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:

DCSA Enterprise Service Delivery (ESD formerly CRM)

2. DOD COMPONENT NAME:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

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
- [x] 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.)*

- [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.

Enterprise Service Delivery (ESD formerly CRM) platform is a FedRAMP certified cloud service provider solution that allows organizations to quickly build new applications directly into ESD leveraging existing platform services, applications and integrations to support IT service automation, resource management and shared support services. ServiceNow information and processes are located off premises in the cloud provider's FedRAMP certified data centers.

DCSA will utilize ESD to build and operate a number of different applications that will assist DCSA to conduct its missions. ESD will be used to support various case management functions, and business processes which will automate internal back-office coordination, proactively addressing issues and will facilitate extra-Agency Partnership engagement. ESD provides application suites and software solutions as well as a single, web application development platform to build, customize and automate applications and work flows at DCSA.

Applications currently operating on ESD include systems that process employee information, track and manage internal DCSA processes, and that provide a means for outside organizations to report information to DCSA. Because DCSA continues to develop applications using ESD, this PIA covers both DCSA applications that currently operate on this platform and similar applications it will develop in the near future. ESD allows DCSA to streamline and simplify application development by providing an existing infrastructure that can be modified and customized depending on DCSA needs.

The ESD portal will be used to support NBIS Financial Management and Customer Billing as well as centralize the IT Service Management, Human Capital Management Office (HCMO), Logistics Management Division (LMD), Acquisition and Procurement, Office of the Chief Information Officer and Program Executive Office (PEO) operations which are distributed across the US. DCSA will have a centralized way to measure, track, and improve areas in which ESD gathers information. The easier access to data opens up new channels of communication and collaboration amongst team members and improves collaboration and performance.

ESD will provide a billing system to integrate with the Personnel Vetting System of Record and with the Defense Agencies Initiative and automated workflow capabilities for the Vetting Risk Operations (VRO) to meet the Trusted Workforce 1.25 requirements. The application used at VRO will consist of records and reports containing financial compilations, as it pertains to personnel security investigations. It will also include investigative billing transactions, invoices, and investigative issue resolutions.

Information Technology (IT) Service Management is responsible for IT service request management. The Service Desk serves as the single point of contact for logging, assigning, tracking, reporting, and resolving service requests for the employees and contractors of DCSA. The types of PII collected will be mainly business personally identifiable information (PII). Employee name, E-mail address, office telephone number, and cubicle number.

DCSA will utilize ESD to support IT service desk functions including trouble tickets, incidents, change requests and IT service request management. There are three avenues for customers to submit a service request: Service Desk customers may initiate a service desk ticket through the self-service portal, by contacting the Service Desk by phone or email to report a service incident. Another method to create tickets comes from separate monitoring systems. These monitoring systems send event information (malware event, server down, etc.) to ESD, which is turned into a ticket assigned to the proper IT support team. Once the information is entered in ESD, a system generated ticket with a unique ticket number is created and the ticket is classified based on priority. The Service Desk ticket is assigned to an appropriate IT Service Desk technician who is responsible for driving the ticket to completion. DCSA IT Service desk technicians are able to update the status of the service request ticket by entering work notes and other updates. The ticket is also accessible by the user in the self-service portal.

After the reported issue is resolved, the IT service technician marks the service desk ticket as resolved and no further action is performed. ESD sends the user a summary and brief customer satisfaction survey. This survey is voluntary and helps DCSA IT service desk improve overall operations. No PII is collected; however, the survey is linked to the user's service desk ticket number. Closed incidents are filtered out of view, but will remain in ESD for reference and reporting purposes. Closed incidents can be reopened if the user or IT service technician reports that service request was not sufficiently resolved.

Oversight and administration of Identity and Access Management (IDAM) services falls under the Chief Information Officer. The PEO has been provided with an exclusion for the purpose of integrating the ESD with the GeoAxIS IDAM solution provided through NGA. The GeoAxIS solution will identify and authenticate users of ESD for Role Based Access Control.

The Program Executive Office (PEO) will oversee and manage the Identity and Access Management for ESD through integration with the GSA GeoAxIS solution. The GeoAxIS solution will identify and authenticate users of the ESD platform for Role Based Access Control. The ESD will automate the System Authorization Access Requests (SAAR) (DD Form 2875) which is used for granting access to all DCSA IT Business and Mission Systems. Currently, all system access requests are completed by the employee and signed by the supervisor for determination of system access level, based on the employee's position. Automation of the SAAR process will eliminate physical chain of custody issues associated with paperwork and allow visibility into end to end coordination of system access. Other Access requests which could ultimately be absorbed into ESD include the Personnel Security System Authorization Request (DD Form 2962).
HCMO is responsible for the management of all SF-182 Authorization, Agreement, and Certification of Training approvals and concurrence. In addition, the Individual Development Plan (IDP) DCSA Form 271 is a HCMO professional career development plan initiated by civilian government employees with input, guidance, and concurrence from the employees' rating official. It serves as an annual action plan to help employees develop certain competencies, knowledge, and skills needed to achieve their professional career goals. HCMO is responsible for the oversight and management of all IDPs. This plan covers the one-year period in which the employee will begin or accomplish the developmental objectives. The types of PII collected will be the employees' social security number, date of birth, home mailing address, and grade.

LMD is responsible for overseeing and managing all equipment that is assigned to DCSA employees and contractors. In addition, LMD is responsible for all equipment that is inventoried, tracked, and retained as custodial records. All hand-receipts must be accounted for. An interface with the Defense Property and Accountability System will be addressed in a later phase of implementation.

ESDP will be used in the very near future as the Freedom of Information, Privacy Act, Appeals, Amendments, Complaints, Expungements, Routine Uses, and PII Breach case management on-line portal. Copies of correspondence by requesters; and other documentation will be maintained pertaining to requests for information released or withheld; summaries and logs of actions taken regarding requests. ESD will allow communication with requesters, managing records collection, reviewing and redacting relevant documents. ESD will also facilitate greater citizen interaction by allowing requesters to check the status of their requests. In addition, ESD will support the Department of Justice Annual reporting requirements. ESD accepts and tracks all FOIA and Privacy Act requests from intake to disclosure. The ESD platform will bring together process, content, and governance which supports an integrated single, unified application for managing the entire lifecycle of requests and appeals from initial inquiry to delivery of documents.

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)*

PII is collected to support work involving reconciliation of financial data involving Background Investigation of subject SSN, full name, and related PII contained within NBIS since DAI records only reflect order transaction but not subject details. VRO CE analysts require PII to ensure alerts are matched to the correct subjects in support of Mission. Security, Insider Threat and Mission Assurance (SITMA) requires PII to support COVID-19 reconstitution activities involving exposure management and optional self-reporting (health status). HCMO requires limited PII for employee file management. PII is collected on Freedom of Information and Privacy Act requests to enable DCSA to locate applicable records and respond to requests made under the Freedom of Information and Privacy Act. Requesters are only asked to provide PII to facilitate the identification of records since there is a large number of Federal employees, contractors, civilians, and military personnel who have identical names and/or birth dates and whose identities can only be distinguished by their SSN.

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.

The cleared individuals on whom the PII will be collected have given permission for information to be collected by voluntarily filling out the SF 85 and/or SF 86 Questionnaire for National Security Positions. Both the SF 85 and SF 86 state "The information you provide on this form, and information collected during an investigation, may be disclosed without your consent by an agency maintaining the information in a system of records as permitted by the Privacy Act [5 U.S.C. 552a(b)], and by routine uses, a list of which are published by the agency in the Federal Register." Both the SF 85 and SF 86 list as a Routine Use, disclosure "to Executive Branch Agency insider threat, counterintelligence, and counter terrorism officials to fulfill their responsibilities under applicable Federal law and policy, including but not limited to E.O. 12333, 13587 and the National Insider Threat Policy and Minimum Standards." Individuals can object to the collection of PII on the questionnaires by declining to complete the questionnaire (e.g. SF 86). A similar consent is present for Exposure Management and Self-Reporting for SITMA and any other ESD platform based application deployed to production.
Requesters submitting Freedom of Information and Privacy Act requests are asked to provide specific PII to enable DCSA to locate applicable records and respond to requests made under the Freedom of Information and Privacy Act. If requesters choose not to provide their PII it may hinder in the search to find applicable records.

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.

As described above, PII data is initially approved and provided voluntarily by individuals as part of the SF 86 or SF 85 data collections. Specific uses of the collected data are described in the Privacy Act statements on all data collection forms. The cleared individuals on whom the PII is collected have given permission by voluntarily filling out the SF 85 and/or SF 86 Questionnaire for National Security Positions. Both the SF 85 and SF 86 state "The information you provide on this form, and information collected during an investigation, may be disclosed without your consent by an agency maintaining the information in a system of records as permitted by the Privacy Act [5 U.S.C. 552a(b)], and by routine uses, a list of which are published by the agency in the Federal Register." In addition, individuals are informed that the information they provide as well as information collected during an investigation, may be disclosed without their consent by an agency maintaining the information in a system of records as permitted by the Privacy Act [5 U.S.C. 552a(b)], and by routine uses, a list of which are published by the agency in the Federal Register. Individuals are also advised that they will not receive prior notice of such disclosures under a routine use.

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 [X] Not Applicable

As described above, PII data in the system is initially approved and provided voluntarily by individuals as part of the SF 86 or SF 85 (both reference the Privacy Act) and the authority of the Personnel Vetting Records SORN for which information can be disclosed without the individual's consent. Individuals who are asked to provide specific PII on forms are always furnished with a Privacy Act Statement and/or Advisory.

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)*

[X]	Within the DoD Component	Specify.	DCSA
[X]	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	DAI, US Military Services, and clearance sponsoring organizations.
[X]	Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Any federal agency with government or contractor employees who are granted a security clearance.
[X]	State and Local Agencies	Specify.	State and local law enforcement agencies
[X]	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.	All contractors under the National Industrial Security Program (NISP)
[X]	Other *(e.g., commercial providers, colleges)*.	Specify.	Colleges and consultants affiliated with the DoD and Federal government

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

[X] Individuals [ ] Databases

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

DD 2962, SF 85, SF86, DD 2875, FS 7600A & B, INV 100, and DCSA Form 335

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 DSS/DCSA V2-01 "Inspector General C

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. 1.1, 1.3, 2.2, 2.6, 2.7, 3.1, 3.2, 4.2, 5.4

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

(3) Retention Instructions.

Records are maintained consistent with the retentions in the GRS items listed in section I (1).

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.

The authorities to collect information are as follows: Executive Orders 10450, 10577, 10865, 12333, and 12968; sections 3301, 3302, and 9101 of title 5, United States Code (U.S.C.); sections 2165 and 2201 of title 42, U.S.C.; chapter 23 of title 50, U.S.C.; and parts 2, 5, 731,

732, and 736 of title 5, Code of Federal Regulations (CFR). In addition, the authority for soliciting and verifying your SSN is Executive Order 9397, as amended by EO 13478. In addition, 5 U.S.C. 552, 5 U.S.C. 552a, 32 CFR 310, and 32 CFR 286 are the authorities to collect information on the INV 100 and DCSA Form 335.
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, and Personal Identity Verification (PIV) of Federal Employees and Contractors.

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.

OMB Control number 0705-0004.