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:

New Public Portal (NP2)

2. DOD COMPONENT NAME:

DoD Business Enterprise

3. PIA APPROVAL DATE:

06/21/22

Defense Counterintelligence and Security Agency (DCSA)

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.

The purpose of NP2 is to provide internal/external agency customers/partners with a secure, multi-factor authenticated means of communication with DCSA legacy systems on roles and responsibilities. This Privacy Impact Assessment (PIA) is being conducted because the NP2 system processes Personally Identifiable Information (PII) about candidates who are undergoing a background investigation and others whose information may be included in background investigation files.

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)*

NP2 is a system that supports personnel vetting operations. The NP2 system enables users to access e-QIP and PIPS/CVS as well as to create private libraries and communicate with other NP2 users concerning background investigations. The information in the private libraries and messages will vary but may include information about the subject of a background investigation, including: first name, last name, address, phone number, aliases used, Social Security Number (SSN), Date of Birth (DOB), Place of Birth (POB), educational information, financial information, personal conduct, legal information, medical information, employment information, and other information requested on the forms listed in Section 1n. In addition, in certain circumstances, name, address, phone number, SSN, spouses, and cohabitants is also maintained, as well as information about others whom the individual identifies or who are identified by the investigator during the course of the investigation. Also, it contains other data that is collected or developed in the course of investigation. The NP2 system also stores invoice information, which contains general information about the background investigation and the agency requesting the investigation, as well as certain information about the subject of the investigation, including name and SSN.

The background investigations consist of several major activities which involve multiple DCSA legacy IT systems. The investigation process is initiated when a sponsoring agency requests an investigation of an identified candidate. The candidate then completes and submits various investigative forms. The information the candidate submits is reviewed and screened by the sponsoring agency's personnel security officer (or designee), who then submits the request for processing through the DCSA legacy system, Electronic Questionnaire for Investigations Processing (e-QIP), a system that provides a means to facilitate the processing of standard investigative forms.

Interviews with the candidate and other people related to the investigation are then scheduled and assigned to an investigator or investigators by another DCSA legacy system, Personnel Investigation Processing System (PIPS). PIPS is the primary system for the processing, storing and administration of background investigations on candidates for national security, public trust and non-sensitive positions within the Federal Government. In addition, other relevant information is gathered (e.g., employment, credit, criminal history), and the investigators then produce various Reports of Investigation (ROI). The ROI is then reviewed for completeness and a general case review is conducted. The case is then closed and prepared for delivery. An electronic or printed paper file is then sent to the sponsoring agency, which makes the final decision/adjudication regarding the candidate's investigation. When the sponsoring agency makes its decision regarding the candidate's investigation, it returns the decision/adjudication to the PIPS system for record keeping.

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.

Subjects of investigation cannot object to the collection or use of their PII in NP2, because NP2 is not a system that subjects of investigation have access to. However, at various points throughout the investigative process (e.g., when completing an eQIP form or at the onset of a personal interview), subjects are informed of the voluntary nature of the collection of their PII and participation in the investigative process; and they may object to participate at those times of collection.

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 do not have the ability to consent to the collection and use of their information in NP2. However, individuals who are the subject of an investigation are notified at the point of collection, at the beginning of an in person interview, and on various consent forms about why their information is being collected and the purposes for which it will be used. Individuals do not have the ability to consent to some uses of their information and decline to consent to other uses.

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

While individuals are not provided with notice specifically about NP2, this risk is mitigated by the issuance of various Privacy Act advisements, at various points of information collection, throughout the vetting processes. While the advisements do not explain the NP2 system specifically, the advisements do provide information concerning how an individual's information will be used. In addition, notification specifically about this system is provided through publication of this PIA.

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.	NP2 transports and processes PII from multiple DCSA legacy systems and among agency personnel with a need.
☒ Other DoD Components	Specify.	Yes All. DoD Components are the primary customers on DCSA's Investigation Background Services personnel vetting operations.
☒ Other Federal Agencies	Specify.	NP2 supports Investigation Background Services for non-DoD customers as well.
☐ 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.	DCSA uses contractors in the background investigations process. These contractors use NP2 for collaboration purposes.
☐ 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

NP2 receives PII records from both agency users and information systems. Users load PII into NP2 for the purpose of collaboration between investigators and customers. Approved users load PII into NP2 to facilitate personnel vetting communications and records exchange. Users also load batch records into NP2 that are then ingested by PIPS. Other DCSA legacy information systems also post records containing PII to NP2 for the purpose of being downloaded by DCSA customers.

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

☒ Information Sharing - System to System ☒ Website/E-Form

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

NP2 does not collect information from the general public or Applicant being investigated. NP2 does collect PII from NP2 users in order to create their user accounts. The information collected to create these accounts includes first name, last name, government email, government phone, org name/agency, and User Principle Name (UPN). NP2 users are limited to DCSA investigators, individuals supporting the investigation process and external agencies that request investigation services.

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 DUSDI 02-DOD Personnel Vetting Recor

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. N1-478-08-002 (the OPM schedule), DAA-0446-2019-0004 (the DCSA

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

(3) Retention Instructions.

The records in NP2 are subject to the retention schedules referenced above. Depending on the type of information and the action taken on that information, various retention periods apply. Files obtained from other agencies in the course of an investigation are retained consistent with the agreement between the agency and DCSA.

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. 137, Under Secretary of Defense for Intelligence; 10 U.S.C. 504, Persons Not Qualified; 10 U.S.C. 505, Regular components: Qualifications, term, grade; Atomic Energy Act of 1954, 60 Stat. 755; Public Law 108-458, The Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 401 note); Public Law 114-92, Section 1086, National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2016, Reform and Improvement of Personnel Security, Insider Threat Detection and Prevention, and Physical Security (10 U.S.C. 1564 note); Public Law 114-328, Section 951 (NDAA for FY2017), Enhanced Security Programs for Department Defense Personnel and Innovation Initiatives (10 U.S.C. 1564 note); Public Law 115-91, Section 925, (NDAA for FY2018) Background and Security Investigations for Department of Defense Personnel (10 U.S.C. 1564 note); 5 U.S.C. 9101, Access to Criminal History Records for National Security and Other Purposes; Executive Order (E.O.) 13549, as amended, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities; E.O. 12333, as amended, United States Intelligence Activities; E.O. 12829, as amended, National Industrial Security Program; E.O. 10865, as amended, Safeguarding Classified Information Within Industry; E.O. 13467, as amended, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information; E.O. 12968, as amended, Access to Classified Information; E.O. 13470, Further Amendments to Executive Order 12333; E.O. 13488, as amended, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating

Individuals in Positions of Public Trust; E.O. 13526, Classified National Security Information; E.O. 13741, Amending Executive Order 13467, To Establish the Roles and Responsibilities of the National Background Investigations Bureau and Related Matters; E.O. 13764, Amending the Civil Service Rules; DoD Manual 5200.02, Procedures for the DoD Personnel Security Program (PSP); DoD Instruction (DoDI) 1400.25, Volume 731, DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees; DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC); Homeland Security Presidential Directive (HSPD) 12: Policy for a Common Identification Standard for Federal Employees and Contractors; Federal Information Processing Standard (FIPS) 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors; and E.O. 9397 (SSN), as amended.

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.

The NP2 system does not collect information directly from individuals: however, some of the information shared/exchanged in NP2, comes from DCSA systems, such as PIPS and e-QIP and information that is covered by the PRA. For example, e-QIP collects information via the forms listed below:
SF-85: Questionnaire for Non-sensitive Positions 3206-0261, expiration 30 November 2024
SF-85P: Questionnaire for Public Trust Positions 3206-0258, expiration 31 January 2024
SF-85P-S: Supplemental Questionnaire for Selected Positions 3206-0258, expiration 31 January 2024
SF-86: Questionnaire for National Security Positions 3206-0005, expiration 28 February 2023