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:

Evaluation of Barracks Security Repairs and Upgrades, With or Without a Coordinated Communication Plan, as a Prevention Strategy for Harmful Behaviors

2. DOD COMPONENT NAME:

Under Secretary of Defense for Personnel and Readiness

3. PIA APPROVAL DATE:

02/24/2025

Office of Force Resiliency

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
- [x] 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
- [x] 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 purpose of this operational assessment is to examine the impact of environmental upgrades made to U.S. Army barracks on reducing fear of crime and crime-related victimization and perpetration. The upgrades involve the replacement of faulty and less secure locks in U.S. Army barracks with newer, more secure models. The assessment will also evaluate the potential additional impact of a coordinated communications campaign about these protective environment upgrades on the previously stated outcomes.

Our quasi-experimental design (QED) will include 300 E1 to E5 U.S. Army soldiers at Time-point 1 and Time-point 2 each for Group 1 (protective environment upgrades only), Group 2 (protective environment upgrades and coordinated communications), and Group 3 (comparison condition). This evaluation will include 1,800 E1 to E5 U.S. Army enlisted Service Members residing in Army barracks in late 2024 and 2025. There are four data collection components: (1) survey testing discussions; (2) surveys; (3) qualitative interviews and (4) fidelity checklist. All the data collection will be done anonymously other than knowing that the data is from a specific Army Garrison. The evaluation team will not link any of our three data sources (survey, qualitative interview and fidelity checklist) with each other or other sources.

(1) Data collection will begin with nine survey testing discussions with enlisted Service Members to ensure that survey items and interview questions are being interpreted as intended by diverse participants. The following personal information is collected to facilitate the scheduling and hosting of these interviews only: Name, military email address, and position/rank. All survey testing discussion data will be de-identified and will not be linked to any survey responses. Participants will receive a $20 incentive for completing a survey testing discussion that will take 30-60 minutes to complete.

(2) Next, each participant in intervention Group 1 (n= 300), intervention Group 2 (n= 300) and comparison (n= 300) Garrisons will complete cross-sectional 15-minute baseline survey generally prior to the installation of the new security locks and related security upgrades as well. A new group of enlisted Service Members in the intervention Group 1 (n= 300), intervention Group 2 (n= 300) and comparison (n= 300) Garrisons will complete a cross-sectional survey 6 months later. In sum, we will collect 300 surveys per condition per time point with E1 to E5 Army soldiers living in barracks (total N = 1,800). Surveys will be administered online with web links sent to participants via their military email addresses and a QR code to an open survey link advertised on posters and leaflets distributed in the barracks in the study. Personal information collected in the surveys includes: Demographic information including race/ethnicity and sex, position/rank, years of service and relationship/marital status. All military email addresses (and personal email addressed where provided) provided to the research team by the barracks manager or similar personnel will be segregated and maintained separately from the survey responses. All participants will receive a $10 incentive for completing a survey.

(3) Select members of the Garrisons receiving the intervention security upgrades will also be asked to participate in 30-60 minute qualitative interviews (at one single point in time), conducted virtually via Teams/Zoom or by telephone, following completion of the second survey.

We will interview a small number of enlisted Service member living in the barracks (n= 10) and barracks/garrison leadership (n= 5) in each Garrison receiving the intervention (Groups 1 and 2) and each Garrison in the comparison group (Total N= 45). The following personal information will be collected to facilitate the scheduling of these interviews: Demographic information, name, military email address, position/rank and relationship/marital status. The interview data will be de-identified and not linked to other data. Participants will receive a $20 incentive for completing a qualitative interview.

(4) We will use a fidelity checklist form to assess the degree to which the intervention (security enhancements) is delivered as intended. Our checklist form will confirm the implementation of the protective environment upgrades (in the two intervention sites) and the implementation of a coordinated communications campaign (in one site). The checklist will also be used in the comparison sites to assess if any unplanned security enhancements were implemented. It will be completed by the barracks manager or that person's designee.

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)*

The research team will be provided a roster of Service Member residents of impacted barracks and their military email addresses to be used to distribute the surveys and authenticate identity. Email addresses will not be linked to any other data sources and will be destroyed at the conclusion of each data collection period. We will also allow entry to the survey via a QR code that will be placed on posters in the barracks encouraging survey participation. The QR code will take the participant to the survey where they will be asked to enter their military email address to enter the survey. The military email address will then be checked against the roster to confirm the person is a valid study participant (we will not be collecting other identifiers such as barrack room numbers).

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.

Military email addresses will be used to confirm and validate participant identity. An initial invitation to participate in the study will be sent to the list of military email addresses (intervention and comparison cohorts), at which time each recruited participant will have the opportunity to decline participation in the study.

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.

Participants will be informed on what personal information will be collected, how it will be stored, shared, and used in analysis. Participants will have the option to decline participation in the research activities (survey testing discussions, surveys, feedback forms, qualitative interviews). Once collected, however, the information may be used for any of the purposes identified above.

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 Advisory
Disclosure of this information is voluntary and will be used to evaluate the effectiveness of the U.S. Army protective environment upgrades made to U.S. Army barracks. When completed, this form contains personally identifiable information and is protected by the Privacy Act of 1974, as amended.

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.	
☒	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	United States Army
☐	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.	NORC at the University of Chicago abides by the following: Privacy Act and Personally Identifiable Information IAW DoDD 5400.11 dated October 29, 2014, The Privacy Act (5 U.S.C. 552a), DoD 5400.11-R, and DoD Directive 5400.11, DoD Privacy Program, DoD 6025.18-R DoD Health Information Privacy Regulation
☐	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

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)*

Zoom or MS Teams is another option for the qualitative interviews

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

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.

Information will not be retrieved by name or unique identifier.

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-0330-2015-0007-0001

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

(3) Retention Instructions.

Temporary. Cut off annually on completion of research project. Destroy 5 years after cutoff.

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 USC 136, Under Secretary of Personnel and Readiness; DoDI 6400.09, DoD Policy on Integrated Primary Prevention of Self-Directed

Harm and Prohibited Abuse or Harm; DoDI 6400.11, DoD Integrated Primary Prevention Policy for Prevention Workforce and Leaders; DoDI 6495.02, Vol 2 (Sexual Assault Prevention and Response: Education and Training).

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.

Pending - https://www.federalregister.gov/documents/2025/01/17/2025-01133/submission-for-omb-review-comment-request