Privacy Impact Assessment
for the

DHS Employee Assistance Program

DHS/ALL/PIA-066

June 11, 2018

Contact Point
Angela Bailey
Chief Human Capital Officer
Office of the Chief Human Capital Officer (OCHCO)
(202) 282-8000

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

Each Federal Executive Branch agency is required to have an Employee Assistance Program (EAP), which is a voluntary, confidential program that helps employees and their family members work through various life challenges that may adversely affect job performance, health, and personal well-being. Department of Homeland Security (DHS) EAP services include assessment, counseling, and referrals for employees and family members with personal or work-related concerns such as job stress, financial issues, legal matters, family problems, office conflicts, and alcohol and substance abuse disorders. EAP assistance may be sought by the employee, by a family member, or at the recommendation of an employee's supervisor. This Privacy Impact Assessment (PIA) is being conducted because DHS EAP service providers collect personally identifiable information (PII) about individuals who receive assistance through the program.

Overview

The Comprehensive Drug Abuse Prevention and Control Act of 1970[1] mandates that each federal agency have an Employee Assistance Program (EAP). Since 1970, numerous laws, regulations, and initiatives have expanded EAPs in federal agencies.[2] The basic goal of agency EAPs is to assure employees of their right, without fear of reprisal, to seek confidential assistance from trained counselors and other service providers available to them through their agencies for issues related to mental health, financial management, legal matters, substance abuse, family problems, office conflicts, and other work-related or personal concerns. More generally, each EAP is intended to promote a climate of mutual trust and to ensure that employees and managers can receive preventive services to help them remain healthy and effective despite the stressful nature of their work.

The policies, procedures, and objectives of the EAP at DHS are governed by DHS Management Directive (MD) 254-02*, Employee Assistance Program.* MD 254-02 requires each DHS Component to provide EAP services and to develop written EAP policies and procedures that address all aspects of EAP operations and related business relationships. While the DHS Office of the Chief Human Capital Officer (OCHCO) is the policy lead for the overall EAP at DHS, each Component is responsible for providing EAP services to its personnel and their families.[3] To this end, Components may negotiate their own contracts, join existing EAP

[1] Pub. L. 91-513.
[2] *See, e.g.,* 5 U.S.C. 7904, Employee Assistance Programs Relating to Drug and Alcohol Abuse; 42 CFR Part 792, Federal Employees' Health, Counseling, and Work/Life Programs; or Executive Order 12564, Drug-Free Federal Workforce.
[3] More information about the overarching DHS EAP can be found at https://www.dhs.gov/employee-assistance-

agreements, or provide in-house counseling that meets the requirements of 5 CFR Part 792, *Federal Employees' Health and Counseling Programs*.[4]

An EAP Policy Manager at OCHCO works with EAP Program Managers at each of the Components to ensure that their Components' policies comply with Department-wide EAP policies. Services required of Component EAPs include: establishing a 24-hour telephone service; recruiting and supporting local counselors in performing their contractual obligations; maintaining an information and referral data bank of community resources; coordinating, planning, and providing employee and management EAP orientation training; providing prevention education and training; providing critical incident response to traumatic events; and providing employee counseling and other services as may be contractually defined. To provide these services, all DHS Components, except the U.S. Secret Service (USSS) which provides in-house services, currently contract with a third-party vendor. Whether in-house or via third-party vendors, all DHS Components must comply with MD 254-02 and with standards defined in OPM's *Federal Employee Assistance Programs: Guiding Principles, Framework, and Definitions*.[5]

Per MD 254-02, participation in an EAP is completely voluntary.[6] An employee or family member may receive assistance through self-referral or through a supervisory referral. Self-referral occurs when an employee or family member voluntarily seeks confidential counseling for himself or herself. Supervisory referral occurs when a supervisor suggests that an employee seek EAP services when the employee's performance, conduct, or attendance has begun to deteriorate, or when the supervisor learns other information that suggests EAP services might be of assistance to the employee.[7] No documentation or records are created or retained by the supervisor in the case of a supervisory referral,[8] and the only information collected by the EAP service provider from a supervisor during a supervisory referral is the employee's name and the presenting issues.[9] No

program-eap. DHS contractors are not afforded EAP services.

[4] *Available at* https://www.gpo.gov/fdsys/granule/CFR-2016-title5-vol2/CFR-2016-title5-vol2-part792/content-detail.html.

[5] General information about each Component's program, processes, and technologies can be found in Appendix A of this PIA. OPM's *Federal Employee Assistance Programs: Guiding Principles, Framework, and Definitions* (September 2008) is *available at* https://www.opm.gov/policy-data-oversight/worklife/reference-materials/eapguide.pdf.

[6] However, admission into an EAP requires an employee to accept a terms of service agreement that reflects the policies and procedures set forth in MD 254-02 regarding confidentiality and disclosure.

[7] EAP personnel counsel supervisors on the best way to refer an employee during the referral process.

[8] Supervisors are advised during mandatory DHS supervisory training that they are prohibited from maintaining personal records related to supervisory referrals. They are also advised of this prohibition by the EAP service provider when making a supervisory referral.

[9] MD 254-02 makes a distinction between formal supervisory referrals and informal supervisory referrals. Per the Management Directive, formal supervisory referrals must be in writing, must be signed by the employee, and may be stored in the EAP system of records but not in any other system of records. In actual practice, however, the EAP does not distinguish between or provide different services for formal and informal supervisory referrals. The only information collected or documented by an EAP service provider during a supervisory referral is the name and presenting issues of the employee being referred. This information is collected so that necessary resources are in

adverse action may be taken against the employee if he or she decides not to heed the supervisor's recommendation to seek EAP services.[10]

Per MD 254-02, it is mandatory for a supervisor to refer an employee to an EAP service provider when notified of a positive drug screening resulting from a DHS drug test. Under such a referral, the employee must sign a release allowing the EAP to notify the employee's supervisor that he or she is cooperating in order to receive EAP services.[11] As with any other supervisory referral, however, an employee who is referred as a result of a positive drug test may elect to accept or reject EAP services. In these cases, the supervisor may additionally elect to pursue administrative or disciplinary action as a remedy if the employee's performance or conduct fails to improve, but a decision to seek a disciplinary or other adverse action against the employee is not within the EAP domain and must be referred to the appropriate Labor and/or Employee Relations professional servicing the Component.

EAP services, including follow-up and monitoring services, are offered at no cost to DHS employees and family members during the assessment/referral framework, which usually lasts up to six sessions. If the EAP participant's issues remain unresolved at the completion of the assessment/referral framework, he or she is referred to a private service provider and becomes responsible for all future monetary costs.

The EAP service providers (vendors) DHS employs must comply with all federal and state laws, including Health Insurance Portability and Accountability Act (HIPAA) regulations regarding client confidentiality.[12] EAP service providers must also comply with all licensing and ethical standards related to their professions. All contracts with EAP vendors contain language that stipulates these laws and standards, including:

- The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Pub. L. 104-191);

---

place to provide quick and effective service should the employee choose to heed the supervisor's recommendation to seek EAP services.

[10] Other disciplinary action based on the same set of behaviors for which a supervisory referral is based may be included in the employee's Official Personnel Folder, but any reference to the EAP referral itself may not. This rule supports MD 254-02's mandate that the EAP remain a completely confidential program that cannot be associated with an adverse personnel action.

[11] The method of notification is up to the vendor so long as it adheres to Health Insurance Portability and Accountability Act (HIPAA) confidentiality provisions and privacy-related clauses in its respective contract.

[12] HIPAA is a federal law that restricts access to individuals' private medical information. HIPAA privacy rules require health care providers and organizations, as well as their business associates, to develop and follow procedures that ensure the confidentiality and security of protected health information (PHI) when it is transferred, received, handled, or shared. This applies to all forms of PHI, including paper, oral, and electronic. Additionally, only the minimum health information necessary to conduct business may be used or shared. For more information about health information privacy, *see* https://www.hhs.gov/hipaa/index.html/.

- Confidentiality regulations related to alcohol and substance abuse patient records (42 CFR Part 2);
- State laws governing the state in which the provider is located, especially those laws covering child and elderly abuse reporting; and
- Professional association standards and codes of ethics.

No DHS officials, including EAP Administrators, may compel an EAP service provider to disclose client information without the client's consent.[13] In order to release client information to any DHS employee or contractor, the client must first sign a release of information agreement with the EAP service provider.[14] This release must specifically state the type of information that will be released from the record and to whom.

There are some exceptional circumstances in which client information may be disclosed to non-DHS third parties without the client's consent. These include cases when there is a direct and imminent threat to the safety or health of the client or to another person.[15] Even in these cases, only the information required to protect the health and safety of the individual is released, and only to the entity that can prevent the harm.[16] The DHS Office of the Inspector General (OIG) may also audit client files on occasion to ensure that vendors are complying with all privacy and information security requirements. However, OIG auditors are bound by the same confidentiality requirements as EAP vendors and in-house service providers should an audit occur.

Although DHS never receives PII from its EAP vendors or its in-house service provider (*i.e.,* USSS), DHS does receive aggregate data from them on an ad hoc basis for management reporting purposes. This aggregate data[17] is shared by email or via online portals from the vendors to the Component EAP Program Managers. None of the aggregate data is linked or linkable to

[13] For the purposes of this PIA, USSS EAP services fall under the vendor designation even though they are provided directly by that Component. Although they are provided in-house, USSS service providers are required to follow the same laws, regulations, and policies as third-party vendors.
[14] As previously stated, an employee who is referred to the EAP by his or her supervisor as a result of a positive drug test must sign a release of information agreement as a condition to receiving EAP services. This release of information agreement specifically allows the provider to inform the supervisor whether the employee is cooperating with the program. Should the employee refuse to provide such a release, he or she may not receive EAP services, and thus he or she may be subject to termination.
[15] For example, a practitioner may be required to provide information to protect the client from suicide or self-harm, to assist in the care or services of the client when there is risk of serious bodily harm, to prevent harm to another person, or to protect the health and well-being of a child or elderly person when the client indicates that he or she is neglecting or abusing that individual. EAP service providers are bound by existing federal and state law to adhere to agency ethical standards and reporting requirements when these situations occur.
[16] This by definition excludes EAP Administrators as well as any other DHS employee or contractor. For USSS, even though it is providing in-house services, its EAP is bound by the same confidentiality and security requirements as a third-party vendor.
[17] Examples of aggregate data that DHS may request from EAP vendors could include overall number of employees using EAP services, number and type of presenting issues identified during intake, or overall number of cases that were not closed within an established timeframe.

individuals.

Component EAP programs also provide promotional materials about their services to DHS employees. These promotional materials typically cover program access information, confidentiality notices, descriptions of services available, and the number of service provider sessions DHS will cover free of charge. None of these promotional materials contain PII.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The Comprehensive Drug Abuse Prevention and Control Act of 1970 (Pub. L. 91-513), amended and expanded by the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act Amendments of 1979 (Pub. L. 96-180), mandated that each federal agency have an EAP. Numerous other legal authorities, regulations, and initiatives are also in place to allow for the collection of information required to provide EAP services. These include:

- 5 U.S.C. 7361, *Drug Abuse* – Establishes that OPM is responsible, in conjunction with other agencies, for developing appropriate prevention, treatment, and rehabilitation programs and services for drug abuse among employees;
- 5 U.S.C. 7362, *Alcohol Abuse and Alcoholism* – Establishes that OPM is responsible, in conjunction with other agencies, for developing appropriate prevention, treatment, and rehabilitation programs and services for alcohol abuse among employees;
- 5 U.S.C. 7901, *Health Service Programs* – Authorizes health programs for federal employees;
- 5 U.S.C. 7904, *Employee Assistance Programs Relating to Drug Abuse and Alcohol Abuse* – Mandates Employee Assistance Programs for employee alcohol and drug abuse;
- 42 U.S.C. 290dd-2, *Confidentiality of Records* – Establishes the confidentiality of federal agency records containing the identity, diagnosis, prognosis, or treatment of any patient for substance abuse;
- 44 U.S.C. 3101, *Records Management by Federal Agencies* – Places responsibility on the head of each federal agency to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency;
- 5 CFR Part 792, *Federal Employees' Health, Counseling, and Work/Life Programs* – Establishes that, to the extent feasible, agencies are encouraged to extend services to families of alcohol and/or drug abusing employees and to employees who have family members who have alcohol and/or drug problems;

- 42 CFR Part 2, *Confidentiality of Alcohol and Drug Abuse Patient Records* – Discusses the confidentiality and consent requirements of alcohol and drug abuse patient records;
- Executive Order 12564, *Drug-Free Federal Workplace* – Requires agencies to establish a drug-free federal workplace program that includes an EAP;
- Drug Abuse Office and Treatment Act of 1972 (Pub. L. 92-255) – Establishes a special action office for drug abuse prevention to concentrate the resources of the nation against the problem; and
- DHS Management Directive Number 254-02, *Employee Assistance Program*, May 31, 2007 – Establishes the policy, procedures, and objectives for the DHS EAP.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The collection of information required to effectively run and maintain an EAP is covered by *DHS/ALL-015 Department of Homeland Security Employee Assistance Program*.[18] This SORN, dedicated to EAP programs provided by DHS, describes categories of individuals, categories of records, and internal and external information sharing practices specific to the DHS EAP.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

A system security plan is not required for the DHS EAP because the program does not currently include technology at the Department level.[19] However, each system used for EAP services has a Security Plan and is required to undergo the DHS Security Authorization Process.[20]

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. Per National Archives and Records Administration (NARA) General Records Schedule (GRS) 2.7, Item 090, EAP Counseling Records that relate to an employee's workplace performance or conduct are destroyed once the employee has met conditions specified by agreement or when an adverse action or performance-based action has been initiated. Per GRS 2.7, Item 091, records that do not relate to an employee's workplace performance or conduct are destroyed seven (7) years after termination of counseling for adults or three (3) years after a minor reaches the age of majority, or when the state-specific statute of limitations expired for contract providers subject to state requirements, but longer retention is authorized if needed for business

[18] DHS/ALL-015 Department of Homeland Security Employee Assistance Program, 73 FR 64971 (October 31, 2008).
[19] Each Component, with the exception of USSS, contracts independently with third-party vendors for services.
[20] Please see Appendix A for additional information regarding EAP services at the DHS Component level.

use. EAP vendors are contractually required to comply with these provisions.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix?

DHS EAP will work with the Office of the Chief Information Officer (OCIO) Paperwork Reduction Act (PRA) Branch to identify any PRA requirements.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Although the exact data elements collected from individuals may differ among DHS Components based on the vendors and presenting issues, the general process is the same across the Department. There are two levels of information collection by EAP vendors. First, EAP vendors at the administrative level collect general intake information to make an effective referral and to track data. Subsequently, the EAP service provider to whom the client was referred during the intake process collects more in-depth clinical information related to the client's presenting issues. This usually occurs during scheduled in person appointments.[21]

Initial intake information may vary across Components, but generally includes:

- Name;
- Whether the individual is an employee or a family member of an employee;
- Gender;
- Phone number;
- Geographic Location (city, state, zip);
- Organization;
- Email address; and
- Presenting issues.

Clinical information collected by the actual service provider may also vary across Components, and usually includes:

- Privacy Act and written consent forms;

[21] For more information about the PII collected through each Component's process, please review Component-specific policy and procedure manuals.

- A psychosocial history and assessment;
- Correspondence with the client;
- Clinical and education interventions; and
- Information about sessions held.

Aggregate data is provided to DHS from vendors on an ad hoc basis for management and program evaluation and reporting purposes. Examples of aggregate data received from EAP vendors includes overall number of employees using EAP services, types of presenting and assessed issues, and overall employee or user satisfaction with services provided. No PII is included in aggregate data reported to DHS.

Some service providers may also have online services that require account creation. This process involves the user creating a username and password, and may also require additional data elements such as email address, age, security questions/answers, and a signature agreeing to terms of use.

2.2 What are the sources of the information and how is the information collected for the project?

Information collected through the EAP process is voluntarily provided by individuals seeking EAP services. Third-party vendors, or the in-house federal EAP counselor in the case of USSS, obtain information directly from the employee or family member seeking assistance. In the event of a supervisory referral, supervisors also provide the EAP with the name of the employee and the employee's presenting issues.

Intake information is collected by the EAP service provider directly from the client and typically via telephone. In some cases, limited intake information is collected online via a web portal hosted by the vendor.

Clinical information is collected during service appointments with the EAP service provider to whom the client was referred. These generally take place in person but may occur over the phone in rare circumstances.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. The DHS EAP does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

All intake information is provided directly by the individual, so accuracy is assumed.[22] EAP clients have the right to access their records at any time, and EAP service providers are required by HIPAA privacy rules to allow clients to amend their protected health information when that information is inaccurate or incomplete.

Management reports that DHS receives from EAP vendors typically aggregate demographic information collected during the intake process, or client satisfaction data collected after services are rendered. The aggregate reports are therefore assumed accurate as well. Clinical information is not used in the generation of aggregate reports beyond high-level descriptions of presenting issues.

DHS does not have access to any information disclosed by clients through EAP programs, nor does it have access to any clinical information or documentation created during or after service appointments. The only information DHS receives regarding EAP are contained in the aggregate data reports that are used to conduct high-level management and program analyses.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a specific over-collection risk related to information that supervisors may provide when reaching out to EAP service provides in order to properly refer an employee.

Mitigation: This risk is not mitigated. When a supervisor refers an employee to the EAP, the supervisor is asked for the name of the employee and his or her presenting issues.[23] However, if the employee chooses not to contact the EAP per the supervisor's recommendation, the EAP service provider may continue to maintain the employee's name and presenting issues.

Privacy Risk: There is a risk that more PII will be collected and retained by a third-party vendor or in-house provider than is needed to provide EAP services.

Mitigation: This risk is partially mitigated. All information collected during EAP services is deemed essential by service providers to provide effective counseling and referrals. Nonetheless, there is an inherent privacy risk of over-collection of clinical information because that information may or may not end up being ultimately relevant to effectively addressing a client's needs. Each case is different; client issues evolve and change; and service providers often collect a wide range

[22] Although a supervisor provides name and presenting issues during a supervisory referral, this information is not intake information since a case cannot be initiated until the employee voluntarily requests services.
[23] The EAP service provider requires this initial PII so that if the employee chooses to follow his or her supervisor's recommendation by calling the intake line, the resources to provide quick and personalized assistance are already organized to ensure faster and more effective service.

of information from clients for the purpose of understanding them holistically and identifying pertinent issues that may not be readily apparent. Consequently, different EAP service providers frequently require different information from their clients depending on the nature of the case. Notwithstanding, all of this information is still covered by HIPAA, MD 254-02, and confidentiality provisions placed in service provider contracts.

Privacy Risk: The data maintained by third-party vendor systems may be vulnerable to breach because security controls may not meet system security levels required by DHS.

Mitigation: This risk is partially mitigated. The Department is responsible for all PII associated with EAP, whether on a DHS system or on a third-party system. DHS, therefore, imposes strict requirements on vendors and clinicians for safeguarding employee records and data. This includes adherence to the DHS 4300A Sensitive Systems Handbook, which provides implementation criteria for the rigorous requirements mandated by DHS's Information Security Program.[24] The privacy of all EAP clients is further mandated by both state and federal laws, including HIPAA and numerous state clinical informed consent laws. Moreover, requirements are written into all EAP vendor contracts requiring the safeguarding of DHS employee and family member data. However, a risk remains that a particular EAP vendor may fail to meet the security requirements that DHS imposes on it.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

EAP service providers use the types of information covered in this PIA to provide thorough and effective services to employees and their family members and to address federal statistical reporting requirements associated with the use of EAP services. Senior leadership at DHS also use aggregate data from the EAP to identify ways to improve the program,[25] and to make decisions about additional training that could be offered if certain presenting issues appear to be significant in number or trending up. A Component may use aggregate EAP data as well for its own management and program analyses or to hold their vendors accountable for EAP services. No aggregate data generated from the DHS EAP is linked or linkable to individuals.

[24] *See* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.
[25] Examples include assessing how effectively the Component is conducting outreach or how satisfied customers have been with EAP services.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. Technology is not used to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly.

3.3 Are there other Components with assigned roles and responsibilities within the system?

Each Component works independently with its in-house EAP or third-party vendor to provide EAP services to its respective workforce and family members, following specific guidelines contained in DHS MD 254-02.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that employee or family member information may be used in a manner inconsistent with its original purpose for collection.

Mitigation: This risk is mitigated. Department personnel and contractors are required to complete annual records management and privacy training. Additionally, the vendor is required to comply with agency ethical standards and all applicable Codes of Professional Conduct and trainings for their respective disciplines. Furthermore, the DHS EAP is bound by federal statutes (*e.g.*, HIPAA) and professional ethics to prevent disclosure of information shared between service providers and program participants without prior written consent. Moreover, per DHS MD 254-02, disciplinary action is warranted for those who misuse EAP records.

Privacy Risk: There is a risk that adverse action may be taken against an employee if DHS management becomes aware he or she is voluntarily using EAP.

Mitigation: This risk is mitigated. Confidentiality is the foundation of the EAP. MD 254-02 dictates that neither job security nor promotion opportunities may be jeopardized by seeking EAP services. The Directive also states that participation in EAP may not be used in support of any disciplinary or adverse action. To this end, EAP records cannot be maintained in an employee's Official Personnel Folder, nor can any information be divulged to DHS personnel without the express written consent of the participant or as otherwise permitted by law. Supervisors who violate these terms are themselves subject to disciplinary action.

Although employees who test positive for drug use must be issued a supervisory EAP referral for counseling and will be asked to sign a signed consent agreement allowing the service provider to notify the agency whether the employee is complying with the service recommendation, any information released to DHS or a third-party must still be agreed to in

advance by the client via a signed consent agreement that specifies what information is to be released and to whom.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Vendor pamphlets and promotional materials are a source of general notice about EAP services that discuss information collected, service confidentiality, and individual privacy protections. This information can generally be found on Component websites and on the DHS EAP website.[26] These websites outline key aspects of EAP services, including that:

- The EAP is confidential;
- Seeking EAP services in and of itself will not affect an employee's security clearance;
- EAP services are free;
- Supervisors may grant a reasonable amount of time during normal working hours to an employee to attend EAP counseling sessions;
- Component EAPs serve family members; and
- EAP is always voluntary.

If EAP information is collected over the phone, the caller is informed that any specific information pertaining to the employee seeking EAP assistance, the reasons for seeking assistance, or any specifics that arise during conversations with EAP counselors, may not be divulged to any other party without the express written consent of the client, except in cases where the law stipulates that information should be shared to protect the safety of the employee or others. The EAP vendor or in-house provider also explains to the caller that the use of EAP services is voluntary and reads a Privacy Act Statement to the caller prior to the information collection.

Additionally, the employee or employee family member must sign an informed consent form prior to receiving service which states that he or she understands the services to be provided and the use parameters of the information that will be obtained. [27]

Notice is also provided to employees or employee family members through publication of this PIA and the EAP SORN.[28]

---

[26] *See* https://www.dhs.gov/employee-assistance-program-eap.
[27] Informed consent forms will vary based on the EAP service provider or vendor.
[28] DHS/ALL-015 Department of Homeland Security Employee Assistance Program, 73 FR 64971 (October 31, 2008).

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The use of EAP services is always voluntary and the employee or employee family member is always able to opt out. Even when supervisors refer employees to EAP or encourage the use of EAP services, participation is still completely voluntary.[29]

Additionally, information concerning an employee or employee family member's status with regard to the EAP may not be divulged without the express consent of the client or as otherwise permitted by law.[30] Informed consent forms also convey to clients that they are not required to provide any personal information and that they may opt out of the program at any time.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that employees who are referred to EAP by their supervisors may not know that their name and presenting issues have already been given by their supervisor to the EAP service provider.

Mitigation: This risk is not fully mitigated. The EAP service provider requires this initial PII so that when the employee calls the intake line, the resources to provide quick and personalized assistance for the presenting issues are already organized. Consequently, EAP service providers may obtain information about employees who never elect to use EAP services despite their supervisor's recommendation. Although this PIA acts as notice and supervisors are required to inform employees when referrals are made, this risk is not fully mitigated.

Section 5.0 Data Retention by the Project

5.1 Explain how long and for what reason the information is retained.

EAP counseling records that relate to an employee's workplace performance or conduct are destroyed in accordance with the client's wishes or as soon as any adverse action or performance-based action is filed against the employee. Records that do not relate to an employee's workplace performance or conduct are destroyed seven (7) years after termination of counseling for adults or three (3) years after a minor reaches the age of majority.

[29] However, if the individual does not provide certain personal information during the initial intake process, he or she cannot be referred to a provider, and thus EAP services cannot be rendered.
[30] *E.g.*, state laws concerning mental health professionals' duty to warn law enforcement of a client's potential to harm others, duty to report child abuse.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Due to the use of various third-party vendors, there could be a failure to adhere to Department retention guidelines and schedules.

Mitigation: This risk is mitigated. All contractors/third-party vendors are committed through the contracting process to abide by all DHS record retention and security requirements. These requirements are a mandatory part of all DHS Statements of Work. The vendor is also required to follow all applicable health care laws.

Because DHS does not have access to EAP vendor records, Component EAP Managers cannot audit the custody of records. However, vendors may be asked to self-audit and to provide a statement each year that retention schedules are being followed. Additionally, the vendor is contractually obligated to allow the DHS Office of Inspector General to conduct periodic reviews to ensure that security and privacy requirements are being implemented and enforced.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Information is not shared outside of DHS as part of normal operations.[31] EAP PII is only shared under exceptional circumstances[32] and as permitted by the Privacy Act, including routine uses listed in the EAP SORN and consistent with the notice provided to clients when they sign-up for services. HIPAA privacy rules also recognize circumstances where health information should be shared to ensure the client receives the best possible services or to protect the health and safety of the client or others. Additionally, a copy of a client's own EAP records may be released to the client or to a third-party pursuant to the client's written request under to the Privacy Act and in accordance with the procedures set forth in 6 CFR Part 5, *Disclosure of Records and Information*.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Information is not shared outside of DHS as part of normal operations. In the exceptional case that information is shared, it is done so pursuant to the EAP SORN, which permits the sharing of EAP information in accordance with the purpose for which the information is collected and the

[31] In this instance, vendors, contractors, and DHS personnel who provide EAP services are all considered employees of the Department.
[32] An example of this would be state laws concerning mental health professionals' duty to warn law enforcement of a client's potential to harm others or duty to report child abuse.

routine uses listed.[33] The purpose of the EAP system of records is to maintain information gathered by and in the possession of the DHS EAP to assist DHS employees and their families, with a variety of personal or work-related issues.

The SORN's routine uses define the circumstances under which EAP information can be shared. The following are brief examples of the information sharing permitted by these routine uses.

- Information is shared with contractors and their agents, grantees, experts, consultants, and others in order to provide EAP services to DHS employees as these services are typically outsourced from the Department (Routine Use C);
- Information can be shared with state and local authorities to report incidents of suspected child abuse (Routine Use D);
- Information can be shared when a client is at risk of harming him or herself or others (Routine Use F);
- Information can be shared to prevent an imminent crime which directly threatens loss of life or serious bodily injury (Routine Use E); or
- Information may be shared when there is a medical emergency (Routine Use G).

6.3 Does the project place limitations on re-dissemination?

Yes. All information collected, maintained, and used by EAP services is covered by the Privacy Act. As such, information may only be disseminated consistent with the Privacy Act or with the routine uses listed in the EAP SORN. Additionally, state and federal laws provide for the client/doctor privilege to restrict the re-disclosure of information by recipients.

State laws may require disclosure for other matters, including intent to harm oneself or others, as well as certain acts of child or elderly abuse. In these cases, only the information that is relevant to the suspected abuse is released, and only to the agency tasked with investigating or taking action to prevent the harm.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Information is not shared outside of DHS as part of normal operations. However, in the event that the sharing of information is required by law, that information would be shared by the EAP service provider to state and local law enforcement, not to DHS. The EAP service provider is required to keep a record of any such disclosures in the client record.

[33] DHS/ALL-015 Department of Homeland Security Employee Assistance Program, 73 FR 64971 (October 31, 2008).

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is the risk of unauthorized disclosure related to information sharing.

Mitigation: This risk is mitigated. EAP service providers are bound by law to adhere to agency ethical standards and all applicable codes of professional conduct related to their respective disciplines. EAP service providers are also bound by HIPAA and other statutes to prevent misuse or improper disclosure of information.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Clients seeking notification of and access to any EAP record about themselves may contact the EAP service provider in writing to request those records. This right is available to EAP clients at any time. When seeking EAP records about oneself, the client must verify his or her identity through procedures put in place by the EAP service provider that maintains the records. Service providers are also available to consult with the client regarding his or her records and to assist with interpreting those records.

Additionally, a client may request their own EAP records through a Privacy Act or Freedom of Information Act (FOIA) request.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals may contact their EAP service providers directly to correct their information.

7.3 How does the project notify individuals about the procedures for correcting their information?

The publication of this PIA and the EAP SORN notify individuals about the mechanisms for accessing and correcting their records via the Privacy Act. Additionally, redress information is provided to individuals by the EAP service provider during the intake process.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that clients may not know how to access, correct, or amend inaccurate EAP information about themselves.

Mitigation: This risk is mitigated. EAP service providers inform employees or employee family members during the intake process of their privacy rights and the vendor's responsibility

to protect information shared with them. Vendor pamphlets and promotional materials available to the public via Component and DHS websites provides further notice of EAP services and the protections clients maintain while using them. Additionally, Component EAP Program Managers can direct employees seeking information about their EAP records to the appropriate EAP service provider and instruct them on their rights regarding those records.

Furthermore, the publication of this PIA and the previously published EAP SORN provide notice of redress procedures.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Personal information collected by EAP service providers is only used to provide EAP services. All records and documentation, whether paper, telephonic, electronic, or computer-based, are managed, transmitted, retained, and maintained in compliance with HIPAA regulations and National Institute of Standards and Technology (NIST) Special Publication 800-53.[34] Each EAP service provider is contractually obligated and has various mechanisms in place to ensure that information is used in accordance with these guidelines.

EAP service providers are required to maintain an IT solution using compliant security controls that fully addresses DHS and Federal IT security and privacy requirements for systems that transmit and maintain PII.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All EAP service providers are required to take privacy and IT security training before accessing sensitive information. Privacy and IT security training is also an annual requirement for all DHS employees. Additionally, the DHS Rules of Behavior apply to all EAP service providers and are covered at orientation training sessions for DHS employees and contractors.

[34] NIST 800-53 outlines the steps in the Risk Management Framework that address security control selection for federal information systems in accordance with the security requirements in Federal Information Processing Standard (FIPS) 200. For more information, *see* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Only authorized EAP service providers are able to access EAP information. Moreover, EAP vendors are contractually required to have processes in place to control physical and logical access to client information. EAP service providers are also required to have an IT solution that is compliant with DHS and Federal IT security and privacy requirements to prevent those without a need to know from accessing client information.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

The DHS EAP does not currently require information sharing agreements or memoranda of understanding. However, in the event one of these documents might be needed, all information sharing and information sharing agreements would be reviewed and approved through an internal DHS process, which includes a review by DHS policy and privacy experts, as well as legal counsel.

Responsible Officials

Angela Bailey
Chief Human Capital Officer
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

APPENDIX A

(last updated April 22, 2021)

Each Component has its own written EAP policy and procedures plan. Below is an overview of information specific to each Component.

DHS Headquarters (DHS HQ)[35]

Third-Party Vendor: Federal Occupational Health Service (FOH)

Notice Provisions: All DHS HQ personnel are provided, during the new employee orientation, a briefing and promotional material establishing how to contact the vendor, the services provided, and privacy protections associated with the EAP, as well as agency/Component contact information should they require further guidance. This information is also provided to new supervisors during mandatory supervisory training. Additionally, clients are notified during the intake process that the program is voluntary and that any information they provide is confidential. They are also read a Privacy Act Statement prior to any information collection.

IT System Supporting Component EAP: Employee Assistance Services System

Reporting Period: Annually

Cybersecurity and Infrastructure Security Agency (CISA)

Third-Party Vendor: Federal Occupational Health Service (FOH)

Notice Provisions: All CISA personnel are provided, during the new employee orientation, a briefing and promotional material establishing how to contact the vendor, the services provided, and privacy protections associated with the EAP, as well as Component contact information should they require further guidance. This information is also provided to new supervisors during mandatory supervisory training. Additionally, clients are notified during the intake process that the program is voluntary and that any information they provide is confidential. They are also read a Privacy Act Statement prior to any information collection.

IT System Supporting Component EAP: WorkLife4You

Reporting Period: Annually

Federal Emergency Management Agency (FEMA)

Third-Party Vendor: Federal Occupational Health Service (FOH)

Notice Provisions: All FEMA personnel are provided, during new employee orientation, a briefing and promotional material establishing how to contact the vendor, the services provided,

[35] HQ Components such as the Science and Technology Directorate (S&T) are serviced by HQ for personal actions; thus, those HQ Components are included here under HQ.

and privacy protections associated with the EAP, as well as FEMA contact information should they require further guidance. Clients are notified during the intake process that the program is voluntary and that any information they provide is confidential. They are also read a Privacy Act Statement prior to any information collection

IT System Supporting Component EAP: WorkLife4You

Reporting Period: Annually

Transportation Security Administration (TSA)

Third-Party Vendor: Federal Occupational Health (FOH)

Notice Provisions: New TSA personnel are briefed on EAP during orientation, as well as supervisors during mandatory supervisory training. TSA provides further notice to employees on an EAP Intranet site; within the MyTSA mobile application (for employees); pamphlets, posters and other marketing materials; and EAP office outreach efforts at TSA Headquarters and through designated EAP/HR representatives at airports. During intake, the EAP vendor is required to explain to employees that services are voluntary and confidential. Prior to receiving service, employees must sign an informed consent form acknowledging they understand the services to be provided and the use parameters of the information submitted.

IT System Supporting Component EAP: WorkLife4You

Reporting Period: Monthly

United States Coast Guard (USCG)

Third-Party Vendor: ESPYR

Notice Provisions: All USCG personnel are provided, during new employee orientation for civilian personnel and onboarding for military personnel, a briefing and promotional material establishing how to contact the vendor, the services provided, and privacy protections associated with the EAP, as well as USCG contact information should they require further guidance. Clients are notified during the intake process that the program is voluntary and that any information they provide is confidential. They are also read a Privacy Act Statement prior to any information collection.

IT System Supporting Component EAP: EAP Expert

Reporting Period: Annually

U.S. Citizenship and Immigration Services (USCIS)

Third-Party Vendor: Federal Occupational Health Service (FOH)

Notice Provisions: All USCIS HQ personnel are given a briefing during New Employee Orientation Program on USCIS's EAP. Specifically, employees are given an overview of services

offered, the vendor's contact information, and the contact information for the agency EAP Program Manager if additional questions or guidance is needed. Information is also provided to new supervisors during mandatory supervisory training. Additionally, clients are notified during the intake process that the program is voluntary and that any information they provide is confidential. Clients must give written authorization before any information is provided to a third-party on their behalf. They also read and sign a Statement of Understanding, which provides an overview of the confidentiality parameters of the program as well as the authority to collect and maintain client information, purpose for collection, how the information may be disclosed in limited circumstances, and that the program participation is completely voluntary. Clients are given a copy of this Statement of Understanding for their records.

IT System Supporting Component EAP: WorkLife4You

Reporting Period: Annually

U.S. Customs and Border Protection (CBP)

Third-Party Vendor: ESPYR

Notice Provisions: All CBP employees are provided, during their onboarding process, a briefing establishing how to contact the vendor, the services provided, and privacy protections associated with the EAP, as well as the CBP point of contact information should they require further guidance. This information is also provided to new supervisors during mandatory supervisory training. Additionally, employees are notified during the EAP intake process that the program is voluntary and that any information they provide is confidential. They are also read a Privacy Act Statement prior to any information collection.

IT System Supporting Component EAP: EAP Expert

Reporting Period: Annually

U.S. Immigration and Customs Enforcement (ICE)

Third-Party Vendor: Federal Occupational Health Service (FOH)

Notice Provisions: All ICE personnel are provided, during new employee orientation, a briefing and promotional material establishing how to contact the vendor, the services provided, and privacy protections associated with the EAP, as well as ICE contact information should they require further guidance. Clients are notified during the intake process that the program is voluntary and that any information they provide is confidential. They are also read a Privacy Act Statement prior to any information collection.

IT System Supporting Component EAP: WorkLife4You

Reporting Period: Annually

United States Secret Service (USSS) – currently also provides in-house EAP services

Third-Party Vendor: Federal Occupational Health Service (FOH) and In-House

Notice Provisions: The EAP is embedded in 13 different training classes that include New Employee Orientation, First Line Supervisor's Seminar, Protective Detail Training, Uniformed Division Training, Special Agent Training, and Emergency Management Team Training. During these classes, personnel are provided a briefing outlining the program's services, as well as outlining how to contact the program specialists and the confidentiality and privacy protections associated with the EAP. Additionally, employees are notified during the intake process that the program is voluntary and that any information they provide is confidential. A Notice of Privacy Practices is also available in the EAP Office and on the Intranet.

IT System Supporting Component EAP: USSS EAP

Reporting Period: Annually

United States Secret Service (USSS) – SHIELD Mental Health Application

Third-Party Vendor: In-House

Notice Provisions: The Employee Assistance Program is implementing the SHIELD application to educate employees on mental health options, connect them with resources, provide a secure dashboard for clinicians to manage request, track data for reporting and storing EAP clinical notes. The SHIELD application will digitize the paper case records for efficient storage and reporting. Employees are notified through a Privacy Act Statement within the application that the information collected is shared voluntary.

IT System Supporting Component EAP: USSS EAP

Reporting Period: Not Applicable