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:

Problematic Sexual Behavior in Children and Youth (PSB-CY)

2. DOD COMPONENT NAME:

Office of Secretary of Defense

3. PIA APPROVAL DATE:

06/21/21

Deputy Assistant Secretary of Defense for Military Community and Family Policy (DASD for MC&FP)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

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

- [X] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [ ] 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.

The Problematic Sexual Behavior in Children and Youth (PSB-CY) Information System supports the requirements of Public Law 115-232 Section 1089, Policy on Response to Juvenile-on-Juvenile Problematic Sexual Behavior Committed on Military Installations. This Public Law mandated the establishment of a centralized database of information on incidents of problematic sexual behavior in children and youth on military installations. The PSB-CY Information System captures inputs from multiple offices, thereby capturing and consolidating record-level information for each incident of PSB-CY that is reported to the DoD. Data captured in the PSB-CY Information System spans the full life-cycle of an incident, from the time of report through case closure/resolution.

The PSB-CY Information System is used to:
A. Document, coordinate, and manage the continuum of care provided to children, youth, and their families in order to identify, report, respond, and intervene in incidents of PSB-CY occurring on U.S. military installations.
B. Ensure and implement well-coordinated safety planning, treatment, and support services that address smooth and uninterrupted referrals to specialized services in order to create and maintain safety for and meet the complex needs of children, youth, and their families involved in incidents of PSB-CY.
C. Support statistical analysis, tracking and reporting to ensure continuous process improvement.

Further, the known data elements for the PSB-CY Information System warranted Impact Level (IL) 5 compliance, as defined in the DoD Cloud Computing (CC) Security Requirements Guide (SRG). This higher level of compliance will further ensure an enhanced level of PSB-CY data protection in support of 18 U.S. Code § 5038, Use of Juvenile Records.

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)*

For the purpose of ensuring the safety and security of children and families, and for the identification, (person) data matching, and mission-related use as defined in Section 1(c) herein.

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.

Consent is through the Privacy Act Statement (PAS) at the time of assessments and interviews.

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.

Consent is through the Privacy Act Statement (PAS) at the time of assessments and interviews.

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

Authority: 10 US Code § 1781 - Office of Military Family Readiness Policy; Public Law 115-232 § 1089.

Purpose: The Problematic Sexual Behavior in Children and Youth (PSB-CY) Information System supports the requirements of Public Law 115-232 Section 1089, Policy on Response to Juvenile-on-Juvenile Problematic Sexual Behavior Committed on military installations. This Public Law mandated the establishment of a centralized database of information on incidents of problematic sexual behavior in children and youth on military installations. The PSB-CY Information System captures inputs from multiple offices, thereby consolidating and tracking record-level information for each incident of PSB-CY that is reported to the DoD. Data captured in the PSB-CY Information System spans the full life-cycle of an incident, from the time of report through case closure/resolution.

The PSB-CY Information System is used to:
A. Document, coordinate, and manage the continuum of care provided to children, youth, and their families in order to identify, report, respond, and intervene in incidents of PSB-CY occurring on U.S. military installations.
B. Ensure and implement well-coordinated safety planning, treatment, and support services to address smooth and uninterrupted referrals to specialized services in order to create and maintain safety for and meet the complex needs of children, youth, and their families involved in incidents of PSB-CY.
C. Support statistical analysis, tracking and reporting to ensure continuous process improvement.

Routine Uses: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may specifically be disclosed as a routine use pursuant to 5 U.S.C 552a(b)(3) as follows:
A. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this system of records.
B. To the appropriate federal, state, local, territorial, tribal, or foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.
C. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.
D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.
E. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.
F. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
G. To appropriate agencies, entities, and persons when (1) the DoD suspects of confirms a breach of the system of records; (2) the DoD determined as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
H. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.
I. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.
The applicable System of Records Notice (SORN) is DPR 50, "Problematic Sexual Behavior in Children and Youth (PSB-CY) Information System"

Disclosure: Voluntary; however failure to provide such information may hinder DoD's ability to provide necessary services needed for the exhibiting child, impacted child(ren), and their families. .

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.	DASD MC&FP
[X]	Other DoD Components	Specify.	DoD Family Advocacy Programs (Services and OSD HQ)
[ ]	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)*

- [X] Individuals
- [ ] Databases
- [ ] Existing DoD Information Systems
- [ ] Commercial Systems
- [ ] Other Federal Information Systems

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

- [X] E-mail
- [ ] Official Form (*Enter Form Number(s) in the box below)*
- [X] Face-to-Face Contact
- [X] Paper
- [ ] Fax
- [X] Telephone Interview
- [ ] Information Sharing - System to System
- [ ] 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 DPR 50

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.

Submitted to DPCLTD on May 10, 2021

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. Office of the Secretary of the Defense Records Disposition Schedule (OSD)

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

(3) Retention Instructions.

Cut off and destroy 5 years after the end of the calendar year the case is closed or when a minor child reaches 23 years old." WHS/RDD concluded that the record content of this system would be covered by the Office of the Secretary of the Defense Records Disposition Schedule (OSD/RDS) N1-330-01-002 "DoD Consolidated Medical Records Schedule." Item 9, Mental Health Records.

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. Section 1781, Office of Military Family Readiness Policy; Public Law (P.L.) 115-232, section 1089, "Policy on Response to Juvenile-on-Juvenile Problematic Sexual Behavior Committed on Military Installations."

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.

Currently working with our IMCO to establish the requirement for an OMB Control Number

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	

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.

Submitted to DPCLTD on May 10, 2021, awaiting approval

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

As documented in the Office of the Under Secretary of Defense for Personnel and Readiness (OUSD(P&R)), Directive Type Memorandum (DTM) 07-015-USD(P&R), "DoD Social Security Number (SSN) Reduction Plan," this memorandum justified the collection and use of the SSN for the purpose of collecting data and case file information from DoD agencies that have a role in reporting and responding to Juvenile-on-Juvenile Problematic Sexual Behavior Committed on Military Installations. Use of the SSN within the PSB-CY Database meets the parameters of section 2.c.(8) and (11), "Computer Matching" and " Legacy System Interface" of DoDI 1000.30 "Reduction of Social Security Number (SSN) Use Within DoD," The SSN is used in conjunction with other approved documentation to affirmatively establish identity and confirm matching of individuals between DoD and other Federal agencies that continue to use the SSN as a primary identifier. The majority of children and youth are not assigned DoDID numbers until the age of ten. The only way to uniquely identify using the above named data source is to request and use the SSN. The process of accurately identifying individuals is critical, to avoid errors in identification that can affect decision making and create risk to individuals privacy and security, In addition, identification errors will result in great cost to the government.

(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".

Not applicable. The requirements cited in Section 2(a)(2) herein are consistent with the guidance for acceptable uses of the SSN (as specified in DoDI 1000.30).

(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

Not applicable. The requirements cited in Section 2(a)(2) herein are consistent with the guidance for acceptable uses of the SSN (as specified in DoDI 1000.30).

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
- ☒ Security Guards
- ☒ Closed Circuit TV (CCTV)
- ☒ Identification Badges
- ☒ Safes
- ☒ If Other, enter the information in the box below

DISA milCloud 2.0 Infrastructure

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

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

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

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

DISA milCloud 2.0 Infrastructure

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

PSB-CY is housed in the milCloud 2.0 Impact Level 5 (IL5) Infrastructure.