Yello Enterprise PIA

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Name of system: Yello Enterprise

(b) Bureau: Global Talent Management (GTM/REE)

(c) System acronym: YE

(d) iMatrix Asset ID Number: 293090

(e) Reason for performing PIA: Click here to enter text.

☒ New system

☐ Significant modification to an existing system

☐ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable): Click here to enter text.

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
This is a new system and is in the beginning phases of assessment and authorization.

(c) Describe the purpose of the system:
Recruiters and Diplomats-in-Residence in the Bureau of Global Talent Management Office of Recruitment, Examination, and Employment (GTM/REE), as well as recruiters across the Department's functional bureaus, host and attend numerous public careers-focused events in order to raise awareness about the Department's work and to recruit for specific positions. The recruitment process is lengthy and requires consistent communication to bring someone with no knowledge about the Department's opportunities to the point where they apply for a position. Recruiters must strengthen and maintain their connections to prospects and points of contact at external organizations. Yello integrates with careers.state.gov and the DOSCareers mobile app to promote upcoming events. GTM/REE must also record and evaluate its efforts to strategically

plan. Yello Enterprise (YE) is a critical tool that allows recruiters to collect information from event attendees, email event attendees after an event, and document information about the event, the organization hosting the event, and the points of contact relating to the event.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

- Personal Email Address
- First Name
- Last Name
- University/Organization
- Current City
- Current State
- Zip Code
- Race or Ethnic Background
- Gender Identity
- Disability Status
- Personal Phone Number

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?
This information collection is in furtherance of the objectives enunciated by the Congress in the Foreign Service Act of 1980.

22 U.S.C. §2651a.Organization of the U.S. Department of State:
https://www.gpo.gov/fdsys/pkg/USCODE-2014-title22/html/USCODE-2014-title22-chap38-sec2651a.htm.

5 U.S.C. §3111 Acceptance of volunteer service:
https://www.gpo.gov/fdsys/pkg/USCODE-2014-title5/html/USCODE-2014-title5-partIII-subpartB-chap31-subchapI-sec3111.htm

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?
☒Yes, provide:

- SORN Name and Number: STATE-31, Human Resource Records
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): Publication Date Friday, July 19, 2013. Volume 78, Number 139. Public Notice 8384; Page 43258.

☐No, explain how the information is retrieved without a personal identifier.
Click here to enter text.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☒Yes ☐No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): A-04-002-01a
- Length of time the information is retained in the system: 10 Years
- Type of information retained in the system:
  Recruitment and General Subject Files. Correspondence, reports and other reference material pertaining to the operation and administration of recruitment functions.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.
☒ Members of the Public
☒ U.S. Government employees/Contractor employees
☐ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐Yes ☒No

(c) How is the information collected?
The information is collected directly from the individuals who voluntarily fill out a sign-in form through the YE Companion application or a YE Registration Link.

(d) Where is the information housed?
☐ Department-owned equipment
☐ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☒ Other

- If you did not select "Department-owned equipment," please specify.

Data is stored in Amazon Web Service (AWS) and is encrypted using AES-256 encryption. Yello data is sandboxed. Yello Enterprise works with a companion mobile app called Yello Pro. As part of the sandboxing process, the system installs each app in its own sandbox directory, which acts as the home for the app and its data. Yello Pro uses Coredata (sqlite) as a data storage mechanism.

(e) What process is used to determine if the information is accurate?
YE depends completely upon the participants for the accuracy of their personal information. Prospects are periodically sent emails that include an option for them to update their information or opt-out of YE.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
Information updates depend entirely on the prospects' choice to update their information. Prospects are periodically sent emails that include an option for them to update their information.

(g) Does the system use information from commercial sources? Is the information publicly available?
YE does not use information from commercial sources or gather information that is publicly available.

(h) Is notice provided to the individual prior to the collection of his or her information?
The individual provides their own information and must agree to the U.S. Department of State's privacy policy before submitting the information. A Privacy Act Statement is currently being drafted and will precede the gathering of personally identifiable information, which will serve as notification to the individual of the collection and use of their information.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No
- If yes, how do individuals grant consent?

Providing the information is strictly voluntary and only needed if individuals choose to complete the form. If they decide to fill out the form, the following questions remain optional – or may be required in the future, so individuals may decline to provide the information:

- Which of the following best describes your race or ethnic background? Please select all that apply.
- What is your Gender Identity?
- Do you have a Disability?
- Have you served in the U.S. Armed Forces?
- Undergraduate/Anticipated Graduation Date
- Mobile Phone Number

Individuals grant consent by reviewing the Department's Privacy Policy and selecting to complete the form all after appropriate notice is given.

(j) How did privacy concerns influence the determination of what information would be collected by the system?
To protect individuals' privacy, wherever possible, the form asks for general information instead of specific details. For example, the form asks for the user to volunteer whether they have a disability—not the name of the specific disability.

Furthermore, information that is not required at the time of the individual's mere interest in the organization, such as Social Security Numbers, is not collected at this stage of the recruitment process. Such highly sensitive PII is reserved for collection at the stage of application submission and is not entered into this system.

5. Use of information

(a) What is/are the intended use(s) for the information?

The primary goal is to inform, engage, and recruit diverse prospects to pursue careers with the U.S. Department of State. The information collected from prospects will be used to analyze and evaluate diversity recruitment efforts and to provide information relevant to the individual's career interest. YE collects data about events and organizations to create a record of past events and to facilitate strategic event planning. YE collects data about points of contact for organizations to help incoming recruiters set up events. Tracking events and collecting prospect data allows GTM/REE to justify the importance of diversity recruitment to Congress.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes, the use of information is relevant to successful diversity recruitment and that is how the information collected in this system will be used.

(c) Does the system analyze the information stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the information?
Click here to enter text.

(2) Does the analysis result in new information?
Click here to enter text.

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?
☐Yes ☐No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

The information will be shared internally (within State Department) with:

- Bureau of Medical Service's recruitment team (MED)
- Bureau of Information Resource Management's recruitment team (IRM)
- Bureau of Diplomatic Security's recruitment team (DS)

- Bureau of Overseas Buildings Operations' recruitment team (OBO)

All of these bureaus have Administrative Users that can access the information in the system.

No information will be shared externally (outside of State Department).

(b) What information will be shared?
All of the information as listed in question 3d will be shared.

(c) What is the purpose for sharing the information?
MED, IRM, DS, and OBO each have their own recruitment teams, which create and attend their own events. Each team needs access to prospect information in order to develop customized email communications for the prospects attending their events, as well as to evaluate how well their recruitment efforts have reached people in groups who have been historically under-represented in the Department.
.

(d) The information to be shared is transmitted or disclosed by what methods?
YE Administrative Users from the various bureaus can create reports of prospect information and then download that information into an Excel spreadsheet that Yello emails to the Administrative User. Yello only allows reports to be emailed to an email address associated with an Administrative User account. Administrators can also email reports to other Administrative Users through YE.

(e) What safeguards are in place for each internal or external sharing arrangement?
System authentication is based upon role-based access control and session management. All actions performed within the system are audited by controls configured for the operating system and database management.

PII is only present in emails in the form of reports sent from YE to approved @state.gov email address. Consequently, the emails are safeguarded by Department wide email server protections. Per State guidelines and procedures, Emails containing PII must be marked accordingly when transmitted to recipients. Furthermore, emails containing PII can be encrypted using the State PIV.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
Yello is used by GTM/REE at recruiting events to allow interested prospects to provide contact information and select areas of interest within the State Department. As such, Yello allows GTM/REE to obtain PII on potential applicants from a wide variety of backgrounds. Although the PII collected is not extensive, it includes details such as disability status and racial identity, that non-employees expect to be handled with due

diligence. All State employees and contractors are given specific PII safeguarding training. Emails containing PII are marked and when possible, encrypted. Yello users are only granted administrator permissions, which allow for the export of PII, on the basis of a specific need for the individual to perform administrative functions within Yello. Administrative users in GTM/REE are chosen by the GTM/REE/REC Branch Chief of Outreach. Administrators in the other bureaus are chosen by their respective supervisors based on their position and role in recruitment efforts. Administrative access is promptly rescinded or granted when administrative users leave or enter positions requiring access. An audit is done, at the very least, on an annual basis in the summer when turnover of Foreign Service employees is high.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

Individuals gain access to their information in three ways:

1. Prospects are periodically emailed with an option to access and edit their information. They may click the "Update Your Profile" link at the bottom of the emails sent to them.
2. Notice provided to the individual before collecting the information identifies the System of Records Notice (SORN) that governs the collection of this information and greater detail on how to access their information can be found in that SORN posted on the Departments Privacy Office website as well as in the Federal Register.
3. If an individual is provided the link to the Department's Yello Enterprise product, then they can view and update their name, email, phone number, LinkedIn URL, university, degree, major, GPA, and graduation date. To do this, they would need to use the same email they used to sign up with the Department and then create a password that includes uppercase letters, lowercase letters, a number, and a special character.
4. Prospects can access their information through their Yello Passport account. Individuals who have an account directly with Yello can view and update their name, email, phone number, university, and graduation date. These changes will be reflected in their user profile in the Department's Yello Enterprise product. They can then log into their account and update their profile at any time at: https://join.yello.co/login.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

If a prospect wishes to correct inaccurate or erroneous information, they may click the "Update Your Profile" link at the bottom of the emails sent to them periodically. This link will bring them to a page where they can submit changes to their information. Participants may also request their information be deactivated by clicking on an "Unsubscribe" button or by sending an email to doscareers@state.gov.

If no, explain why not.

Click here to enter text.

(c) By what means are individuals notified of the procedures to correct their information?

Individuals are notified by email with clear instructions to "Update Your Profile" included. This information is also provided to them at the time of collection.

8. Security Controls

(a) How is the information in the system secured?

YE is password protected and only Administrative Users who have been issued a username and who have set a password to the site may access information.

Yello Enterprise has access control policies in place to ensure that all users with elevated access are reviewed and approved prior to access being granted. Access control policies and procedures ensure that unauthorized users cannot gain access to Yello and the PII data contained within the system. Yello also provides audit logs of administrative actions taken by users, and these logs can be reviewed to ensure that only approved users and exporting PII for approved purposes. Yello utilizes approved encryption technologies to encrypt the PII data stored within the system.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

Administrative users in GTM/REE are chosen by the GTM/REE/REC Branch Chief of Outreach. Administrators in the other bureaus are chosen by their respective supervisors based on their position and role in recruitment efforts. Administrative access is promptly rescinded or granted when administrative users leave or enter positions requiring access. An audit is done, at the very least, on an annual basis in the summer when turnover of Foreign Service employees is high.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

The system tracks who logs in and when, as well as any actions taken in YE, including emails, exporting information, creating/deleting/editing events, prospects, and campus/organizations. The GTM/REE Marketing Team acts as a system administrator and closely monitors actions taken on the YE.

(d) Explain the privacy training provided to authorized users of the system.
The Department's user policy and rules of behavior are the general terms under which federal employees and contractors use the system. The Department requires all new employees and contractors to attend Cyber Security Awareness training before or immediately after the employment start date and prior to being granted access to the system. Additionally, employees must also complete online course PA-459, Protecting Personally Identifiable Information (PII). In addition, the OpenNet account request form signed by all employees and contractors includes a "Computer Security Awareness Form" that provides privacy orientation. To retain access, all Department personnel must complete annual Cyber Security refresher training, which has a privacy component. Access to data is limited to cleared U.S. Government employees and contractors.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No
If yes, please explain.
An account holder must sign-in with a username and password to gain access to the information. If the user's session remains inactive, the user must log-in again. All data is encrypted using AES-256 encryption when stored in AWS. AWS KMS uses FIPS 140-2 validated hardware security modules.

(f) How were the security measures above influenced by the type of information collected?
Only employees who need access to the information to perform their key responsibilities, such as planning recruitment events or engaging with prospects, are allowed access to YE. Access is also limited by the number of available paid account licenses. Appropriate use of the information is monitored by their supervisors and the GTM/REE Marketing Team as a system administrator. Security measures are reassessed on an annual basis and security updates are made more often as needed. Access to YE is reassessed whenever there is turnover of administrative users. High turnover generally occurs in the summer, which is when we do an annual audit of administrative users as well.

9. Data Access

(a) Who has access to data in the system?
Administrative Users have access to the system and all the data held within.

Non-administrative users only have access to their individual information.

The only individuals with access to all the data in the system are Administrative Users. The majority of the Administrative User accounts are held in GTM/REE. Additionally, the bureaus listed in question 6a each have one Administrative User to access the system itself.

(b) How is access to data in the system determined?

Access directly to the data in the system is determined by GTM/REE management and the management of the specific bureaus listed in question 6a. This determination is made based on their role within a Department recruitment team as assessed by their individual management. Those individuals identified by leadership will be granted Administrative User accounts and can access the information directly in YE.

Access to the information itself, once exported from the system, is determined by the role of the recruiter in the respective bureaus. They, as well, require access to the information to complete key responsibilities of their position to warrant access.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☐Yes ☒No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

All Administrative Users that have usernames and passwords to the system will have access to all the data in the system.

Non-administrative users do not use username/passwords and can only access their data as they are inputting that data into the system, or updating their profile information, using the email address that they used during their initial data submission.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

There is a limited number of paid account licenses associated with a username and password. Employees requesting access to YE must do so through their supervisor and demonstrate a required need of the information to perform their work on a Department recruitment team. Relevant supervisors then submit the request to the GTM/REE Marketing Team as the YE system administrator who grants access. Anytime users no longer need access, because they leave the position or their role on the recruitment team changes, then their access is promptly rescinded. Additionally, an audit of administrative users is conducted on an annual basis.