PRIVACY IMPACT ASSESSMENT (PIA)

For the

Joint Services Support (JSS) System
National Guard Bureau (NGB)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☒ **Existing DoD Information System**
- ☐ **Existing Electronic Collection**
- ☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: 14629
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☐ **Yes**
- ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier *** NEED TO OBTAIN ***

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

[SEC. 582 of PUBLIC LAW 110-181. YELLOW RIBBON REINTEGRATION PROGRAM. 28 JANUARY 2008]:
"The Secretary of Defense shall establish a national combat veteran reintegration program to provide National Guard and Reserve members and their families with sufficient information, services, referral, and proactive outreach opportunities throughout the entire deployment cycle."

[CNGB POLICY AND IMPLEMENTATION GUIDANCE FOR THE DoD YELLOW RIBBON REINTEGRATION PROGRAM. 20 JULY 2009]:
"In collaboration with DoD and with input from the ARNG and ANG Directorates, help establish a single interactive DoD YRRP website portal that contains the national calendar of DoD YRRP events. The office will assist the ARNG and ANG Directorates with the development of a joint interactive automated process for States to request DoD YRRP event funds. Access to service and state specific data will be provided."

[38 U.S.C. § 4301 – 4335. USERRA. 1994]:
The Uniformed Services Employment and Reemployment Rights Act of 1994 (USERRA, 38 U.S.C. §

4301 – 4335) is a federal law intended to ensure that persons who serve or have served in the Armed Forces, Reserves, National Guard or other "uniformed services:" (1) are not disadvantaged in their civilian careers because of their service; (2) are promptly reemployed in their civilian jobs upon their return from duty; and (3) are not discriminated against in employment based on past, present, or future military service.

[DODM 7730.54-M, Volume 1, Enclosure 7. 25 May 2012]
"Report a CEI program data record for each current employment status for RC Service members in the Ready Reserve for the CEI program data. The data quality goal is 100 percent. Each RC shall require their Service members to annually review, verify, and update their CEI program data. SELRES AGR Service members are not required to report their full-time military employment data as CEI but may enter any part-time, student, or specified volunteer employment status. Each RC shall be accountable for ensuring CEI program data compliance such that every Employment Status Code satisfies the annual recertification, each with valid and accurate CEI program data."

[10 U.S.C. 10145, 12302.]

[EO 9397 (SSN).]

[PERFORMANCE WORK STATEMENT]:
"Increased mobilization of the National Guard to Afghanistan, Iraq and at home has raised the need to provide additional support services across all phases of deployment to Service members and their families. The introduction of the Congressionally-mandated Yellow Ribbon program has further underscored this requirement. These facts have heightened the need to get the right people to the right place at the right time to facilitate a more efficient, effective, and coordinated approach to delivery of J1 Support Program Services."

In order to execute the Yellow Ribbon Reintegration Program (YRRP) directives mandated by Congress, the Joint Services Support (JSS) system was developed and implemented to provide Service members, and their families with relevant information, resources, events and points of contacts across various DoD support programs, throughout the Active, Guard and Reserve service components.

The Joint Services Support (JSS) system is a centralized, web-based portal that also manages the life cycle of concurrent events held nationwide for Service members and their families. The collection of personally-identifying information (PII) is required for event registration, confirmation, local/regional event planning, comparison of projected/actual attendance, requisite funding and facility logistics. In addition, collection is required for post event reporting to National Guard and Reserve Component leadership, and ultimately to the United States Congress. Both quantitative data and qualitative feedback from participants is collected to support longitudinal study/outcome-based reporting over time.

In addition to the Yellow Ribbon mandate, the JSS system will also support collection and storage of Civilian Employer Information (CEI) to fulfill the USERRA mandate, as specified in DoDM 7730.54-M, Volume 1, Enclosure 7. The Defense Manpower Data Center (DMDC) will cease operation of CEI website by the end of fiscal year 2012, as a result, the JSS will provide the function instead to allow Service members to continue to report their CEI.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

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

OVERVIEW:

The Joint Services Support (JSS) system's consolidates and publishes program-specific content for seven distinct DoD programs. It also increases awareness, enhances the discoverability of the vast number of events and resources that are available to Service members and their families, fosters community collaboration, provides tools for program staff and the community, and encourages the registration and participation in local/regional events held across the country. Participating programs include:

A. Yellow Ribbon Reintegration Program (YRRP)
B. NGB Employer Support Program (ESGR)
C. Family Program (FP)
D. Financial Management Awareness Program (FMAP)
E. NGB Sexual Assault Prevention & Response Program (SAPR)
F. Psychological Health Program (PHP)
G. Warrior Support (WS)

DETAILS:

To satisfy the mandates mentioned in section 2, item F of this PIA, the Joint Services Support (JSS) system plans to collect and store information for the two initiatives (Yellow Ribbon Reintegration Program and Civilian Employer Information), per the following.

1. Yellow Ribbon Reintegration Program's Requirements for Data Collection and Storage:
1.1. Data Collected Directly from End User:
Basic personal information is collected and stored*.

1.2. Data Stored:
Basic military, unit, and entitlement information is collected and stored*.

2. Civilian Employer Information Requirements for Data Collection and Storage:
2.1. Data Collected Directly from End User:
Basic civilian employer information is collected and stored*.

*Detailed field-by-field descriptions are available on request from NGB J1 office.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Like any other DoD or commercial information system, if PII were to be accessed by an unauthorized individual - all or some of the data elements listed above could be revealed.
From a technical perspective, there are multiple safeguards in place to ensure PII is ONLY accessible by those authorized, which are covered in Section-3-g.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. At this time, information is not shared with entities external to the JSS system. However, information may be shared with Defense Manpower Data Center (DMDC) in the future.

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

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

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

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

Yes. On the JSS portal, a body of text is presented to the user that states the terms of use, privacy policy, and privacy act statement. The user can elect to accept or decline. If a user were to object to the collection of their PII, they can still navigate the resources available on the web site, however may not participate in any activity which requires the data elements mentioned in section 2, item g.

(2) If "No," state the reason why individuals cannot object.

j. 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.

Users who have registered in the system are not able to give or withhold consent for specific uses based on the way the system is programmed; however, if individuals no longer wish to consent for use of their information, they may submit a written request asking that their personal information be removed from the JSS system. All communications will be via e-mail and be channeled through the helpdesk. When received by a JSS technical support representative, the request is forwarded to the JSS development team in the form of a support ticket, with a full audit trail that records the date, time, details and chronology of actions taken. The record is marked with an administrative note in the database and the user is informed that the request is complete.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☒ **Other** ☐ **None**

Describe each applicable format.

The NGB Privacy Policy and the Terms of Use for the JSS system can be found at http://www.jointsupportservices.org on the home page, behind hyper links labeled with the respective titles.

PRIVACY POLICY

This privacy policy statement has been developed to reflect our commitment to our users' privacy.

Why We Collect Your Information

In order for us to provide you with access to the full breadth of functionality on this website, we ask that you create a user profile, which consists of your Name, location, contact information, role and other details that allow us to communicate with you effectively and provide information relevant to you. We do not sell your information to third-parties outside of the organization. In addition, as with most web servers on the World Wide Web today, our server automatically logs information about the environment of each visitor to a website. This type of data-collection is standard, and consists of information that is not personally-identifiable, such as Browser type, Operating System, page response times, and information for statistical analysis to measure visitor interest areas and to provide you with the best experience possible when browsing our website.

How We Collect Information
Below are some of the ways in which information may be collected online and how it may be used.

Use of Cookies
Our Web site may use cookies to keep track of the user's session for the purposes of enhancing the user experience. Cookies are small text files that are stored on a visitor's browser and are used for keeping track of settings or data for a particular Web site. Among other things, we may use cookies to

deliver content specific to our users' interests.

Aggregate Information
Aggregate information about which pages are frequently accessed (for example, links within the site, courses, etc.) is only used for internal review as we continue to improve our Web site.

User Profile
A user profile is created with information that you provide to us and is used for authentication when you login to the site. It can also be used for a) verifying your identity should you wish to contact us, b) marketing information useful to the user, and c) displaying information on the site that is most relevant to the user.

Information Actively Provided by Our Visitors
There are several places where users may choose to provide personally identifiable information about themselves or others. We may augment the information you provide by correlating, collecting, and storing additional information from other Department of Defense (DoD) systems. Unless we tell you otherwise, we will use the information for the purpose the information was provided.

How You Can Access or Correct Your Information
You may review your profile online, have it deleted, and/or withdraw permission for its continued use by contacting us (see Contact Us section)

To protect your privacy and security, we will also take reasonable steps to verify your identity before granting access or making corrections.

Links
Our site contains links to other sites. While we make best effort to screen all sites linked from the system to ensure that they comply with our linking standards, we are not responsible for privacy practices or content of these sites.

Discussion Forums

We host discussion forums which are available for your use. You should NEVER disclose any personal information. You should not enter any forum on the Internet that requires you to disclose any personal information prior to entering. The forums are monitored by our staff regularly.

Online Surveys

Our occasional online surveys are voluntary and anonymous; they are used to improve our site and better serve our clients. When demographic information is collected, we do not ask for any personally identifying information.

Security

This site has security measures in place to protect against the loss or unauthorized/unintentional alteration of the information under our control.

Children's Guidelines

We caution children that they should not divulge their personal information on the Web. Our forums are moderated, and while our moderators cannot prevent children from divulging personal information, they use their best efforts to ensure that personal information is not divulged. In compliance with CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA), we do not allow children of age 12 and under to register online. If during routine audits, such an account is found, appropriate measures are taken to remove from the system immediately.

Acceptance of policy

By visiting our site, you accept the terms and conditions of this Privacy Policy, and consent to our collection, storage and use of your information, as described in this Privacy Policy and elsewhere in

our Site. We reserve the right to modify this Privacy Policy at any time and from time to time. Your continued use of the site after we either personally notify you or generally post such changes will constitute your acceptance of those changes.

Contacting Us

If you have any questions about this privacy statement, the practices of this site, or your dealings with the Joint Services Support (JSS) system, you can contact us by sending an e-mail to feedback@jointservicessupport.org or by regular mail at the following address:

National Guard Bureau (NGB) Manpower and Personnel Directorate (J1), Joint Support Personnel System; 111 South George Mason Drive, Arlington Hall 2, Arlington, VA 22204-1373.

TERMS OF USE

We provide this Web site (the "Site") subject to the following terms and conditions (the "Terms"). By accessing this Site, you agree to these Terms. We reserve the right to change the Terms at any time by updating this posting, and use of this Site following any such changes shall constitute acceptance of such changes.

Copyright & Trademarks:

This Site and all the Contents are the exclusive property of National Guard Bureau J-1 or its licensors, and the trademarks, service marks, designs, logos and other intellectual property displayed on this Site (collectively, the "Trademarks") are the registered and unregistered Trademarks of National Guard Bureau J-1 or its licensors. The Site, the Contents and the Trademarks are protected pursuant to U.S. and international copyright and trademark laws. The content of this site, including but not limited to the text and images herein and their arrangements, unless otherwise noted, are Copyright ©. All Rights Reserved. All trademarks referred to are the property of their respective owners.

Grant of License:

National Guard Bureau J-1 grants you a non-exclusive, non-transferable limited license to access, download, display and print copies of the content displayed on the Site (the "Content") on any computer for DoD use only, subject to the provisions of this Agreement, and provided that you retain all copyright and other proprietary notices displayed on the Content. You may not otherwise reproduce, modify, distribute, republish, download, upload, disclose or commercially exploit the Content without the prior written consent of National Guard Bureau J-1.

Forums and Public Communication:

You agree that you will not post or publish on this Site any materials that:

- are threatening, libelous, defamatory, obscene, pornographic and/or profane;
- constitute or encourage conduct that would constitute a criminal offence or give rise to civil liability or otherwise violate any law;
- infringe the intellectual property, privacy or other rights of any third party;
- contain advertising or false or misleading statements; or
- contain a computer virus or other disruptive or destructive components.

National Guard Bureau J-1 does not regularly review information posted to the Site and is not responsible for such information. National Guard Bureau J-1 reserves the right to refuse to post and the right to remove any information from this Site, in whole or in part, at its sole discretion, at any time, without notice. Except as may be otherwise provided in written agreements between National Guard Bureau J-1 and the users of the Site specified therein, you acknowledge and agree that National Guard Bureau J-1 shall own and have the unrestricted right to use, publish and otherwise

exploit any and all information that you post or otherwise publish on the Site, and you hereby waive any claims against National Guard Bureau J-1 for any alleged or actual infringements of any rights of privacy or publicity, moral rights, or rights of attribution in connection with the use and publication by National Guard Bureau J-1 of such submissions.

Notices of Infringement:

If you believe that any portion of your intellectual property right has been infringed by any submissions posted on the Site, please contact us, giving a written statement that identifies the right or rights claimed to have been infringed and the infringing materials, explains why you believe, in good faith, that the exercise of the intellectual property right is unauthorized, confirms that you believe your statement to be accurate, contains the signature of the intellectual property right owner, and provides your name and contact information. Subject to an opportunity to review such statement, National Guard Bureau J-1 will remove any posted submission that infringes the copyright or other intellectual property right of any person under U.S. or other applicable law. National Guard Bureau J-1 reserves the right to prohibit persons who repeatedly submit infringing or unlawful material from posting further submissions.

Termination of Site and Site Access:

We reserve the right to change the contents of this site or to discontinue it at any time, as well as the right to deny access to the site to any person whom we have reasonable grounds to believe may be using the site for an unlawful or unauthorized purpose or in a manner that may harm us.

Disclaimers:

THIS SITE AND THE CONTENT ARE PROVIDED "AS IS" WITH NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. National Guard Bureau J-1 IS NOT HEREIN ENGAGED IN RENDERING PROFESSIONAL ADVICE AND SERVICES TO YOU. National Guard Bureau J-1 SHALL HAVE NO RESPONSIBILITY OR LIABILITY WITH RESPECT TO ANY INFORMATION PUBLISHED ON LINKED WEB SITES, CONTAINED IN ANY USER SUBMISSIONS PUBLISHED ON THE SITE, OR PROVIDED BY THIRD PARTIES. National Guard Bureau J-1 MAKES NO REPRESENTATIONS OR WARRANTIES WHATSOEVER AS TO THE OWNERSHIP, ACCURACY OR COMPLETENESS OF THE CONTENT OR THAT THIS SITE WILL OPERATE WITHOUT INTERRUPTION.

Liability:

TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAWS, IN NO EVENT SHALL National Guard Bureau J-1 OR ITS THIRD-PARTY CONTENT PROVIDERS BE LIABLE FOR ANY DAMAGES OR ANY KIND, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, COMPENSATORY, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, PUNITIVE OR OTHER DAMAGES, OR FOR LOST REVENUES OR PROFITS, EVEN IF National Guard Bureau J-1 HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES, ARISING OUT OF OR RELATING IN ANY WAY TO THIS SITE, THE CONTENT, OR THE USE OF THIS SITE.

PRIVACY ACT STATEMENT

• Authority: SEC. 582 of PUBLIC LAW 110-181. YELLOW RIBBON REINTEGRATION PROGRAM. 28 JANUARY 2008; CNGB POLICY AND IMPLEMENTATION GUIDANCE FOR THE DoD YELLOW RIBBON REINTEGRATION PROGRAM. 20 JULY 2009; 38 U.S.C. § 4301 – 4335. USERRA. 1994; DoDM 7730.54-M, Volume 1, Enclosure 7; 10 U.S.C. 10145, 12302; EO 9397
• Principal Purpose: This information will be used to verify the identity of eligible populations to provide enhanced information, referrals and resources; support mandates of the Yellow Ribbon Reintegration Program (YRRP) and Employer Support Program (ESGR).
• Routine Uses: None. The "Blanket Routine Uses" set forth in the Systems of Record Notices also applies to this system.

• Disclosure: Voluntary. However, failure to provide the requested information will result in denial of access to system functions.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.