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 collection requirements,
and records management requirements.*

EAP Expert – Software
Used and housed by NRC's EAP Contractor – EAP Consultants, LLC

Date: July 17, 2019

A.   GENERAL SYSTEM INFORMATION

    1.   Provide a detailed description of the system:

EAP Expert is a case management system that has been designed with all major EAP roles in mind. Roles such as; Intake, Program Management, Clinical Management, Client-File Management, Accounting, Administration, Marketing, and Statistical Reporting. Additionally, the software will track and report presentations and critical incident responses. EAP Expert is a software in which each user must have a license to operate the system. Each user is given a username and password on a password protected desktop. The access to files on Expert is limited to the user's need. The user accesses the system to access files, based on their level of access, that are needed daily by that user.

    2.   What agency function does it support?

Allows the agency to provide nationwide EAP services to NRC HQ Employees and Regional employees and their dependent family members as required by Executive Order 12564, Public Law 99-570 (5 U.S.C. §§7361 and 7362), Public Laws 96-180 and 96-181 and Public Law 79-658.

By allowing the agency to establish a health service program to promote and maintain the physical and mental fitness of employees as outlined in Title 5 U.S.C. 7901, Public Law 79-658 and required per Executive Order 12564, Public Law 99-570 (5 U.S.C. §§7361 and 7362), Public Laws 96-180 and 96-181 and Public Law 79-658.

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

- *Built on MSDE/SQL server;*
- *HIPAA compliant;*
- *Module toolbar for quicker access to your information and multiple window functionality;*
- *Track leads and create new companies;*
- *Calculate ROI on utilization reports*
- *Client Files – manage cases from open to close;*
- *Organization module – manage contracts, track account management time;*
- *Clinical Resources – Provider relations management tool;*
- *Utilization report – executive summary, batch reporting and benchmark by industry;*
- *Info calls – get credit on the utilization report for calls that don't count as a case;*
- *Reports – ability to create and customize reports;*

4. **What legal authority authorizes the purchase or development of this system?**

   Title 5 U.S.C. 7901, Public Law 79-658 and Executive Order 12564, Public Law 99-570 (5 U.S.C. §§7361 and 7362), Public Laws 96-180 and 96-181 and Public Law 79-658.

5. **What is the purpose of the system and the data to be collected?**

   EAP Expert is a case management system that has been designed with all major EAP roles in mind. Roles such as; Intake, Program Management, Clinical Management, Client-File Management, Accounting, Administration, Marketing, and Statistical Reporting. Additionally, the software will track and report presentations and critical incident responses.

6. **Points of Contact:**

Project Manager	Office/Division/Branch	Telephone
Sarah Linnerooth Hoenig	OCHCO/HCAB	301-415-7113
Business Project Manager	**Office/Division/Branch**	**Telephone**
Rick Grancorvitz	OCHCO/HCAB	301-287-0805
Technical Project Manager	**Office/Division/Branch**	**Telephone**
Brendan Cain	OCHCO/HCAB	301-287-0552
Executive Sponsor	**Office/Division/Branch**	**Telephone**
Jason Shay	OCHCO/ADHROP	301-287-0590
ISSO	**Office/Division/Branch**	**Telephone**
Brendan Cain	OCHCO/HCAB	301-287-0552
System Owner/User	**Office/Division/Branch**	**Telephone**
Sarah Linnerooth Hoenig	OCHCO/HCAB	301-415-7113

7. **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

    b. **If modifying or making other updates to an existing system, has a PIA been prepared before?**

    Yes

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

    ML19198A292

    (2) **If yes, provide a summary of modifications or other changes to the existing system.**

    Annual review and updated to new PIA template.

8. **Do you have an NRC system Enterprise Architecture (EA)/Inventory number?**

    Yes

    a. **If yes, please provide Enterprise Architecture (EA)/Inventory number.**

    20190049

    b. **If, no, please contact EA Service Desk to get Enterprise Architecture (EA)/Inventory 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, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public (provide description for general public (non-licensee workers, applicants before they are licenses etc.)).

The information maintained on the system consists of Federal employees and dependents of the federal employees who call requesting EAP services

(2)   IF NO, SKIP TO QUESTION B.2.

b.   What information is being maintained in the system about an individual (<u>be specific</u> – e.g. SSN, Place of Birth, Name, Address)?

The information maintained about the employees and their dependent family members calling for EAP services includes the employee's date of birth, telephone number, address, employment status (full time, part time, supervisor), presenting issue/concern and services they requested (counseling, information about services or work/life services).

c.   Is information being collected from the subject individual?

EAP Consultants collects data directly from the individual. In some cases a supervisor or human resources specialist will provide information about individuals that may be requesting services.

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

The information collected by the employee is the same information as mentioned above: employee's date of birth, address, telephone number, employment status (full time, part time, supervisor), presenting issue/concern and services they requested (counseling, information about services or work/life services). If the information is collected by a supervisor, EAP Coordinator or human resources, the information includes employee name and presenting concerns. At times, the employee's address, employment status, date of birth and telephone number are also collected.

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

Yes

Information is collected from employees' dependent family members who contact EAP Consultants directly to receive services. The family members' date of birth, address, telephone number and presenting issue/concern and services they requested (counseling, information about services or work/life services). The name of the NRC employee who is related to the dependent family members who is requesting services is also collected as well.

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

    No

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

e. **Is the information being collected from existing NRC files, databases, or systems?**

No

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

f. **Is the information being collected from external sources (any source outside of the NRC)?**

Yes

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

    See answer to question 1d.

g. **How will information not collected directly from the subject individual be verified as current, accurate, and complete?**

N/A

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

Telephonically

2.   **INFORMATION NOT ABOUT INDIVIDUALS**

    a.   **Will information not about individuals be maintained in this system?**

       Yes

       (1)   If yes, identify the type of information (be specific).

          Information about NRC as an agency is collected, such as the contracted services, primary contacts within the agency, the on-site EAP Manager's contact information (phone, email and address), the locations of the agency, the contract number, the monthly fee the agency pays for the EAP services, the contract date, the utilization rate of EAP services used by the agency, the account manager, the population of employees at the agency, any notes regarding contacts with primary contacts within the agency, any presentations or critical responses that were requested, the requestor's name and contact information for the presentations and critical responses, the reason for these requests and the date, time and locations that the presentations and critical responses will occur.

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

       All information listed above comes from internal agency sources. This information is gathered from the internal agency contacts and logged as it is received. Much of the information is gathered from the original contract for services between NRC and EAP Consultants, LLC.

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 data in this system.**

       The data collected regarding individuals is used to connect the employees and the agency with the appropriate services that EAP offers. Aggregate data is also collected to report utilization, satisfaction and for billing of services as outlined in the contract between NRC and EAP Consultants

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

       Yes

3. Who will ensure the proper use of the data in this system?

EAP Consultants Account and Project Manager, Norman Winegar, LCSW, and the Relationship Manager, Heather Graham, LCSW oversee the use of the data regarding the agency's usage of the EAP program.

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?

All information and activities with the agency are documented and saved in the EAP Expert Software.

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

Yes

Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.

Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data (i.e. tables or data arrays).

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

The aggregate data is filed on the EAP Consultants, LLC secure server. It is maintained by the account manager, Norman Winegar, LCSW and the relationship manager, Heather Graham, LCSW. The aggregate data is utilized to evaluate services provided. This data provides an overview of the number of calls received by NRC employees and dependents, the number of presentations and critical responses performed as well as the number of participants, the broad reason for requesting services, the gender of callers, the number of cases that were completed within the EAP Sessions completed and the satisfaction rating of the services by the clients.

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

Not applicable. The data is pulled directly from data in EAP Expert.

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

The aggregate data is saved on the secure server in which a user must have a pre-authorized password to get into the system. The server is behind a locked door which is located in our locked facility in which only employees of EAP Consultants have access.

6.   **How will data be *retrieved* from the system? Will data be retrieved by an individual's name or personal identifier (name, unique number or symbol)? (Be specific.)**

Yes

    a.   **If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**

The individual data will be retrieved either by a file number or by the individual's name. The aggregate data is retrieved by the agency name.

7.   **Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register?**

Yes

    a.   **If "Yes," provide name of SORN and location in the Federal Register.**

Employee Assistance Program Records - 14

8.   **If the information system is being modified, will the SORN(s) require amendment or revision?**

No

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

No

    a.   **If yes, explain.** N/A

        (1)   **What controls will be used to prevent unauthorized monitoring?** N/A

10. **List the report(s) that will be produced from this system.**

   N/A

   a. **What are the reports used for?** N/A

   b. **Who has access to these reports?** N/A

D. **ACCESS TO DATA**

   1. **Which NRC office(s) will have access to the data in the system?**

      None

      (1) **For what purpose?** N/A

      (2) **Will access be limited?** N/A

   2. **Will other NRC systems share data with or have access to the data in the system?**

      No

      (1) **If yes, identify the system(s).** N/A

      (2) **How will the data be transmitted or disclosed?** N/A

   3. **Will external agencies/organizations/public have access to the data in the system?**

      No

      (1) **If yes, who?** N/A

      (2) **Will access be limited?** N/A

      (3) **What data will be accessible and for what purpose/use?** N/A

      (4) **How will the data be transmitted or disclosed?** N/A

E.   RECORDS AND INFORMATION MANAGEMENT (RIM) - RETENTION AND DISPOSAL

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are temporary (eligible at some point for destruction/deletion because they no longer have business value) or permanent (eligible at some point to be transferred to the National Archives because of historical or evidential significance). These determinations are made through records retention schedules and NARA statutes (44 U.S.C., 36 CFR). Under 36 CFR 1234.10, agencies are required to establish procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic information systems or enhancements to existing systems. The following question is intended to determine whether the records and data/information in the system have approved records retention schedule and disposition instructions, whether the system incorporates Records and Information Management (RIM) and NARA's Universal Electronic Records Management (ERM) requirements, and if a strategy is needed to ensure compliance.

1) **Can you map this system to an applicable retention schedule in NRC's Comprehensive Records Disposition Schedule(NUREG-0910), or NARA's General Records Schedules?**

   Yes.

   a.   **If yes, please cite the schedule number, approved disposition, and describe how this is accomplished (then move to F.1).**

   - **For example, will the records or a composite thereof be deleted once they reach their approved retention or exported to an approved file format for transfer to the National Archives based on their approved disposition?**

     This previous schedule (GRS 1 item 26.a.) is superseded by GRS 2.7 item 091 – EAP Records not related to performance or conduct.

     Temporary. Destroy 7 years after termination of counseling for adults or 3 years after a minor reaches the age of majority, or when the state-specific statute of limitations has expired for contract providers subject to state requirements, but longer retention is authorized if needed for business use.

   b.   **If no, please contact the Records and Information Management (RIM) staff at ITIMPolicy.Resource@nrc.gov.**

F.   TECHNICAL ACCESS AND SECURITY

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

Each user has a computer password to log into our internal network. EAP Expert then requires an additional password to log in. The location of the computers that access the EAP Expert Software are located in a locked facility in which only those with the appropriate FOBs have access. Data on the EAPC case management system is backed-up daily and stored on multiple servers with an additional backup securely stored off-site. Encryption, strong authentication procedures and other security controls make personally identifiable information unusable by unauthorized personnel.

Access to PHI is limited to those who have a need to know. Where possible, we use encryption, strong authentication procedures, and other security controls to make personally identifiable information unusable by unauthorized individuals.

2. **What controls will prevent the misuse (e.g., unauthorized browsing) of system data by those having access?**

EAP expert will log the user off after 30 minutes of inactivity. In addition, the location of the computers is in a locked area where only those with access to EAP expert are present and have access to that locked area.

3. **Are the criteria, procedures, controls, and responsibilities regarding access to the system documented?**

Yes

(1) If yes, where?

On the secure on-site server.

4. **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?

5. **Which user groups (e.g., system administrators, project managers, etc.) have access to the system?**

All approved EAP Consultant employees including system administrators, account managers, relationship manager, intake staff and support staff. All have signed documentation and are trained regarding client confidentiality.

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

Yes

a. If yes, what will be collected?

The time and date and person accessing the information.

7. **Will contractors be involved with the design, development, or maintenance of the system?**

No

If yes, and if this system will maintain information about individuals, ensure <u>Privacy Act</u> and/or PII contract clauses are inserted in their contracts.

FAR clause 52.224-1 and FAR clause 52.224-2 should be referenced in all contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function.
PII clause, "Contractor Responsibility for Protecting Personally Identifiable Information" (June 2009), in all contracts, purchase orders, and orders against other agency contracts and interagency agreements that involve contractor access to NRC owned or controlled PII.

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

Data on the EAP Consultants case management system is backed-up daily and stored on multiple servers with an additional backup securely stored off-site. In the event of failure or malfunction of equipment at our offices, data can be retrieved and recovered. Encryption, strong authentication procedures and other security controls make personally identifiable information unusable by unauthorized personnel.

- To maintain the security of electronic data, virus scan updates are downloaded daily, all computers are password protected, the server includes a sophisticated firewall and router, and all computer data is backed up daily and stored remotely. Access to PHI is limited to those who have a need to know. Where possible, we use encryption, strong authentication procedures, and other security controls to make personally identifiable information unusable by unauthorized individuals.

- EAPC currently use a Microsoft Windows 2011 Small Business Server configured with Active Directory which allows only users with the appropriate file and folder permission from being accessed on our server. No one without an EAP login with the appropriate rights will be able to access secure information.

- EAPC has the industry leading Cisco ASA Security Firewall that protects our organization from be accessed be external entities. Only traffic initiated from the inside is allowed to traverse the firewall to the Internet and all other traffic has to be implicitly allowed.

- EAPC performs maintenance in the server to make sure that the latest updates and patches are applied to thwart ongoing vulnerabilities.

SERVER INFRASTRUCTURE: EAPC hardware includes 4 servers currently:

- SERVER I: hardware RAID 10 with 2x 1000GB drives
- SERVER II: hardware RAID 10 with 2x 1000GB drives

The backup server runs a differential copy, comparing the last backup to the current file system on the server. It copies any changed files and keeps copies of any files that have been deleted. For SERVER I and SERVER II, backup server keeps snapshots of the backup for 14 days.

The failure of a single hard disk on SERVER I and SERVER II, would require replacing the failed drive and a RAID rebuild. This is generally a straightforward procedure and provides for quick recovery and return to redundancy.

9.   **Is the data secured in accordance with FISMA requirements?**

Yes

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

Not accredited.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OCIO/GEMS/ISB Staff)

System Name: EAP Expert - Software

Submitting Office: Office of the Chief Human Capital Officer

A.   PRIVACY ACT APPLICABILITY REVIEW

_____   Privacy Act is not applicable.

__X__   Privacy Act is applicable.

Comments:
EAP Expert is covered by NRC's Privacy Act System of Records NRC 14, Employee Assistance Program Records.

Reviewer's Name	Title	Date
Sally A. Hardy	Privacy Officer	11/01/2019

B.   INFORMATION COLLECTION APPLICABILITY DETERMINATION

__X__   No OMB clearance is needed.

_____   OMB clearance is needed.

_____   Currently has OMB Clearance. Clearance No._____

Comments:
The information collected from non-Federal employees is for the use by EAP Consultants only and is not being collected on the behalf of the government.

Reviewer's Name	Title	Date
David Cullison	Clearance Officer	8/30/19

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.

Comments:

Reviewer's Name	Title	Date
Marna B. Dove	Sr. Program Analyst, Electronic Records Manager	10/21/19

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 __November 29, 2019_____
Anna T. McGowan, Chief
Information Services Branch
Governance & Enterprise Management
    Services Division
Office of the Chief Information Officer

**TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS**

TO: **Jason Shay, Office of the Chief Human Capital Officer**	

Name of System: **EAP Expert - Software**	

Date ISB received PIA for review:
       July 17, 2019
	Date ISB completed PIA review:
	       November 1, 2019

Noted Issues: EAP Expert is covered by NRC's Privacy Act System of Records NRC 14, Employee Assistance Program Records.	

Anna T. McGowan, Chief
Information Services Branch
Governance & Enterprise Management
    Services Division
Office of the Chief Information Officer
	Signature/Date:
	
	   /RA/ November 29, 2019

Copies of this PIA will be provided to: *Thomas Ashley, Director* *IT Services Development & Operation Division* *Office of the Chief Information Officer* *Jonathan Feibus* *Chief Information Security Officer (CISO)* *Governance & Enterprise Management* *Office of the Chief Information Officer*