PRIVACY IMPACT ASSESSMENT (PIA)

For the

Navy Drug Screening Program (NDSP)
Department of the Navy - BUPERS

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	DADMS ID: 46527
☐	**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.

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

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.

Authorities:

OPNAV Instruction 5350.4D, Navy Alcohol and Drug Abuse Prevention and Control, dated 4 Jun 09

5 U.S.C. 301, Departmental Regulations
5 U.S.C. 302, Delegation of Authority
4 U.S.C. 3101, 4 U.S.C. 3702
E.O. 9397 (SSN), as amended

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.

NDSP is used on workstations at DOD locations worldwide by unit or base drug testing program coordinators or their delegates. It is a standalone application, and no internet connectivity is required. NDSP provides all military services, including Reserve and National Guard, with an automated, standardized application to randomly select personnel to be tested and record the results in the NDSP at the unit level. Access to the NDSP is controlled by unique user name login and password, and limits access required to complete the testing process. NDSP is capable of random selections from personnel listed in the roster, creates all the paperwork needed to process the samples, provides barcode labels for the sample bottles, and allows for statistical reports to be compiled for the local program personnel.

NDSP is the first step in the drug testing process for the Department of Defense. NDSP identifies the personnel to be tested, tracks the testing, provides unit statistics and generates barcoded documentation and labels to submit samples to the Forensic Drug Testing Laboratories. NDSP randomly selects personnel from a unit provided personnel roster database for participation in a Forensic Drug Test. Results are manually entered into NDSP.

Personal information collected: Name, Social Security Number, Gender, Test Results

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

Members with access to the system complete the annual DoD Information Assurance Awareness training per DIACAP requirements. NDSP is Risk Management Framework (DIACAP) accredited and is subject to the monthly and annual Risk Management Framework (DIACAP) verification/confirmation scans.

The perceived threats are primarily computer hackers, disgruntled employees, state sponsored information warfare, and acts of nature (e.g., fire, flood, etc.).

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. Because of this possibility, appropriate security and access controls listed in this PIA are to be put in place.

All systems are vulnerable to "insider threats." All System Managers will be vigilant to this threat by limiting system access to those individuals who have a defined need to access this information. There are defined criteria to identify who should have access to the applications. These individuals have gone through extensive background and employment checks.

Security perimeter protections (firewall, intrusion detection, router access control list, etc.) provided by the hosting enclave. Additionally, strict access control policies and procedures are implemented to ensure is restricted only to those individuals with a need-to-know through role based access schema.

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. DON shore and fleet designated Urinalysis Program Coordinators and Help Desk Support.

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify.

☐ **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.

NDSP does not collect information directly from the individual. Either an updated unit roster is uploaded to NDSP as new personnel report onboard or an individual's information is entered upon check-in by the command urinalysis coordinator.

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.

NDSP does not collect information directly from the individual. Either an updated unit roster is uploaded to NDSP as new personnel report onboard or an individual's information is entered upon check-in by the command urinalysis coordinator.

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.

NDSP does not collect information directly from the individual. Either an updated unit roster is uploaded to NDSP as new personnel report onboard or an individual's information is entered upon check-in (the Administrative Office provides the PAS at check-in and information may be provided from the individual to the command urinalysis coordinator if they arrived before a new roster could be uploaded) by the command urinalysis coordinator.

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.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

☒ Name	☐ Other Names Used	☒ Social Security Number (SSN)
☐ Truncated SSN	☐ Driver's License	☐ Other ID Number
☐ Citizenship	☐ Legal Status	☒ Gender
☐ Race/Ethnicity	☐ Birth Date	☐ Place of Birth
☐ Personal Cell Telephone Number	☐ Home Telephone Number	☐ Personal Email Address
☐ Mailing/Home Address	☐ Religious Preference	☐ Security Clearance
☐ Mother's Maiden Name	☐ Mother's Middle Name	☐ Spouse Information
☐ Marital Status	☐ Biometrics	☐ Child Information
☐ Financial Information	☐ Medical Information	☐ Disability Information
☐ Law Enforcement Information	☐ Employment Information	☐ Military Records
☐ Emergency Contact	☐ Education Information	☒ Other

If "Other," specify or explain any PII grouping selected.	Other: Test Results, Unique Identification Code, Command/unit name, Batch Number and Specimen Number.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

Unit provided personnel roster database and individual (the Administrative Office provides the PAS at check-in and information may be provided from the individual to the command urinalysis coordinator if they arrived before a new roster could be uploaded) .

(3) How will the information be collected? Indicate all that apply.

☒	**Paper Form**	☒	**Face-to-Face Contact**
☐	**Telephone Interview**	☐	**Fax**
☐	**Email**	☐	**Web Site**
☐	**Information Sharing - System to System**		
☐	**Other**		

Unit provided personnel roster database.

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

For verification of the member's name selected, matching the corresponding SSN for testing.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

Mission-Related: As part of the urinalysis verification process and for the specimens sent to the appropriate DoD laboratory for testing of the samples. The laboratory uses SSNs only.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

☐ **Yes** ☒ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

☒ **Users** ☐ **Developers** ☐ **System Administrators** ☐ **Contractors**

☐ **Other**

If "Other," specify here.

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

☐ **Security Guards**	☐ **Cipher Locks**
☐ **Identification Badges**	☐ **Combination Locks**
☐ **Key Cards**	☐ **Closed Circuit TV (CCTV)**
☒ **Safes**	☒ **Other**

The information is encrypted within the NDSP software database and password protected within the computer database. Filed copies are kept locked away in appropriate designated filing systems.

(2) Technical Controls. Indicate all that apply.

☒ **User Identification**	☐ **Biometrics**
☒ **Password**	☐ **Firewall**
☐ **Intrusion Detection System (IDS)**	☐ **Virtual Private Network (VPN)**
☒ **Encryption**	☐ **DoD Public Key Infrastructure Certificates**
☐ **External Certificate Authority (CA) Certificate**	☒ **Common Access Card (CAC)**
☐ **Other**	

If "Other," specify here.

(3) Administrative Controls. Indicate all that apply.

☐ **Periodic Security Audits**

☐ **Regular Monitoring of Users' Security Practices**

☒ **Methods to Ensure Only Authorized Personnel Access to PII**

☒ **Encryption of Backups Containing Sensitive Data**

☐ **Backups Secured Off-site**

☐ **Other**

If "Other," specify here.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

☒ **Yes. Indicate the certification and accreditation status:**

☐	**Authorization to Operate (ATO)**	**Date Granted:**	In Progress
☐	**Interim Authorization to Operate (IATO)**	**Date Granted:**	
☐	**Denial of Authorization to Operate (DATO)**	**Date Granted:**	
☐	**Interim Authorization to Test (IATT)**	**Date Granted:**	

☐ **No, this DoD information system does not require certification and accreditation.**

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Each step of the urinalysis testing process is conducted using established procedures and documented via use of chain-of-custody documents.

Collection, Use, Processing,Disclosure: All samples collected and associated documents are in constant control of the Urinalysis Coordinator until such time that the samples are packaged with the associated documents and properly mailed to the laboratory for testing. The member's personal information from NDSP does not leave the command during normal use. Samples sent to the laboratory for testing cannot have the members name associated with it. The laboratories tests the results per the UIC, Batch Number assigned to a group of samples, the individual specimen number assigned to the individual social security number. The only documents leaving the command are the bottle labels which are attached to the bottles and the DD Form 2624.

Retention, Destruction: Once the member departs the command his or her information is deleted from the database.

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

The perceived threats are primarily computer hackers, disgruntled employees, state sponsored information warfare, and acts of nature (e.g., fire, flood, etc.).

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. Because of this possibility, appropriate security and access controls listed in this PIA are to be put in place.

All systems are vulnerable to "insider threats." All System Managers will be vigilant to this threat by limiting system access to those individuals who have a defined need to access this information. There are defined criteria to identify who should have access to the applications. These individuals have gone through extensive background and employment checks.

The following controls are used to mitigate the risks:

a) Access Controls: Access controls limit access to the application and/or specific functional areas of the all applications. These controls consist of privileges, general access, password control and discretionary access control. Additionally, each user is associated with one or more database roles. Each role provides some combination of privileges to a subset of the application tables. Access to information/records is limited to person (s) responsible for servicing analyzing the record in the performance of the official duties and who are properly screened and are cleared for the "need to know." Users are granted only those privileges that are necessary for their job requirements (e.g., need-to-know). The same roles that protect the database tables also determine what functionality is enabled for the users currently logged on.

b) Confidentiality: Confidentiality ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes.

c) Integrity: Integrity ensures that data has not been altered or destroyed in an unauthorized manner.

There are no servers for NDSP. The application is installed on a standalone workstation that's not connected to the internet.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

Describe here.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee Signature	HINES.KEVIN.BARCLAY.1117508052 Digitally signed by HINES.KEVIN.BARCLAY.1117508052 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=HINES.KEVIN.BARCLAY.1117508052 Date: 2014.06.03 16:40:23 -05'00'
Name:	Kevin Hines
Title:	Navy Drug Screening Program (NDSP) Manager
Organization:	OPNAV N170A Office of Navy Alcohol and Drug Abuse Prevention (NADAP)
Work Telephone Number:	901-874-4250
DSN:	312 882-4250
Email Address:	kevin.b.hines@navy.mil
Date of Review:	03 Jun 14
Other Official Signature (to be used at Component discretion)	BURNS.MARVIN.1115082767 Digitally signed by BURNS.MARVIN.1115082767 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=BURNS.MARVIN.1115082767 Date: 2014.07.01 15:19:08 -05'00'
Name:	Marvin Burns
Title:	BUPERS IA
Organization:	BUPERS 07
Work Telephone Number:	901 874 4836
DSN:	882-4836
Email Address:	marvin.burns@navy.mil
Date of Review:	

Other Official Signature (to be used at Component discretion)	PROTSMAN.ROBERT.SCOTT.1154204233 Digitally signed by PROTSMAN.ROBERT.SCOTT.1154204233 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=PROTSMAN.ROBERT.SCOTT.1154204233 Date: 2014.07.02 09:53:11 -05'00'
Name:	LT Robert Protsman
Title:	BUPERS IAO
Organization:	BUPERS 07
Work Telephone Number:	(901) 974-2378
DSN:	882-2378
Email Address:	robert.protsman@navy.mil
Date of Review:	2 JUL 2014
Component Senior Information Assurance Officer Signature or Designee	TURNER.LODEL.1185429756 Digitally signed by TURNER.LODEL.1185429756 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=TURNER.LODEL.1185429756 Date: 2014.07.02 14:14:37 -05'00'
Name:	Lodell Turner
Title:	BUPERS IAM
Organization:	BUPERS 07
Work Telephone Number:	(901) 874-2271
DSN:	882-2271
Email Address:	lodell.turner@navy.mil
Date of Review:	02 July 2014
Component Privacy Officer Signature	PATTERSON.ROBIN.W.1229323403 Digitally signed by PATTERSON.ROBIN.W.1229323403 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=PATTERSON.ROBIN.W.1229323403 Date: 2014.09.09 19:11:20 -04'00'
Name:	Robin Patterson
Title:	Head, FOIA/Privacy Act Program Office (OPNAV DNS-36)
Organization:	Office of the Chief of Naval Operations (CNO)
Work Telephone Number:	202-685-6545
DSN:	
Email Address:	robin.patterson@navy.mil
Date of Review:	

Component CIO Signature (Reviewing Official)	MUCK.STEVEN.ROBERT.1179488597 Digitally signed by MUCK.STEVEN.ROBERT.1179488597 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=MUCK.STEVEN.ROBERT.1179488597 Date: 2014.09.10 12:45:33 -04'00'
Name:	For Barbara Hoffman
Title:	Principal Deputy CIO
Organization:	Office of the Department of the Navy Chief Information Officer (DON CIO)
Work Telephone Number:	703-695-1842
DSN:	
Email Address:	barbara.hoffman @navy.mil
Date of Review:	10 September 2014

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.