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:

EventPLUS Platform

2. DOD COMPONENT NAME:

Defense Human Resources Activity

3. PIA APPROVAL DATE:

01/14/20

Defense Personnel and Family Support Center (DPFSC)

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)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] 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.

EventPLUS is a comprehensive data, learning, and event management system that supports DPFSC program events and stakeholders. The system was developed and funded as an event management tool to bring uniformity to the National Guard and Reserve Components in event management, implementation, and reporting, as well as its portfolio of programs for data, learning, and events management. The learning management system provides opportunities for DPFSC stakeholders (Service members, volunteers, and associated communities) to access a wealth of online trainings which focus on relevant topics for various military audiences. For events, the system is used to register and approve attendees, report hours, track attendance, create event agendas, request funds and event support, and conduct post-event satisfaction surveys, as well as collect, store, and report pertinent event information. The data management capabilities include the collection and tracking of ESGR Statement of Support Nominations, and the tracking of ESGR Patriot Award delivery.

The following additional capabilities will be included as part of the centralized system: a content management system to make simple website changes (e.g. updating links, posting articles, etc.); SMS/telephony messaging services to receive attendee feedback and participate in attendee learning assessments; e-mail marketing services to share event information and resources and confirm and share registration information; and reporting and analytics in order to support DPFSC's internal programs and external stakeholders (e.g. Reserve Component Program Managers and Event Planners).

Types of information to be collected include: Service affiliation, name, DoD Identification Number, date of birth, gender, phone number, email address, activation and mobilization dates, unit name, and home and unit address. In addition, employment information (type of employment, dates of employment) and employer information (past and current employer name address and phone number) will be collected to allow members of the National Guard and Reserve Component personnel and their family members to submit nominations for employer awards review any prior employer Uniformed Services Employment and Reemployment Rights Act instances, as well as allow civilian employers to request a statement of support.

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)*

Mission-related 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.

Individuals provide information voluntarily and are presented with a Privacy Act Statement at the point of collection. Failure to provide information, however, may inhibit participation in DPFSC events.

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.

Individuals provide information voluntarily and are presented with a Privacy Act Statement at the point of collection. By providing the information the individual is consenting to the specific use outlined in the Privacy Statement and System of Records Notice. Failure to provide information may inhibit participation in DPFSC events.

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

AUTHORITY: 10 U.S.C. 10502, Chief, National Guard Bureau; 38 U.S.C. 4301-4335, Employment and Reemployment Rights of Members of the Uniformed Services; 10 U.S.C. 10145, Ready Reserve: placement in; 10 U.S.C. 12302, Ready Reserve; Public Law 110-181, Section 582, Yellow Ribbon Integration; 20 CFR part 1002, Regulations Under the Uniformed Services Employment and Reemployment Rights Act of 1994; 10 USC Chapter 58, Benefits and Services for Members Being Separated or Recently Separated; DoD Instruction 1342.28, DoD Yellow Ribbon Reintegration Program; DoD Manual 7730.54-M, Vol.2, Reserve Components Common Personnel Data System (RCCPDS): Personnel Reports, and DoD Manual 7730.54 Vol. 1, and Reserve Components Common Personnel Data System: Reporting Procedures.

PRINCIPAL PURPOSE(S): To facilitate comprehensive data, learning, and event management in support of DPFSC program events and stakeholders.

ROUTINE USE(S): Routine uses may be found in the applicable system of records notice INGB 004, Joint Services Support System (JSS) at: https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/608082/ingb-004/

DISCLOSURE: Voluntary, however, failure to provide information may inhibit participation in Defense Personnel and Family Support Center (DPFSC) events.

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

☐ Within the DoD Component	Specify.	
☒ Other DoD Components	Specify.	Active, Guard and Reserve Service Components
☐ 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.	Goldbelt Glacier, Affinity eSolutions Inc. DoD Directive 8500.01 Cybersecurity, DoD Instruction 8510.01 DoD Risk Management Framework (RMF) for DoD Information Technology (IT), DoD Directive 5400.11 DoD Privacy Program, DoD 6025.18-R DoD Health Information Privacy Regulation, DoD 5200.2 R Personal Security Program, and Homeland Security Presidential Directive (HSPD) 12.
☐ 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

Information is collected directly from the individual when registering as a user, registering to attend an event, or reporting their civilian employer information.

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

[X] Information Sharing - System to System [X] Website/E-Form

[ ] Other *(If Other, enter the information in the box below)*

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.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier INGB 004

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. See Below

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

(3) Retention Instructions.

For Event Records (OSD 103-16): Temporary. Cut off Event/Project files upon completion of event. Destroy 10 years after cutoff.

For Training Records (OSD 202-48.1): Temporary. Cut off when course is revised or discontinued. Destroy 40 years after cutoff.

For Award Records (OSD 212-02): Temporary. Cut off annually, in the calendar year upon which the final determination (approval/disapproved) was made. Destroy 15 years after cutoff.

For Messaging/Marketing Records (OSD 102-09): Temporary. Cut off and destroy when superseded or obsolete or when customer requests the Agency to remove the records

For User-name Records (OSD 1601-02): Temporary. Cut off and destroy when business use ceases

For Reporting and Analytic Records (OSD 101-01.2): Temporary. Cut off annually. Destroy 5 years after cutoff or discontinuance, whichever is first.

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.

10 U.S.C. 10502, Chief, National Guard Bureau; 38 U.S.C. 4301-4335, Employment and Reemployment Rights of Members of the Uniformed Services; 10 U.S.C. 10145, Ready Reserve: placement in; 10 U.S.C. 12302, Ready Reserve; Public Law 110-181, Section 582,

Yellow Ribbon Integration; 20 CFR part 1002, Regulations Under the Uniformed Services Employment and Reemployment Rights Act of 1994; 10 U.S.C. 1566, Voting Assistance: Compliance Assessments, Assistance; DoD Instruction 1000.04, Federal Voting Assistance Program (FVAP); DoD Instruction 1342.28, DoD Yellow Ribbon Reintegration Program (YRRP); DoD Manual 7730.54-M, Vol.2, Reserve Components Common Personnel Data System: Personnel Reports, and DoD Manual 7730.54 Vol. 1, and Reserve Components Common Personnel Data System: Reporting Procedures.

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.

[X] 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.

0704-0553

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)*

☐ Biometrics	☒ Birth Date	☒ Child Information
☐ Citizenship	☒ Disability Information	☒ DoD ID Number
☐ Driver's License	☐ Education Information	☐ Emergency Contact
☒ Employment Information	☐ Financial Information	☒ Gender/Gender Identification
☒ Home/Cell Phone	☐ Law Enforcement Information	☐ Legal Status
☒ Mailing/Home Address	☒ Marital Status	☐ Medical Information
☒ Military Records	☐ Mother's Middle/Maiden Name	☒ Name(s)
☐ Official Duty Address	☐ Official Duty Telephone Phone	☐ Other ID Number
☐ Passport Information	☒ Personal E-mail Address	☐ Photo
☐ Place of Birth	☒ Position/Title	☐ Protected Health Information (PHI)[1]
☐ Race/Ethnicity	☒ Rank/Grade	☐ Religious Preference
☐ Records	☐ Security Information	☐ Social Security Number (SSN) *(Full or in any form)*
☒ Work E-mail Address	☐ If Other, enter the information in the box below	

Service affiliation, work phone number, and other preferences to improve event and voter experience (e.g, allergies, absentee ballot information)

DPFSC collects the full names and dates of birth for children attending events. We also ask the parents whether or not their children have any special requirements for accommodation consideration and to facilitate age specific, evidence-based curriculum to support military children during all phases of the deployment cycle through our Project Youth Extension Services program.

DPFSC collects both home and unit addresses to ensure confirmation of Service and family member registration for the conduct of successful DPFSC sponsored events.

If the SSN is collected, complete the following questions.

(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

☐ Yes ☐ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☐ Yes ☐ No

b. What is the PII confidentiality impact level[2]? ☐ Low ☒ Moderate ☐ High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- [ ] Cipher Locks
- [ ] Combination Locks
- [ ] Key Cards
- [x] Security Guards
- [x] Closed Circuit TV (CCTV)
- [x] Identification Badges
- [ ] Safes
- [ ] If Other, enter the information in the box below

(2) Administrative Controls. *(Check all that apply)*

- [x] Backups Secured Off-site
- [x] Encryption of Backups
- [x] Methods to Ensure Only Authorized Personnel Access to PII
- [x] Periodic Security Audits
- [x] Regular Monitoring of Users' Security Practices
- [ ] If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

- [x] Biometrics
- [x] Encryption of Data at Rest
- [x] Firewall
- [x] Role-Based Access Controls
- [x] Virtual Private Network (VPN)
- [x] Common Access Card (CAC)
- [x] Encryption of Data in Transit
- [x] Intrusion Detection System (IDS)
- [ ] Used Only for Privileged (Elevated Roles)
- [x] If Other, enter the information in the box below
- [ ] DoD Public Key Infrastructure Certificates
- [x] External Certificate Authority Certificates
- [ ] Least Privilege Access
- [x] User Identification and Password

Only two factor authentication

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?