failed transmission; and a billing search report.

a. What are the reports used for?

The reports are used for tracking submissions and responses to and from the FBI.

b. Who has access to these reports?

The four Criminal History Check system operators have access to these reports.

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.

The paper fingerprint cards are destroyed within three months of the FBI results being sent back to the licensees. The electronic CHC system submissions to the FBI are deleted from the system as soon as NRC has confirmation that the FBI received the submission. The electronic CHC system responses received from the FBI are saved for 365 days and set to automatically delete at that time.

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

Yes.

a. If yes, list the disposition schedule.

GRS 18, Item 22a.

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. Who will have access to the information in the system?

Access to the information in the CHC system is strictly controlled, and is limited to the four operators of the Criminal History Program. The individuals undergo a rigorous background clearance process and have a minimum of a secret clearance.

(1) Will access be limited?

No. The four CHC system operators have access to all of the data in the system.

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

No, not directly.

c. How will information be transmitted or disclosed?

All data exchange will take place over encrypted data communication networks. The EIE system is used to collect the electronically sent data from each licensee using a PKI certificate assigned to each licensee EIE user as well as each CHC system operator. The USB flash drives used to physically transport the electronic data from the EIE system to the CHC system are assigned to each operator and are encrypted and password-protected. The CHC system transmits data via a direct connection to the FBI. Both the EIE system and the CHC system are physically accessed from within the cipher-locked Criminal History Program room, though they operate on different networks.

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

The CHC system is located within a cipher locked room, requires a login and password, and is limited to the four operators of the system.

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

Yes.

(1) If yes, where?

The CHC Project Manager created a user manual containing this information. This document resides in the Criminal History Program locked room.

2. **EXTERNAL ACCESS**

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

No.

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

Not applicable.

c. How will this information be transmitted/disclosed?

Not applicable.

F. TECHNICAL ACCESS AND SECURITY

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

The CHC system utilizes a user id and password and only the four CHC system operators are allowed access to the system. The system is on a closed network within a cipher locked room.

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

No.

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

Not applicable.

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

Access to the data is strictly controlled and is only accessed by the Project Manager and the other three operators of the CHC system. The FBI acts as the system administrator when there is a problem with the system.

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

No.

a. If yes, what will be collected?

Not applicable.

5. Will contractors have access to the system?

   No.

   a. If yes, for what purpose?

      Not applicable.

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

   All individuals with access privileges have undergone vetting and suitability screening. All data exchange will take place over encrypted data communication networks. The EIE system is used to collect the electronically sent data from each licensee using a PKI certificate assigned to each licensee EIE user as well as each CHC system operator. The USB flash drives used to physically transport the electronic data from the EIE system to the CHC system are assigned to each operator and are encrypted and password-protected. Both the EIE system and the CHC system are accessed from within the cipher-locked Criminal History Program room though they operate on different networks.

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

   The Privacy Impact Assessment (PIA) is the first step in the process for FISMA compliance. Once the PIA has been approved, ADM will begin work on the Security Categorization document.

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

      CHC has not been certified and accredited. The schedule for certification and accreditation has not been determined.

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

System Name: Criminal History Check (CHC) System

Submitting Office: Office of Administration (ADM)

A. PRIVACY ACT APPLICABILITY REVIEW

___ Privacy Act is not applicable.

_X_ Privacy Act is applicable. See comments.

COMMENTS:

The CHC system is maintained as part of NRC's Privacy Act system of records NRC-39, "Personnel Security Files and Associated Records."

Reviewer's Name	Title	Date
Sandra S. Northern	Privacy Program Officer	April 21, 2008

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

___ No OMB clearance is needed.

___ OMB clearance is needed.

_X_ Currently has OMB Clearance. Clearance No. 3150-0002

Comments:

The information collected has been approved by OMB and assigned control number 3150—0002**.**

Reviewer's Name	Title	Date
Gregory Trussell	Team Leader	April 21, 2008

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

___ Additional information is needed to complete assessment.

___ Needs to be scheduled.

_X_ 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:

These records are scheduled under General Records Schedule 18, item 22a.

Reviewer's Name	Title	Date
Tracy Clark	Records Management Analyst	4/21/08

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: ***04/22/2008***

Russell A. Nichols, Acting 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 Hagan, Director, Office of Administration**	
Name of System: **Criminal History Check (CHC) System**	
Date RFPSB received PIA for review: **April 4, 2008**	Date RFPSB completed PIA review: **April 22, 2008**
Noted Issues: Information in CHC is protected by Privacy Act and maintained as part of NRC's system of records NRC-39, "Personnel Security Files and Associated Records." The information collected has been approved by OMB and assigned control number 3150—0002**.** Records are scheduled under General Records Schedule 18, item 22a.	
Russell A. Nichols, Acting Chief Records and FOIA/Privacy Services Branch Information and Records Services Division Office of Information Services	Signature/Date: ***/RA/*** ***04/22/2008***
Copies of this PIA will be provided to: *James C. Corbett, 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*	