Adapted Privacy Impact Assessment

Handshake

6/29/2023

Contact

Bureau of Land Management
Annette Cathcart
U.S. Department of the Interior
1849 C Street
Washington, DC NW 20240
830-225-3459
acathcar@blm.gov

One Privacy Impact Assessment (PIA) may be prepared to cover multiple websites or applications that are functionally comparable as long as agency or bureau practices are substantially similar across each website or application. However, any use of a third-party website or application that raises distinct privacy risks requires a complete PIA exclusive to the specific website or application. Department-wide PIAs must be elevated to the Office of the Chief Information Officer (OCIO) for review and approval.

SECTION 1: Specific Purpose of the Agency's Use of the Third-Party Website or Application

1.1 What is the specific purpose of the agency's use of the third-party website or application and how does that use fit with the agency's broader mission?

The mission of the Bureau of Land Management (BLM) is to sustain the health, diversity, and productivity of public lands for the use and enjoyment of present and future generations. BLM relies on successful recruitment and engagement outreach efforts to attract, hire, and retain a world-class government workforce, particularly for mission critical or hard-to-fill positions.

Handshake is a third-party career sourcing and recruitment services platform that connects essential partners such as college, universities, students, higher educational organizations, and employers to advance recruitment activities to acquire top talent into enterprises. Utilizing Handshake, participating BLM programs and offices can highlight the bureau's mission, strengthen the visibility of BLM employment opportunities, and facilitate recruiting efforts by engaging diverse groups of students qualified to apply for BLM positions.

Handshake is already being used by the federal agencies below. Notably, these agencies have the same privacy mandates as does the Bureau of Land Management. BLM is also striving to be an employer of choice in a very competitive labor market.

- U.S. Department of State
- Federal Bureau of Investigation (FBI)
- Central Intelligence Agency (CIA)
- National Aeronautics and Space Administration (NASA)
- U.S. Environmental Protection Agency (EPA)
- U.S. Department of Energy (DOE)
- U.S. Department of Defense (DOD)
- National Institutes of Health (NIH)
- U.S. Department of Justice (DOJ)
- U.S. Department of Homeland Security (DHS)
- Handshake allows federal agencies to access a vast talent pool of individuals who are actively seeking job opportunities. The platform enables recruiters to filter candidates based on specific criteria such as major, GPA, skills, and location, making it easier to identify and target qualified individuals for federal positions.

- Federal agencies can leverage the visibility offered by Handshake to promote their organizations and job openings. Handshake allows agencies to create branded profiles, share information about their mission, and highlight the unique benefits of working for the federal government. This increased visibility can help attract top talent who may not have considered federal positions otherwise.
- Handshake provides an efficient and user-friendly application process. Candidates can upload their resumes, transcripts, and other necessary documents directly to the platform, eliminating the need for manual paperwork. This streamlined process saves time for both candidates and federal recruiters, allowing for a smoother and more efficient recruitment process.
- Handshake offers features for targeted communication, allowing federal agencies to send personalized messages and notifications to specific groups of candidates. Recruiters can send updates about application deadlines, interview schedules, and other relevant information directly through the platform, ensuring timely and effective communication with potential candidates.

1.2 Is the agency's use of the third-party website or application consistent with all applicable laws, regulations, and policies? What are the legal authorities that authorize the use of the third-party website or application?

Participating BLM programs and offices are responsible for using Handshake in accordance with applicable laws, regulations, and policies and will identify specific legal authorities that cover their activities in BLM Privacy Notices, as appropriate.

Legal authorities that authorize typical BLM use of Handshake include the following: Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99); Paperwork Reduction Act (44 U.S.C. 3501); Presidential Memorandum, "Building a 21st Century Digital Government," May 23, 2012; OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010; OMB Memorandum M-17-06, Policies for Federal Agency Public Websites and Digital Services, November 8, 2016; OMB Circular A-130, Managing Information as a Strategic Resource, July 28, 2016; and 370 DM 312.2, Workforce and Succession Planning.

SECTION 2: Any PII that is Likely to Become Available to the Agency Through the Use of the Third-Party Website or Application

2.1 What PII will be made available to the agency?

The Employer Accounts of participating BLM programs and offices are administered by the Owner (a role limited to one individual per employer profile) or a designated Account Administrator (a role available to Premium partners only). If a BLM program or office chooses to allow additional individual employees to access the Handshake service

through its Employer Account, the granting Owner or Account Administrator is responsible for overseeing the use of Handshake by those individual employees. Depending on their role-based permissions and privileges, the level of Handshake they are using (i.e., Core or Premium), and the recruitment activities they are engaging in,

BLM Handshake users may have access to the limited, non-sensitive PII a) made available by students on their public profile and b) by Handshake users who engage in BLM recruitment activities.

Handshake receives personal data about students from Partner Universities, other third-party data sources, or when students create a Student or Alumni Account, update their profile, respond to questions or surveys on the Handshake website, or otherwise use the site.

University Partners share information about their students with Handshake so the service can provide them with capabilities that they use to manage their internal and external career center functions. Every student file that a University Partner uploads to Handshake must include information for the following student information fields:

- Email Address
- Student Username
- Student First Name
- Student School Year (i.e., Freshman, Sophomore, Junior, Senior, First Year Community/Technical College, Second Year Community/Technical College, Certificate Program, Masters, Masters of Business Administration, Accelerated Masters, Doctorate, Postdoctoral Studies, or Alumni)
- Cumulative Grade Point Average (GPA)
- Student Major
- Education Level (i.e., High School, Associates, Certificates, Advanced Certificates, Bachelors, Masters, Doctorates, Postdoctoral Studies, Non-Degree Seeking, Technical Diploma)
- Expected Graduation date (i.e., Month and Year)

Handshake recommends that University Partners pre-populate the following student information fields, but providing the information is not required:

- Student Last Name
- Student Middle Name
- Student's Preferred Name
- Additional Email Addresses (if applicable)
- Departmental GPA
- Minor Name
- College Name (e.g., the "Ross School of Business" at the University of Michigan)
- Education Start Date
- Education End Date (i.e., when a student is expected to graduate)
- Attendance Status (i.e., currently enrolled or has graduated)
- Student ID Number
- Campus Name (used for schools that have multiple campuses as part of their Handshake setup)

- Ethnicity
- Gender
- Work Study Eligibility
- Mobile Number
- Staff Email Address (i.e., email address of the staff member that the student is assigned to)
- Student Hometown
- Athletic Status
- First Generation College Student Status
- Veteran Status

Where FERPA applies to data shared by University Partners, Handshake stores, uses, and shares it in compliance with the statute. The ethnicity and gender fields are for internal reporting purposes only and are not available to employers or used by employers for outreach. (The ethnicity and gender information that is imported by a student's educational institution is different from the ethnicity and gender data that students can voluntarily share.)

University Partners are responsible for sending students an email that contains information about how to enable their Student Account. After students "claim their account" and Handshake confirms their association with the University Partner, Handshake will pre-populate the student profiles with the information provided by their university. Students may add information for any fields not pre-populated by their university or upload a profile picture and documents that contain personal information (e.g., a resume or transcript). Students may also create a Handshake account if their school is not a University Partner by using their .edu email address and updating their profile or uploading a profile picture and documents that contain personal information (e.g., a resume or transcript).

Upon agreeing to the Handshake Terms of Service and Privacy Policy, students are presented with several profile visibility options. No student data uploaded to Handshake by a University Partner or added by a student is ever viewable by BLM or any other employer until a student has chosen to make their profile public to users with an Employer Account. All Student Account users can apply for jobs, register for in-person events or fairs, and schedule appointments without making their profile visible to employers or other students. Student Account users must select either the Employers or Community profile privacy options to participate in a virtual fair 1:1 session, group session, virtual event, or connect with peers via Campus Profiles and messaging. Student data may become available to privileged BLM Handshake users when Student Account users at schools that have approved BLM access make their profile public to Employers and a) RSVP to attend a University-hosted career fair that a participating BLM program or office is attending or b) RSVP to attend a BLM-hosted virtual job event.

At a Handshake virtual career fair, each approved employer will be able to schedule either a) five 30-minute group meetings (for up to 50 students each) where multiple recruiters can attend, talk with students, and share their screen or b) 10-minute 1:1 meetings with students hosted by up to 15 recruiters where each recruiter can set their own schedule and choose qualifications students must meet to attend. BLM Handshake Core or Premium users scheduled to attend a virtual career fair will primarily conduct

group meetings and will be able to see the profiles and uploaded documents (if applicable) of registered students in accordance with their profile visibility settings. BLM and other employers will be able to view limited information of registered students who have restricted their profile visibility (i.e., their name, primary contact email, University, and educational college (engineering, liberal arts, etc.)). Any other personal information in their profile will be hidden or masked from an employer's view, including their profile photo, GPA, sponsorship status, professional skills, personal bio, and resume. During virtual career fairs, BLM and students will have access to video, audio, and text-based chat on the platform. BLM programs and offices may opt to use an approved external videoconferencing provider (e.g., Zoom for Government) to participate in a virtual career fair. The display name of students will be visible to privileged BLM users of the approved external videoconferencing provider.

At a BLM-hosted virtual event using Handshake Core or Premium, BLM users and students will have access to the video, audio, and text-based chat capabilities offered by an external videoconferencing provider (e.g., Zoom for Government) and will be able to see the profiles and uploaded documents of registered students who have set their profile to be visible. The display name of students will be visible to privileged BLM users of the approved external videoconferencing provider. BLM Handshake Premium users will have access to video, audio, and text-based chat on the platform. BLM will not be able to send virtual event invitations to students whose profiles are not visible to Employer Accounts.

Participating BLM programs and offices will direct individuals interested in applying for bureau employment opportunities to the USAJOBS.gov website (operated by the Office of Personnel Management (OPM)) to complete the application process. BLM Handshake users will not collect resumes or other application documents using Handshake.

BLM Handshake users may also correspond with University Partners on the platform to facilitate recruitment activities. Limited PII will become available to BLM Handshake users during these exchanges, such as a University Partner's name, job title, and their educational institution.

2.2 What are the sources of the PII?

Sources of PII are Handshake users that have made their PII available to other users using their profile privacy options. Handshake users may be:

- Students or alumni seeking a job or career advice;
- Employers planning to engage in recruitment activities;
- Career center or school employees; or
- Invited mentors.

2.3 Will the PII be collected and maintained by the agency?

BLM Handshake users will not designedly use the platform to collect and maintain PII. BLM Handshake users may interact with Education Partners users on the platform to facilitate recruitment activities, but they will not maintain this information within the

Department of the Interior (DOI) network. BLM programs and offices will send bulk event invitations to students who meet selected criteria for recruitment on the platform but will direct students to USAJOBS.gov to submit applications. There may be unusual circumstances where user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of DOI policy. BLM may maintain and use information provided by a user and/or the contents of posts, chats, or private messages to notify the appropriate agency officials or law enforcement organizations.

2.4 Do the agency's activities trigger the Paperwork Reduction Act (PRA) and, if so, how will the agency comply with the statute?

Typical BLM use of Handshake will not invoke the Paperwork Reduction Act (PRA). Any planned use of Handshake that will invoke the PRA will require a complete PIA exclusive to the use of Handshake, as well as coordination with the BLM Information Collection Clearance Officer.

SECTION 3: The Agency's Intended or Expected Use of the PII

3.1 Generally, how will the agency use the PII described in Section 2.0?

BLM Handshake users will not designedly use the service to collect, maintain, or disseminate PII.

BLM Handshake users do not access or collect any PII while using the service to post job announcements that direct students to USAJOBS.gov to learn about available employment opportunities and complete the application process. BLM will not retain any personal information about a candidate until an application is submitted through USAJOBS.gov. Once an application is submitted through USAJOBS.gov, BLM and its Human Resources services provider will use the PII provided in the normal course of Human Resources functions and procedures for job recruitment.

BLM programs and offices registered to participate in a University Partner-sponsored virtual career fair will do so without downloading and maintaining or any PII regarding registered students on the DOI network.

Neither BLM Handshake Core nor Premium users will target or contact individual students. BLM programs and offices that use Handshake to host virtual events will send bulk invitations to students at their approved schools who meet selected criteria based on their profile information. Through the Candidate Hub, BLM Handshake Premium users will have a greater number of search fields available to them than BLM Handshake Core users.

Any BLM programs or offices proposing to use Handshake in a way beyond those described in this Adapted PIA must coordinate with the BLM APO and security officials to conduct an assessment to determine privacy and security risks and requirements.

3.2 Provide specific examples of the types of uses to which PII may be subject.

The capabilities of participating BLM programs and offices using Handshake will depend on their level of service (i.e., Core or Premium) and the role-based permissions and privileges set by the Owner or their Account Administrator. All use must be in accordance with the Handshake Terms of Service and Privacy Policy and the uses described in this Adapted PIA.

With Handshake's Core level of service, participating BLM programs and offices will be able to:

- Post unlimited job postings to target schools;
- Send invitations to students for events in accordance with Handshake Core messaging limits; and
- Host virtual events for single schools and sign up for university-hosted career fairs.
- BLM Handshake Core users will not download or maintain any student PII that becomes available to them while hosting virtual events for single schools using an approved external videoconferencing provider or participating in any University-hosted career fairs on the platform.
- With Handshake's Premium level of service, participating BLM programs and offices will be able to:
- Post unlimited job postings to target schools;
- Send invitations to up to 5,000 students at once with no annual limits;
- Message in bulk with advance search capabilities;
- Wage unlimited smart campaigns; and
- Access in-application Talent Analytics to measure recruitment efficiency.

BLM Handshake Premium users will not download or maintain any student PII that becomes available to them while hosting virtual events (either on the platform or while using an approved external videoconferencing provider) or participating in any University-hosted career fairs on the platform.

Neither BLM Handshake Core nor Premium users will send direct messages to individual students on the Handshake platform or use Handshake to conduct interviews. All BLM Handshake users will direct students to USAJOBS.gov to complete the application process for opportunities presented during a virtual career fair, a virtual event, or through a shared job post.

There may be unusual circumstances where user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of DOI policy. BLM may maintain and use information provided by a user and/or the contents of posts, chats, or private messages to notify the appropriate agency officials or law enforcement organizations. BLM will secure such information in accordance with the applicable DOI privacy and security policies.

SECTION 4: Sharing or Disclosure of PII

4.1 With what entities or persons inside or outside the agency will the PII be shared, and for what purpose will the PII be disclosed?

All Handshake users have an opportunity to review the Handshake Privacy Policy and Terms of Service before they create a Handshake account. The Handshake Privacy Policy outlines what PII and non-personal data the service collects from users and how it uses the information. The Handshake Privacy Policy also details the limited circumstances in which the service will share information with third parties beyond the Handshake platform.

BLM programs and offices using Handshake will not designedly collect, track, download, or maintain the PII of student users. Student Handshake users must apply for advertised positions through USAJOBS.gov. BLM and its Human Resources services provider will use the PII provided in the normal course of Human Resources functions and procedures for recruitment.

Privileged Handshake users in participating BLM programs and offices will have access to analytics on the platform and will share only aggregated and anonymized recruitment data (e.g., event attendance numbers, numbers of schools reached, and gender/ethnicity/veteran status numbers for event attendees) with internal stakeholders to evaluate the effectiveness of recruiting activities.

There may be unusual circumstances where user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of DOI policy. BLM may maintain and use information provided by a user and/or the contents of posts or private messages to notify the appropriate agency officials or law enforcement organizations.

4.2 What safeguards will be in place to prevent uses beyond those authorized under law and described in this PIA?

To prevent uses beyond those authorized under law and described in this PIA, BLM Handshake users must be aware of and comply with DOI privacy and security requirements, Handshake's Privacy Policy and Terms of Service, and the parameters set by their assigned roles.

Handshake is responsible for protecting its users' privacy and the security of their data. Beyond its official uses of Handshake, BLM does not control the content or Privacy Policy on Handshake. Handshake users can set their own profile settings to help protect their information. Participating BLM programs and offices must review and approve content for public dissemination on the Handshake platform or through related recruitment activities prior to posting to assess and mitigate risks of the unauthorized disclosure of personal or agency information.

BLM Handshake users must use the service in accordance with the Handshake Privacy Policy and Terms of Service. Handshake may remove, edit, block, and/or monitor content or accounts containing content that it determines in its sole discretion violates the platform's Terms of Service. BLM Handshake users must request and receive approval from a school prior to posting jobs there. They must also acknowledge and agree that, to ensure their compliance with these Terms, Handshake may review the application flow

associated with any new post before it becomes available to students on the Handshake platform. Privileged BLM Handshake users, while able to search and filter student results based on a wide range of criteria, must agree to maintain a fair and equitable recruitment process, refrain from sending unsolicited marketing messages, and behave ethically. They also must agree not to discriminate based on ethnicity, national origin, religion, age, gender, sexual orientation, disability, or veteran status as prohibited by law. By using Handshake, BLM users agree not to stalk, defame, bully, harass, abuse, threaten, intimidate, or impersonate any people or entities.

To protect Handshake users and their data privacy, BLM programs and offices using Handshake may not use the data of students or other users for the purpose of marketing any employment opportunities other than the opportunities they have presented through the service. Handshake also prohibits the storage of any student's or other user's data for the purpose of (1) marketing employment opportunities to the applicant in the future or (2) allowing any third party to use the data for marketing or any other reason.

Any BLM programs or offices proposing to use Handshake in a way beyond the boundaries set forth in this Adapted PIA must coordinate with the BLM APO and security officials to conduct an assessment to determine privacy and security risks and requirements.

SECTION 5: Maintenance and Retention of PII

5.1 How will the agency maintain the PII, and for how long?

BLM programs and offices must retain the records they create while using Handshake and engaging in other recruitment-related activities in accordance with DOI policy and records retention schedules approved by the National Archives and Records Administration (NARA). BLM programs and offices using Handshake will not designedly collect, track, download, or maintain the PII of student users and must coordinate with the BLM Records Officer to ensure that appropriate records schedules are in place to cover the records they may create during their recruitment-related activities. BLM programs and offices must also be mindful of any active litigation holds.

Any Handshake user applying for a BLM position posted on Handshake will be directed to the appropriate job announcement on USAJOBS.gov to complete the application process. BLM and its Human Resources services provider must maintain application-related records in accordance with DRS-1.2A Short-Term Human Resources Records (DAA0048-2013-0001-0004). The records must be retained for 3 years after the decision is made on the position or it is cancelled, and then destroyed.

In accordance with NARA Guidelines and Departmental policy, approved disposition methods include shredding or pulping for paper records and degaussing or erasing for electronic records.

5.2 Was the retention period established to minimize privacy risk?

BLM programs and offices routinely minimize privacy risk by limiting their collection of PII

to what is necessary to facilitate and manage official bureau activities and refraining from collecting sensitive PII. Limited PII may become available to BLM Handshake users during recruitment-related activities. BLM Handshake users typically will not designedly collect PII from students.

In cases where PII is part of records that support bureau business, BLM will retain the records in accordance with the applicable NARA-approved schedule(s) following consultation with the BLM Records Officer. BLM programs and offices will retain PII that is not part of a Federal record subject to NARA retention requirements as needed, then promptly destroy it in accordance with approved destruction methods to minimize privacy risk.

SECTION 6: How the Agency will Secure PII

6.1 Will privacy and security officials coordinate to develop methods of securing PII?

Security officials and the BLM APO must coordinate to identify and resolve issues and analyze the risks posed by any third-party service that BLM has proposed for use. BLM programs and offices coordinated with the BLM APO and security officials to complete a Privacy Threshold Analysis (PTA) to analyze their proposed use of Handshake. Through the PTA, the BLM APO determined that an Adapted PIA would be required to assess and mitigate privacy risks.

There are also mandatory requirements for all BLM employees and contractors to complete security and privacy awareness training and sign the DOI Rules of Behavior form before acquiring access to the DOI network, systems, and information. BLM employees and contractors who have significant privacy responsibilities must also complete role-based security and privacy training, as applicable. Security officials and the BLM APO will coordinate with the BLM DOI Talent Data Steward to assign training and monitor completion.

6.2 How will the agency secure PII? Describe how the agency will limit access to PII, and what security controls are in place to protect the PII.

The DOI website Privacy Policy does not apply to Handshake. The Handshake Privacy Policy specifies what PII and non-personal data Handshake collects from users and how Handshake uses the information to manage its services and business. Both BLM and Handshake employ technical, physical, and administrative controls to secure PII.

All data stored and processed through the Handshake platform is encrypted in transmission using TLS 1.3, encrypted at rest using AES 256, and stored in the United States. Handshake tests every build of the service for security vulnerabilities such as SQL Injections, cross-site request forgery, session vulnerabilities, cross site scripting, file access, authentication, and many other potential security concerns. A qualified engineer peer reviews each change made to the Handshake codebase. Handshake continuously uses security assessments to examine the platform and tests for known Web application vulnerabilities. Handshake also partners with third-party agencies to verify the security of the Handshake platform through external scans. The Handshake security team

prioritizes the remediation of any discovered vulnerabilities and addresses them in accordance with their severity. Handshake annually contracts with a third-party security firm to conduct a full penetration test of the Handshake system.

Handshake uses Google Cloud to manage data storage, system back-ups, server management, and cloud management tools. The physical security in Google data centers is a layered security model. Physical security includes safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. In addition, Google uses security measures such as laser beam intrusion detection and 24/7 monitoring by high-resolution interior and exterior cameras to detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Experienced security guards, who have undergone rigorous background checks and training, routinely patrol the data centers. Access to the data center floor is only possible through a security corridor that implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter.

Handshake embeds security and privacy throughout its hiring and on-boarding processes. A team at Handshake vets all potential employees by performing internal and external reference checks. Where local labor law or statutory regulations permit, Handshake may also conduct criminal, credit, immigration, and security checks commensurate with the desired position. Handshake employs dedicated security and privacy teams comprised of senior engineering leaders, attorneys with a focus on user privacy best practices, and representatives from the Handshake executive leadership team. All new Handshake employees must go through security training as an early part of the on-boarding process. During on-boarding, employees set up key security safeguards such as two-factor authentication on all sensitive systems. As a part of on-boarding, all team members also go through detailed FERPA training. Handshake's Security and Privacy team also lead company-wide refresher training throughout the year to reinforce the importance of security and privacy. These training sessions are often combined with security tests.

BLM Employer Accounts are administered by the BLM Owner or a designated Account Administrator (a role available to Premium users only). If a BLM program or office chooses to allow additional individual employees to access the Handshake service through its Employer Account, the granting Owner or Account Administrator is responsible for overseeing the use of Handshake by those individual employees. Role-based permissions and privileges, which can be set by the Owner and Account Administrators, will restrict the activities a BLM Handshake user may engage in on the platform, as well as what information the user will be able to access. BLM Handshake users are required to use their official email address and will have access only to the account they use to conduct recruiting activities on the platform. BLM Handshake users also must access their account while using DOI-approved devices, not personal devices.

All BLM employees and contractors must coordinate with their supervisor and other appropriate officials to ensure that physical, technical, and administrative safeguards are in place protect the records in their custody. BLM Handshake users can help further safeguard PII that becomes available to BLM through Handshake or related recruitment activities by safeguarding their user credentials and avoiding the storage of records on

shared networks or folders accessible to individuals who do not have an official need-to-know. All BLM employees and contractors are responsible for safeguarding all information they remove from their official duty station and information they create at any alternative workplace in accordance with the Federal Records Act, Privacy Act, Freedom of Information Act, and other Federal laws, regulations, and DOI policies.

BLM Handshake users will direct students interested in applying for a position to USAJOBS.gov to complete the application process. PII received through the application process on USAJOBS.gov is secured in accordance with DOI Privacy Act regulations and applicable DOI privacy and security policies. Access to the DOI network is restricted to authorized users with multi-factor authentication controls, servers are located in secured facilities behind restrictive firewalls, and access to databases and files is controlled by the system administrator and restricted to authorized personnel based on the need-to-know principle. Other security controls include continuously monitoring threats, rapid response to incidents, mandatory security and privacy awareness training, mandatory role-based security and privacy training (as applicable), and the DOI Rules of Behavior. All BLM Handshake users must report any suspected or confirmed compromise of their Handshake accounts or recruitment-related information to the appropriate DOI officials in accordance with established procedures.

There may be unusual circumstances where user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of DOI/BLM policy. In these cases, BLM may maintain and use information provided by a user and/or the contents of posts or private messages to notify the appropriate agency officials or law enforcement organizations as required by law. BLM will secure such information in accordance with the applicable DOI privacy and security policies.

SECTION 7: Identification and Mitigation of Other Privacy Risks

7.1 What other privacy risks exist, and how will the agency mitigate those risks?

BLM systems do not share data with Handshake. Handshake receives personal data about students from Partner Universities, other third-party data sources, or when students create a Student or Alumni Account, update their profile, respond to questions or surveys on the Handshake website, or otherwise use the site. The Handshake Privacy Policy that all users must review explains what data the service collects, how it uses the data, and the limited circumstances where it may share the data. BLM does not have any control over the personal information posted or shared by other Handshake users. All users can mitigate privacy risk by controlling the viewability of their PII via their profile settings and through discretion with respect to the personal information they provide in uploaded documents, posts, comments, or direct communications with other Handshake users.

Handshake places a small piece of software referred to as a “session cookie” on the computer of site visitors. Handshake also uses this cookie to recognize account holders on return visits and expedite the login process. Handshake users can remove this and other cookies through their browser preferences menu, but they will not be able to log

into the service if their cookies are disabled. Handshake's email communications contain Web beacons or similar technology which track when the email has been opened or read. This functionality sends the resulting records back to Handshake, which may be associated with other information a user has provided the service. As of the date of this Adapted PIA's publication, Handshake is unable to respond to Do Not Track signals that may be sent by some browsers.

Handshake may also reference a site visitor's device identifier or other information about where their visit originated if they visit from a mobile device. When an individual uses the Handshake mobile app, the service collects analytic information about the user's device, such as the Internet Protocol address, Operating System version, and the clickstream. For a limited set of features (e.g., displaying a user's precise location on a map at a career fair), Handshake allows users to opt-in to its collection of precise location data (GPS data). Handshake does not share precise location data with third parties and does not combine precise location data with personal information for advertising purposes. The Handshake Privacy Policy is accessible for review in the app stores.

FERPA is focused on protecting student data. The consequences for violating FERPA are serious. Handshake retains FERPA experts and incorporates FERPA training into the employee on-boarding process to maintain FERPA compliance. The FERPA-protected data that Universities upload to Handshake is used by the career center for purposes of tracking engagement, maintaining counseling notes, and other key functions allowed by Handshake. This data transfer is permitted by FERPA under the service provider exception. When a student logs in to Handshake, they "claim their account" and are in full control over how their information is shared with third parties on the platform. When students opt into sharing and making their profiles searchable, they are taking ownership of the FERPA data and that information is no longer protected by their school's FERPA responsibility.

The Handshake Privacy Policy also reminds users that the service does not accept any responsibility or liability for the privacy and security policies of sites operated by Employers and University Partners. Users must exercise caution before proceeding to any third-party service or entering into any transaction with third parties linked to from the services. Users must also be cautiously aware of the information they share with integrated applications and should take care to avoid disclosing sensitive PII, which could be used by unintended persons to commit fraud or identity theft, or for other harmful or unlawful purposes. Neither BLM nor Handshake are responsible for the contents of any linked site that they do not manage.

Handshake is not responsible for any personal data that users submit to Employers using the service. BLM Handshake users typically will not designedly collect PII from students. BLM programs and offices will direct students interested in applying for bureau job opportunities to USAJOBS.gov, which uses login.gov (a General Services Administration (GSA) service) to authenticate individual access. The login.gov Security Statement, Privacy Policy, and a Privacy Act Statement are available for review on the sign-in page. The login.gov PIA is available for review on the GSA PIA Web page. The USAJOBS.gov Privacy Policy is accessible for review via a link in the footer of the site's Web pages. The USAJOBS.gov PIA is available for review on the OPM PIA Web page.

If Handshake makes minor changes to its Terms of Service without materially changing user rights, the service will post the modified Terms on its website. Handshake will notify users by email, through the Handshake service, or by presenting users with a new Terms of Service to accept if the service makes a modification that materially changes user rights. When users continue to use the Handshake service after a modification is posted, users are accepting the modified terms. The BLM APO will reassess the Handshake Privacy Policy annually (at a minimum) and in response to changes and will update this Adapted PIA if necessary.

There is a risk that Handshake users attending a BLM-hosted virtual event on the platform or through an external videoconferencing provider will not receive a notice regarding the bureau's privacy practices. In accordance with DOI policy, BLM Handshake users are responsible for providing a Privacy Notice at appropriate points during recruitment-related activities to inform individuals about how BLM will handle any PII that becomes available to the bureau through those activities. These Privacy Notices and the DOI website Privacy Policy serve to remind users that BLM has no control over access restrictions or privacy procedures on third-party websites and users are subject to third-party website privacy and security policies. Users who have any questions about BLM's privacy practices may contact the BLM Privacy Program at blm_wo_privacy@blm.gov

Handshake cautions its users not to initiate an audio or video recording of any third party in violation of wiretapping laws. By initiating any audio or video recording through Handshake, users must have express permission from all persons appearing in the audio or video recording where required by law. Handshake will not be liable for any users' failure to comply with applicable laws. BLM Handshake users typically will not record while using Handshake or engaging in related recruitment activities. BLM programs and offices will consult with the BLM APO to provide an appropriate Privacy Notice to obtain consent from individuals prior to initiating any audio or video recordings, as applicable.

All Handshake users must guard their account against compromise by protecting their account information, regularly updating their password, and taking appropriate action if their account is compromised. Although both BLM and Handshake employ technical, administrative, and physical controls to help prevent security breaches, neither can guarantee that a privacy breach will never occur. In the event of a breach on the platform, Handshake will take reasonable steps to investigate the situation and, where appropriate, notify affected individuals in accordance with any applicable laws and regulations. BLM Handshake users must report any suspected or confirmed privacy breach immediately to their supervisor and local IT help desk, the BLM APO, or the DOI Computer Incident Response Center (CIRC).

Minimizing the retention of PII is a basic privacy principle. BLM programs and offices using Handshake will not designedly collect, track, download, or maintain the PII of student users and must coordinate with the BLM Records Officer to ensure that appropriate records schedules are in place to cover the records they may create during their recruitment-related activities. BLM does not control Handshake's maintenance of user data. Handshake account holders can access their personal data through their account settings in the Handshake platform or by contacting the service to request a personal data report. Handshake users can choose to deactivate their account so that

they are no longer viewable on the platform or they can make their account private. They may also request that Handshake delete information about them. However, Handshake may be obligated as a service provider to a Student Account user's college or university to retain certain data. Student users can request deactivation or deletion by sending a message to Handshake or by contacting their university to request deletion of their information. Users who have any questions about Handshake's privacy practices may contact the service directly either by mail or by email at privacy@joinhandshake.com.

7.2 Does the agency provide appropriate notice to individuals informing them of privacy risks associated with the use of the third-party website or application?

All Handshake users have an opportunity to review the Handshake Privacy Policy and Terms of Service prior to creating an account on the platform. By creating a Handshake account, a user agrees to both the Handshake Terms of Service and the Privacy Policy. The Handshake Privacy Policy specifies what PII and non-personal data the service collects from its users and how it uses, processes, and stores the information. If Handshake makes minor changes to its Privacy Policy, the service will post the modified Privacy Policy on its website. Handshake will notify users of any modifications that will materially change their rights.

Participating BLM programs and offices will ensure, to the extent feasible, that they display appropriate branding and provide notice to individuals on the privacy implications of their use of Handshake through this Adapted PIA, a link to the Handshake Privacy Policy, links to BLM's official website and the DOI website Privacy Policy, and an activity-specific Privacy Notice (where applicable) to explain:

- That Handshake and any external videoconferencing provider used by BLM (if applicable) is controlled and operated by a third-party and is not a U.S. Government website;
- That the Department of the Interior's website Privacy Policy does not apply to Handshake or any external videoconferencing provider used by BLM (if applicable) and BLM has no control over any external service's access restrictions or privacy procedures; and
- How BLM will use PII that becomes available to the bureau through its use of the service and related recruitment activities.

SECTION 8: Creation or Modification of a System of Records

8.1 Will the agency's activities create or modify a "system of records" under the Privacy Act of 1974?

Typical BLM use of Handshake will not create or modify a Privacy Act system of records. Related recruitment activities conducted through USAJOBS.gov, addressed in 8.2. below, will create a system of records. BLM programs and offices that will create a system of records through their use of Handshake or other recruitment-related activities facilitated through use of the platform must a) coordinate with the BLM APO to identify the applicable SORN or the need to publish a new one and b) provide an appropriate

notice to individuals and maintain the records in accordance with the applicable SORN. The BLM APO will also update this Adapted PIA as required to provide notice.

There may be unusual circumstances where interactions between Handshake users indicate evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of DOI policy. BLM may use information provided by a user and/or the contents of posts or private messages to notify the appropriate agency officials or law enforcement organizations. The bureau's maintenance of this information may create a system of records.

8.2 Provide the name and identifier for the Privacy Act system of records.

The DOI-08, DOI Social Networks SORN, 76 FR 44033 (July 22, 201 1); modification published 86 FR 50156 (September 7, 2021), c overs the cases in which BLM's maintenance of information of user interactions on a third-party platform to notify agency officials and/or law enforcement organizations may create a system of records. Participating BLM programs and offices will direct all student Handshake users to USAJOBS.gov to submit applications for job announcements. BLM and its Human Resources services provider will maintain any PII collected through USAJOBS in accordance with the applicable personnel system of records notices, which may include OPM/GOVT-1, General Personal Records (77 FR 79694, Dec ember 11, 2012; modification published 80 FR 74815, November 30, 2015), OPM/GOVT-5, Recruiting, Examining, and Placement Records (79 FR 16834, March 26, 2014; modification published 80 FR 74815, November 30, 2015; modification published 86 FR 68291, December 1, 2021), and DOI-85, Payroll, Attendance, Retirement, and Leave Records (83 FR 34156, July 19, 2018).

DOI Privacy Act SORNs are available for review on the DOI SORNs Web page. Government-wide SORNs maintained by other agencies are available for review on the DOI SORNs Web page. Government-wide SORNs maintained by other agencies are available for review through the Federal Privacy Council's SORN Dashboard tool.