

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:

NAVAIRSYSCOM / Command Operations / HCM

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)

- ☐ From members of the general public ☐ From Federal employees
- ☒ from both members of the general public and Federal employees ☐ Not Collected (if checked proceed to Section 4)

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

- ☐ 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 U.S. DoD Civilian and contractor personnel who possess 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

PII elements collected in the Yello Pro IT application as follows: Citizenship, Disability Information, Education Information, Employment Information, Military Records, Other Information (location preference, Schedule A.

Records Management: Employee candidate intake data profile information.

Reason for PIA Submission: PIA is being submitted for privacy and ATO re-accreditation.

Controlled Unclassified Information (CUI): This application will maintain/collect Controlled Unclassified Information (CUI) in the CUI category of General Privacy.

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? ☒ 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 / providing PII data if they choose not to.

f. Do individuals have the opportunity to consent to the specific uses of their PII? ☒ 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 / information.

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.)

☒ Privacy Act Statement ☒ Privacy Advisory ☐ Not Applicable

PRIVACY ACT STATEMENT

AUTHORITY: 5 U.S.C. §1104, 1302, 3301, 3304, 3320, 3361, 3393, and 3394. SORNS: NM01850-2, Physical Disability Evaluation System Proceedings (December 06, 2013, 78 FR 73515), N12293-1, Human Resources Civilian Portfolio (May 02, 2012, 77 FR 25993) and N12300-2, and Joint Employment Management System (JEMS) (March 10, 2008, 73 FR 12714).

PURPOSE: We need the information requested in this form to evaluate your qualifications. Other laws require us to ask about citizenship, military service, etc. to provide the U.S. Office of Personnel Management and other required federal agencies as required to rate applicants for federal jobs.

ROUTINE USES: Information collected is to confirm information from your records concerning academic record, tenure of employment, civil service status, length of service, and date and nature of action for separation as shown on personnel action forms.

DISCLOSURE: Providing this information is voluntary. Note that failure to furnish the requested information may delay or prevent review of your qualifications and could eventually prevent employment at the NAVAIRSYSCOM organization.

Controlled Unclassified Information (CUI) Advisory DoD Warning Banner

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Controlled Unclassified Information (CUI) Advisory

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

☒ 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 (i.e. Army, Navy, Air Force)

Specify.

☐ Other Federal Agencies (i.e. Veteran's Affairs, Energy, State)

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)

☐ In-Person Contact

☐ Paper

☐ Fax

☐ Telephone Interview

☐ Information Sharing - System to System

☒ Website/E-Form

☐ Other (If Other, enter the information in the box below)

Website/E-Form: Submitted via link - <https://navair.yello.gov/app/collect/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 NM01850-2, N12293-1, N12300-2

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.d.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-2017-0007-0004

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

(3) Retention Instructions.

Individual Record SSIC: 12212 / Large Aggregation Disposition SSIC for record disposition: 12000-16
Disposition Instructions: TEMPORARY: Destroy when survivor or retirement claims are adjudicated or when records are 129 years old,

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 statute 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.

NM01850-2, Physical Disability Evaluation System Proceedings (December 06, 2013, 78 FR 73515). Authorities: 5 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 1216a, Determinations of Disability: Requirements and Limitations on Determinations; DoD 6025.18-R, DoD Health Information Privacy Regulation; and E.O. 9397 (SSN), as amended.

N12293-1, Human Resources Civilian Portfolio (May 02, 2012, 77 FR 25993). Authorities: 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.

N12300-2, Joint Employment Management System (JEMS) (March 10, 2008, 73 FR 12714). Authorities: 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 5013, Secretary of the Navy.

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.

Per OMB ID Control Number: 0703-0088 / Expiration date 30 Sep 2026. OMB Renewal Package was submitted to Echelon 1 Office Information Management (OIM) on: 9/22/26.