PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

YELLO PRO

2. DOD COMPONENT NAME:

Department of the Navy

3. PIA APPROVAL DATE:

10/11/22

NAVAIRSYSCOM

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [x] New DoD Information System
- [ ] New Electronic Collection
- [ ] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

YELLO PRO will serve as the single authoritative talent recruiting system providing leadership with enterprise-wide visibility into potential hiring candidates of the enterprise and make informed investment decisions with respect to the development of the workforce. YELLO PRO is hosted in a government approved cloud service provider (CSP) data center. The CSP provides security controls that are inherited by the YELLO PRO system. The YELLO PRO application, maintained by Yello, is a Software as a Service (SaaS) based application undergoing FedRAMP Moderate review. Application security will in some cases be manually inherited from Yello or a shared responsibility with the Navy. Application maintenance will be a shared responsibility between Yello and Navy Systems Commands. Authorization and access to the system is only granted to US DoD Civilian and contractor personnel who posses a valid clearance. This is a CONUS solution only. The NAVAIR CSB will be used to facilitate the use of this application. Yello Government Recruiting Solution (YGRS) is based in the Goverment Community Cloud.

The following list are the data information sources for the application use:

- Federal Approved Connected Systems: Okta - User management configurations and user data; New Relic - Application and network monitoring; USA Jobs - Government posted job information; Slack - System metadata; Jira - System metadata; AWS GovCloud - Infrastructure;
- Non-Federal Approved Connected Systems: Airbrake - Application error logs; Daxtra -Application resume parsing service; Ubuntu OS package repository; GitLab - code repository; Google Analytics - User Analytics; Google Workspace -Yello internal email and documents; LocationIQ - Geoip location services; Pendo - User Analytics; Salesforce Government - Customer relation management system; Sendgrid - Email services and reputation management; TinyUrl - Links to resources (e.g., events).; TokBox - Video conferencing; Twilio - SMS messages; YE Commercial - External candidate data
- From Individuals: Paper resume from printout or recruiting events; and electronic exports of candidates

PII elements collected in the Yello Pro IT application (in order as listed/selected in Section 2a):

Citizenship: Must determine if they are US or not for Federal Positions and follow on security clearance qualification

Education Information:

- Degree Level: Used to determine positions eligible for (entry, experienced, etc.)
- University: Used for verification with their university's registrar and accreditation
- Major: Qualification for which type of job series they qualified for: e.g, 08XX, 15XX, 22XX, etc.
- Overall GPA: Qualification for special programs and hiring authorities
- Transcript: To review courses and their applicability to meet position qualifications
- License(s)/Certification(s): To confirm skills for position qualification

Employment Information:

- Position Seeking: Candidate's level of expertise
- Career Field of Interest: Aligns to the job category they are applying for e.g. admin, IT, cyber, logistics, etc.

- Resumes: Collected from individual(s) at recruiting events (both paper and electronic)
Gender/Gender Identification: ERIG data captured to assess diversity efforts (voluntary and for EEO use only)
Home/Cell Phone: Used to contact individual
Military Records:
- Active Duty: (True or False) to determine hiring preference
- Separation Month: what month candidate separated military
- Separation Year: What year candidate separated military be available
First and Last Name: How to address candidate
Personal E-mail Address: Used to contact the individual
Race/Ethnicity: ERIG data captured to assess on diversity efforts (voluntary and for EEO use only)
Work E-mail Address: Used to contact staff employees
Other Information:
- Location Preference: Where the candidate prefers to work
- Veteran Disability (30%+): to determine if eligible for special hiring authority
Schedule A: (yes or no) to determine if eligible for special hiring authority

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

Verification, Identification, Authentication, Data Matching, and Administrative Use

e. Do individuals have the opportunity to object to the collection of their PII? [X] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Candidates may opt out of sharing data. They are not required to fill it out if they don't want to.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [X] Yes [ ] No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Candidates may opt out of sharing data.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

[X] Privacy Act Statement [ ] Privacy Advisory [ ] Not Applicable

PRIVACY ACT STATEMENT -
1. AUTHORITY: Title 5 of the United States Code sections 1104, 1302, 3301, 3304, 3320, 3361, 3393, and 3394 provide The U.S. Office of Personnel Management and other Federal agencies the authority to rate applicants for Federal jobs.
2. PURPOSE: The information requested in this electronic application will be used to evaluate your employment qualifications for organizational employment positions available.
3. ROUTINE USES: We will use the information collected/provided to confirm your records concerning your education qualifications, employment history/status, and military records as applicable.
4. DISCLOSURE: Providing this information is voluntary. Please be advised failure to provided the requested information may delay or prevent review of your qualifications and may potentially prevent future employment with our organization.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

[X] Within the DoD Component	Specify.	NAVAIRSYSCOM's Branch Managers, Hiring Managers, Recruiters, Human Capital Management (HCM) Administrators, HCM System Administrators, and Yello Pro Administrators
[ ] Other DoD Components	Specify.	
[ ] Other Federal Agencies	Specify.	
[ ] State and Local Agencies	Specify.	

☐ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)* Specify.

☐ Other *(e.g., commercial providers, colleges).* Specify.

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☒ Individuals
☐ Databases
☐ Existing DoD Information Systems
☐ Commercial Systems
☒ Other Federal Information Systems

Other Federal Information Systems:
Okta - User management configurations and user data;
New Relic - Application and network monitoring;
USA Jobs - Government posted job information; Slack - System metadata;
Jira - System metadata

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

☐ E-mail
☐ Official Form (*Enter Form Number(s) in the box below)*
☒ Face-to-Face Contact
☒ Paper
☐ Fax
☐ Telephone Interview
☐ Information Sharing - System to System
☒ Website/E-Form
☐ Other *(If Other, enter the information in the box below)*

Paper: standard resume
Website/E-Form: https://navair.recsolu.com/external/form/Sg6QVQqYfqD-4u6aM0nBYg

k. Does this DoD Information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

☐ Yes ☐ No

If "Yes," enter SORN System Identifier N12293-1

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. DAA-GRS-2017-0011-0002

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Large Aggregation SSIC: 12000-19
Disposition: TEMPORARY: Destroy 2 years after termination of register

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply).

(a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) If direct or indirect authority does not exist, DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component must be identified.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
5 U.S.C. 301, Department Regulations; 5 U.S.C. Chapters 11, Office of Personnel Management; 13, Special Authority; 29, Commissions, Oaths and Records; 31, Authority for Employment; 33, Examination Selection, and Placement; 41, Training; 43, Performance Appraisal; 51, Classification; 53, Pay Rates and Systems; 55, Pay Administration; 61, Hours of Work; 63, Leave; 72, Antidiscrimination, Right to Petition Congress; 75, Adverse Actions; 83, Retirement; 99, Department of Defense National Security Personnel System; 5 U.S.C. 7201, Antidiscrimination Policy; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; E.O. 9830, Amending the Civil Service Rules and Providing for Federal Personnel Administration, as amended; 29 CFR 1614.601, EEO Group Statistics; SECNAV Instruction 12250.6, Civilian Human Resources Management in the Department of the Navy; and E.O. 9397 (SSN), as amended.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ Yes ☐ No ☒ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

Command has worked with DNS-14 on submission of 60 day FRN for DoD for submission. as of 21 JULY 2022.