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:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

11/17/2025

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
- ☐ 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
- ☐ 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 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. The NP2 system supports personnel vetting operations by processing Personally Identifiable Information (PII) about candidates who are undergoing a background investigation and others whose information may be included in background investigation files. The NP2 system enables users to access Electronic Questionnaire for Investigations Processing (e-QIP) and Personnel Investigation Processing System (PIPS) 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. 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 methods of PII collection are as follows:

• Collaboration Tools: NP2 offers a private library (for file sharing) and a messaging tool (for communication) to facilitate collaboration in support of personnel vetting operations.

• CVS Batch Processing: CVS users load a file into NP2 which contains subject PII and allows the authorized user to submit records containing Clearance, Polygraph, and Homeland Security Presidential Directive (HSPD)-12 data.

• CE Batch Processing: The RAP Back application enables authorized users to upload batch files to revalidate the Rap Back subscription for subjects that are enrolled in the Rap Back program. This application provides users the ability to process multiple Rap Back enrollments, subscriptions and validations.

• NP2 eDelivery: OPM PIPS Imaging System (OPIS) will send eDelivery Case files to NP2 when Agencies are authorized and programmed to receive their closed case results through NP2.

• Invoicing: Enterprise Service Delivery Platform (ESDP) sends lists of outstanding invoices to NP2 to support the Billing and Collection business process.

• IAM: NP2 does not collect information from the general public directly. NP2 collects 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 Principal Name (UPN). NP2 users are limited to individuals supporting the investigation process and external agencies that request investigation services.

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)*

• Collaboration Tools: NP2 offers a private library (for file sharing) and a messaging tool (for communication) to facilitate collaboration in support of personnel vetting operations. 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. 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.
• CVS Batch Processing: The Central Verification System (CVS) is a database that contains information on security clearances, background investigations, and other determinations. It's a primary tool for federal agencies to share information and make reciprocal decisions. CVS is used to identify existing investigations or adjudications, supports reciprocity and information sharing, and provides real-time clearance updates.
• CE Batch Processing: The CE Batch Processing function is used to support Continuous Evaluation (CE), which is a process that involves regularly reviewing a cleared individual's background to ensure they continue to meet security clearance requirements and should continue to hold positions of trust.
• NP2 eDelivery: e-Delivery is the electronic packaging and delivery of closed investigations to customer agencies in a usable format. It eliminates the mail out of hardcopy investigative files and allows DCSA customer agencies to receives the files electronically. NP2 e-Delivery is processed each evening, 24 hours a day, 7 days a week, year-round, including weekends and holidays.
• Invoicing: OCFO uses NP2 to deliver invoice products CV, ESP, ISP, and BI.
• IAM: NP2 collects the minimum amount of security attributes of users to identify them and facilitate system authorization decisions.

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

NP2's Login Page displays the following banner at the bottom of the page: "The information contained herein is subject to the provisions of the Privacy Act of 1974 (5 U.S.C. 552a). This information should be handled in a manner to prohibit its unauthorized disclosure."

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.	Personnel Vetting
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Department of the Army, Department of the Navy, Department of the Air Force
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*		Environmental Protection Agency, Department of Agriculture, Department of Commerce, Department of Education, Department of Energy, Department of Health and Human Services, Department of Homeland Security, Department of Housing and Urban Development, Department of the Interior, Department of Justice, Department of Labor, Department of State, Department of

Specify. Transportation, Department of the Treasury, Department of Veterans Affairs, Central Intelligence Agency, Federal Bureau of Investigation, National Security Agency, Immigration and Customs Enforcement, Customs and Border Protection, Transportation Security Administration, Federal Emergency Management Agency, Secret Service, Drug Enforcement Administration, Bureau of Alcohol Tobacco Firearms and Explosives, U.S. Marshals Service, Federal Aviation Administration, Internal Revenue Service, Bureau of Engraving and Printing, U.S. Mint, Financial Crimes Enforcement Network, Office of the Comptroller of the Currency, Social Security Administration, Centers for Disease Control and Prevention, Food and Drug Administration, National Institutes of Health, Centers for Medicare and Medicaid Services, Substance Abuse and Mental Health Services Administration, U.S. Geological Survey, National Park Service, Fish and Wildlife Service, Bureau of Land Management, Bureau of Indian Affairs, U.S. Forest Service, Rural Development, Food and Nutrition Service, Animal and Plant Health Inspection Service, Food Safety and Inspection Service, Federal Trade Commission, Securities and Exchange Commission, Federal Communications Commission, Federal Energy Regulatory Commission, Nuclear Regulatory Commission, Equal Employment Opportunity Commission, National Labor Relations Board, Federal Election Commission, Consumer Financial Protection Bureau, Small Business Administration, General Services Administration, Office of Personnel Management, Government Accountability Office, Congressional Budget Office, Library of Congress, Government Publishing Office, Smithsonian Institution, National Archives and Records Administration, Office of Management and Budget, U.S. Agency for International Development, Peace Corps, Federal Deposit Insurance Corporation, Federal Reserve System, Export-Import Bank, Millennium Challenge Corporation, National Science Foundation, National Aeronautics and Space Administration, Environmental Protection Agency, National Endowment for the Arts, National Endowment for the Humanities, Institute of Museum and Library Services

☒ State and Local Agencies

Specify. DC Courts, DC Pretrial Services, Court Services and Offender Supervision Agency

☒ 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. Contractors:
DNI Emerging Technologies, LLC (NP2 SA), Harmonia Holdings Group, LLC (NP2 DBA), and SJ Technologies Inc. (NP2 Dev).

Language in the contract that safeguards PII:
While the contract does not include the FAR clauses 52.224-1, 52.224-2, or 39.105 verbatim, contract language does require contractors to comply with the Privacy Act and all associated agency rules when designing, developing, or operating a system of records. For the purposes of the Act, the contractor is legally considered an "employee of the agency," making its personnel subject to the same civil and criminal penalties as federal employees for any violations.

☐ 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
- [x] Existing DoD Information Systems
- [ ] Other Federal Information Systems
- [ ] Databases
- [ ] Commercial Systems

NP2 receives PII from PIPS, OPIS, ESDP.

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

- [ ] E-mail
- [ ] In-Person Contact
- [ ] Fax
- [x] Information Sharing - System to System
- [x] Other *(If Other, enter the information in the box below)*
- [ ] Official Form (*Enter Form Number(s) in the box below)*
- [ ] Paper
- [ ] Telephone Interview
- [ ] Website/E-Form

Agency Liaisons must input their user's PII into NP2's account registration worksheet when creating a user account, 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. DAA-0446-2019-0004-0004, GRS 5.6 170, and GRS 1.1 010

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

(3) Retention Instructions.

DAA-0446-2019-0004-0004: Destroy entire file 3 years after employment or access to agency facilities and equipment terminates.
GRS 5.6 170: Temporary. Destroy in accordance with the investigating agency instruction.
GRS 1.1 010: Temporary. Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.

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.

SF-85: Questionnaire for Non-sensitive Positions, 3206-0261, expiration December 2027 (OPM)
SF-85P: Questionnaire for Public Trust Positions, 3206-0258, expiration April 2027 (OPM)
SF-85P-S: Supplemental Questionnaire for Selected Positions, 3206-0258, expiration April 2027 (OPM)
SF-86: Questionnaire for National Security Positions, 3206-0005, expiration November 2026 (OPM)
Personnel Vetting Questionnaire (PVQ): 3206-0279, expiration November 2026 (OPM)