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:

Restricted Sexual Assault Serial Offender Database (CATCH)

2. DOD COMPONENT NAME:

Department of the Navy

3. PIA APPROVAL DATE:

09/17/24

NCIS

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 Sexual Assault Serial Offender database (CATCH) is used to collect and compare law enforcement records of sexual assault, including restricted and unrestricted reports for the purpose of identifying serial assault offenders. The NDAA does not allow the information collected to be used to impinge any right or benefit of any individual while in a restricted status. If the victim requests the report to be released as an unrestricted allegation, the report would be treated as a law enforcement report. 5 U.S.C. § 552a(j)(2) exempts law enforcement agencies from the requirements of 5 U.S.C § 552a(d)(2), "right of amendment."

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)*

Data match and suspect identification

e. Do individuals have the opportunity to object to the collection of their PII? [ ] Yes [x] 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.

5 U.S.C. § 552a(d)(2) exempts law enforcement agencies from the Privacy Act requirement to obtain consent from subjects prior to collecting information that is relevant to a criminal investigation.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] 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.

Information collected is only used to identify correlation between other occurrences of assault gathered by way of restricted and unrestricted reports and is maintained confidentially until such time as a CATCH participant provides consent to change the status of the corresponding report to unrestricted.

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
- [x] Privacy Advisory
- [ ] Not Applicable

Privacy Advisory must contain the following notifications:
* The victim is informed that the information is being used to track potential sexual predators in the military.
* The victim is informed that no information from the restricted report will be released for any purpose, including promotion, retention, or criminal prosecution of the alleged perpetrator, unless the victim changes the nature of the allegation from "restricted" to "unrestricted."
* Any report that becomes "unrestricted" could potentially be used as part of a law enforcement investigation and subsequent criminal

prosecution. As such, information given in the report could potentially become public during the discovery and trial phase of the prosecution.

5 U.S.C § 552a(j)(2) makes no further requirements for information collected as part of a law enforcement investigation.

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.	NCIS
[x]	Other DoD Components	Specify.	Air Force OSI, Army CID
[x]	Other Federal Agencies	Specify.	US Coast Guard/CGIS
[ ]	State and Local Agencies	Specify.	
[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.	General Dynamics IT, Contract# N0017819D7693, Task Order# N0018921F3028. The Seaport NexGen IDIQ contains Privacy Act Notification, 52.224-1; Privacy Act -52.224-2; and Privacy and security Safeguards -52.239-1 Navy security policy requires that all positions be given a sensitivity value based on level of risk factors to ensure appropriate protective measures are applied. Contractor employees under this task order are recognized as Non-Critical Sensitive [ADP/IT-II] positions when the task order scope of work require physical access to a federally controlled base, facility or activity and/or requiring access to a DoD computer/network, to perform unclassified sensitive duties. This designation is also applied to contractor employees who access Privacy Act and Protected Health Information (PHI), provide support associated with fiduciary duties, or perform duties that have been identified as National Security Positions. At a minimum, each contractor employee must be a US citizen and have a favorably completed NACLC or T3 or T3R equivalent investigation to obtain a favorable determination for assignment to a non-critical sensitive or IT-II position. The investigation consists of a standard NAC and a FBI fingerprint check plus law enforcement checks and credit check. Each contractor employee filling a non-critical sensitive or IT-II position is required to complete: • SF-86 Questionnaire for National Security Positions (or equivalent OPM investigative product) • Two FD-258 Applicant Fingerprint Cards
[ ]	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
[x]	Existing DoD Information Systems	[ ]	Commercial Systems
[ ]	Other Federal Information Systems		

DoD Person Search (DPS)
https://pki.dmdc.osd.mil/appj/dps/index.html

Site Visitors: DoD and other federal agencies that use research or investigative tasks to perform their official duties.

Purpose: DoD Person Search(DPS) is a web-based application that interfaces with the Authenticated Data Repository (ADR). It can be used for researching and viewing information on personnel and/or dependents.

Login required: Yes. Clients/users of this application have a DMDC Account assigned through EMMA or the DMDC Security Online Web Application

Login types: CAC, PIV (activation of PIV Authentication Certificate is required)

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
- [x] Paper
- [ ] Fax
- [ ] Telephone Interview
- [ ] Information Sharing - System to System
- [x] Website/E-Form
- [x] Other *(If Other, enter the information in the box below)*

PII collected from existing DoD Information Systems, as noted above.

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 N05580-2

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-NU-2015-0005-0016

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

(3) Retention Instructions.

Per SORN N05580-2 Restricted files are destroyed after 50 years. Destruction of records will be accomplished by deletion from the system. No other paper or digital records will be created or maintained.

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 Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, Pub.L. 113-291§543, RESTRICTED REPORTING: Limited Use by MCIOs of Certain Information on Sexual Assaults from Restricted Reports.
SecDef shall submit to SASC and HASC a plan that will allow an individual who files a restricted report to elect to permit a MCIO, on a confidential basis, and without affecting the restricted nature of the report, to access certain information in the report, including identifying information of the alleged perpetrator if available, for the purpose of identifying individuals who are suspected of perpetrating multiple sexual assaults. Required plan elements: 1) an explanation of how the MCIO would use, maintain, and protect information in the restricted

report; 2) an explanation of how the identity of an individual who elects to provide access to such information will be protected; 3) a timeline for implementation of the plan during the one-year period beginning on the date of the submission of the plan to the SASC and HASC. IMPLEMENTATION: DoD Plan Allowing Restricted Reporting Victims to Disclose Suspect or Incident Information for the Purpose of Identifying Serial Offenders – CATCH Plan (Dec 2015)

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 0703-0069 INVESTIGATION OF ADULT SEXUAL ASSAULT IN THE DEPARTMENT OF DEFENSE