PRIVACY IMPACT ASSESSMENT (PIA)

For the

Catch a Serial Offender (CATCH)
Naval Criminal Investigative Service (NCIS)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☒ **New DoD Information System** ☐ **New Electronic Collection**

☐ **Existing DoD Information System** ☐ **Existing Electronic Collection**

☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☐ **Yes, DITPR** Enter DITPR System Identification Number

☐ **Yes, SIPRNET** Enter SIPRNET Identification Number

☒ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ **Yes** ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

TBD

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number	OMB Package has been submitted.
Enter Expiration Date	

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should 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)

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The purpose of CATCH is to identify service members who are repeat sexual assault offenders. The program is directed to victims who elect to file a Restricted Report. No victim PII will be included in a Restricted Report, but subject PII may be furnished by victims willing to provide this information through CATCH. CATCH data will be juxtaposed across MCIO entries of similar data, with the goal of identifying traits in common, and potentially identifying a serial offender. A detailed escalation procedure will then commence, with the intended purpose of identifying serial offenders while protecting victim rights and identity.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The PII contained in the CATCH system will be used to identify individuals involved in potential felonious activities. The system will be built to DoD and federal standards (DoD Risk Management Framework RMF) for Law Enforcement Sensitive but Unclassified data, and physically housed at a federal data center with all of the safeguards required to acquire the Authority to Operate (ATO) of a system so designated. All PII data will be encrypted at rest, and during transmission, and access controls will be in place to limit the access to authorized users only.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. NCIS, AFOSI, USACID

☒ **Other DoD Components.**

Specify. SAPRO

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. All contractors will be US citizens, and cleared to handle law enforcement sensitive data.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

The NDAA does not allow the information collected to be used to impinge any a 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".

j. 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.

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.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐	**Privacy Act Statement**	☒	**Privacy Advisory**
☐	**Other**	☐	**None**

Describe each applicable format.

Privacy Advisory must contain the following notifications:

* 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.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.