

**U.S. Department of Commerce
NOAA**



**Privacy Impact Assessment
for the
NOAA Ship Fleet Support System (NOAA2220)**

Reviewed by: Mark Graff, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
 Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment NOAA/ OMAO/Ship Fleet Support System

Unique Project Identifier: 006-48-01-15-02-3601-00

Introduction: System Description

NOAA2220 covers sixteen ships with similar general functions and operating characteristics, security needs, and operating environments, and shore-based applications that support the ship missions. Common shipboard IT infrastructure functions include network connectivity, domain authentication, internet connectivity and general business support services, such as file and print services. Ships are configured with satellite communication systems, such as Inmarsat and VSAT, and connect to NOAA networks and the internet via contract satellite service providers. While each ship has common (or class similar) configurations, mission requirements require each to have a unique configuration. To facilitate their inclusion in a consolidated System Security Plan (SSP), each ship and subsystem is described in the System Security Plan.

The NOAA fleet of ships are managed, operated and maintained by NOAA's Office of Marine and Aviation Operations (OMAO), Marine operations centers (MOC), located in Norfolk, Virginia, Honolulu, Hawaii and Newport, Oregon. Additional ship specific support is provided through port office facilities in Woods Hole, Massachusetts; Davisville, Rhode Island; Charleston, South Carolina; Pascagoula, Mississippi; San Diego, California; and Ford Island, Hawaii. Limited pier side support is also provided to ships in Newport, RI and Kodiak, Alaska.

Typical PII transactions in the NOAA2220 system consist of transmitting information to and from NOAA Workforce Management Office, to facilitate Human Resources (HR) processes, processing of benefits for wage mariners, and continuation of medical care for sick and injured mariners, and as required by other government agencies and industry.

For HR processes and processing of wages, NOAA2220 collect: name, work and home addresses, telephone numbers and email addresses and passport number for travel purposes. This data is secured through physical controls for facilities and encryption at rest for soft copies.

Currently NOAA2220 stores Health Insurance Portability and Accountability Act (HIPAA) information in a secure manner (for hard copies they are secured by physical control implemented at each facility that meets NIST SP 800-53 rev.4 requirements and for soft copies data is encrypted at rest) at Marine Operation Center-Atlantic (MOC-A), Marine Operation Center Pacific (MOC-P), and HQ. The HIPAA information consists of medical information for NOAA employees and guests that sail on a NOAA vessel, as well as for contractors who will be on board for more than 24 hours. Whenever this information needs to be transmitted it is done via secure means by Accellion, secure e-mail, or fax (with notification to the recipient so he/she will be standing at the fax machine). There are multiple medical officers who share responsibility for collecting and transmitting HIPAA information. Any medical officer that has this responsibility is trained and aware of how to handle such information.

Information sharing is conducted on an as needed basis after both authorization and need to know have been determined. Most information that needs to be shared is collected and sent to the NOAA Workforce Management Office for dissemination. There are some instances where NOAA employees' PII will be sent to other Department of Commerce (DOC) agencies and to other federal agencies if the employees are detailed temporary or permanently.

Legal authorities to collect PII and/or BII:

NOAA2220's legal authorities to collect PII are: Title 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.C. 3101, 3309, Title 29 U.S.C 651-78, Title 28 U.S.C. 2671-2680, Executive Order 12196, Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966, Title 33 U.S.C. 853i; 853j; 853j-1; 853t; 854; 854a-1; 857-5, 857a, 855, Title 37 U.S.C; Executive Order 10450, Title 16 U.S.C. 143, and Executive Order 11222.

NOAA2200 is a moderate level system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- This is a new information system.
 This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

X This is an existing information system with no new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)

a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License	x	j. Financial Account	
c. Employer ID	x	g. Passport	x	k. Financial Transaction	
d. Employee ID	x	h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify): HR and Medical Files/Records are stored in NOAA2220 on file servers that have least privilege functions enforced on them and only authorized personnel can view them and whenever these records are transmitted it is done via fax or Accellion to service entities. DOB, HIPAA information and other PII are collected only when needed by the requesting staff office in order to provide continuity of care, maintain official records (personnel records/officer records), and HR Processes including hiring, travel and performance appraisals.					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name	X	h. Place of Birth	X	n. Financial Information	
c. Alias	X	i. Home Address	X	o. Medical Information	X
d. Gender		j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education	X	r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Medical records regarding injuries and sickness acquired while underway as necessary to facilitate care when at sea and ashore.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs	X	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)					

--

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify) Sometimes we have NOAA employees that transfer within DOC to other offices such as DOC Office of the Inspector General (OIG) and we are required to transfer PII information. Whenever PII is transmitted to DOC or other federal agencies, it is done via fax or Accellion.					

Non-government Sources					
Public Organizations		Private Sector	X*	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

*Private medical office

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)					
Smart Cards		Biometrics			
Caller-ID		Personal Identity Verification (PIV) Cards			
Other (specify):					

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
---	--

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities					
Audio recordings		Building entry readers			
Video surveillance	X	Electronic purchase transactions			
Other (specify):					

There are not any IT system supported activities which raise privacy risks/concerns.
--

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
To determine eligibility		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Medical care			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

NOAA2220 gathers PII as necessary and requested in order to facilitate the HR processes, provide continuity of medical care to injured and sick wage mariners/NOAA Corp Officers/Visitors riding NOAA vessels, and perform administrative functions such as the training and relocation of employees (Federal employees/contractors).

For HR processes and processing of mariner wages, we collect: name, work and home addresses, telephone numbers and email addresses and passport number for travel purposes. This information is collected through hiring processes, mid-term and annual evaluation periods, and awards. This information is stored on a file server and encrypted at rest

NOAA2220 collects Health Insurance Portability and Accountability Act (HIPAA) information which consist of medical information (health examination information) for OMAO employees. All of OMAO employees are federal employees; however there may be times when a LO may send a contractor to a ship for over a period of 24 hours and thus a medical evaluation will be conducted. In addition, any person becoming injured or ill on a ship would be treated, and the treatment would become part of the person’s medical record. This applies to guests on the ships, also (Federal employees, contractors, members of the public).

NOAA2220 collects information only at the behest of other primary care providers and line offices. Requests for information can come from Veterans Administration, Primary Care Providers, Workforce Management or other line offices as they staff personnel for shipboard research objectives. Medical records will be shared as needed with an individual’s primary care physician.

Whenever an NOAA/OMAO employee transfers to another DOC or federal agency or to a private physician, we are required to transmit those individuals’ PII (Medical information and additional PII, along with a signed consent form). PII is transmitted via Accellion.

NOAA2220 collects two forms of identification (Commerce ID, Driver’s license number and/or passport number in order to issue a CAC or Alt tokens. The system also collects user-id and date-time access information for federal employees and contractors with a valid CAC cards at MOC-P and MOC-A. The form used to collect this information is DD-2841. These forms are stored on NOAA1200 on a file server once received by Local Registration Authority (LRA).

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov’t agencies			
Public			
Private sector	X*		
Foreign governments			
Foreign entities			
Other (specify):			

*To new private physician

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	---

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input type="checkbox"/>	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.
--------------------------	---

	Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. (*Check all that apply.*)

Class of Users			
General Public		Government Employees	X
Contractors			
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. (*Check all that apply.*)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Public Health Services Privacy Act statement in release requests for medical information. It is included in this PIA, just before the signature page.	
X	Yes, notice is provided by other means.	Specify how: The line office provides notice to the employee/contractor on medical-related forms that have the privacy act statement included. Medical information is taken (by medical staff) with the sick/injured person on site and is conveyed strictly for continuity of care. This information is only available within OMAO by qualified medical personnel. A release of information form must be submitted in order for this information to be disseminated outside of the line office and signed by the individual whose information is being released. Performance plans provide notice as part of the forms, but no privacy act statement is included.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII. A release of information form must be submitted in order for this information to be disseminated outside of the line office and signed by the individual whose information is being released.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: A release of information form MUST be signed by the patient
---	---	---

		<p>prior to information being released by or to OMAO. If this document is not signed, medical staff does not release the information. This medical information is used <i>only</i> to determine the level of care/intervention needed for a patient. The release is only for medical information, as stated on the privacy act statement.</p> <p>For administrative functions: Certain users (Privileged Users) may decline to provide PII info on a DD-2841 form; however, this will prevent them from receiving a Alt Token and that will prevent them from being HSPD-12 compliant. NOAA/OMAO employees may decline to provide PII information on performance evaluations.</p>
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	<p>Specify how:</p> <p>A release of information form MUST be signed by the patient prior to information being released by or to OMAO. If this document is not signed, medical staff does not release the information. This medical information is used <i>only</i> to determine the level of care/intervention needed for a patient. The release is only for medical information.</p> <p>For administrative functions: Employees are able to consent to particular uses of their PII. Whenever information is requested from an employee for a particular use within the office or bureau, their signature is required or it will not be released.</p>
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	<p>Specify how:</p> <p>Medical information is updated as new injuries/sicknesses occur to the patient. This information requires a release form to be signed by the patient in order for it to be released. All individuals are made aware of the opportunity to update PII during their employment process and at each annual, bi-annual, or every five year requirement for physicals.</p> <p>For administrative functions, individuals have an opportunity to update their information by contacting the servicing line office in writing to update/review PII pertaining to them in accordance with their guidelines. Otherwise, during</p>
---	---	---

		each evaluation period each employee will have an opportunity to update their PII before signing their evaluation form.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. (*Check all that apply.*)

x	All users signed a confidentiality agreement or non-disclosure agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: NOAA2220 has security controls in place to audit user activities to network share drives where PII/BII is stored.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>4/22/2016</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
x	Contractors that have access to the system are subject to information and privacy security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

NOAA2220 employs hard drive encryption for the laptops that OMAO medical staff uses to store employees PII. This encryption is FIPS 140-2 validated.

For HR information, NOAA2220 employs Virtual Local Area Networks (VLANs)*, and all data is behind firewalls for protection from outside adversaries.

* A VLAN is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any 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.”

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i> : NOAA-10, NOAA Diving Program File; DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons, DEPT-7, Employee Accident Records, DEPT-18, Employees Information Not Covered by of Other Agencies and NOAA-22, NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSD). Also, OPM/GOVT-1, General Personnel Records, OPM-2, Employees Performance File Records apply.
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Management Office requires medical records be handled in accordance with (IAW) Record Schedule 311-02. When applicable all other PII is handled in accordance with NOAA and DOC record schedules: 1700, 200, 600, or other applicable
---	---

	Records Management Schedules. NOAA2220 relies on the servicing staff office to maintain these documents in accordance with the NOAA defined records schedule.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. (Check all that apply.)

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X
Other (specify): When a NOAA2220/OMAO medical staff employee departs and returns their laptop to NOAA2220 IT staff the machine is sanitized in accordance with NIST SP 800-88 requirements. The same is conducted for servers within the NOAA2220 boundary that stores HR information on employees.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. (Check all that apply.)

x	Identifiability	Provide explanation: The information directly identifies a large amount of individuals using names, phone numbers, address, HIPAA information.
x	Quantity of PII	Provide explanation: There is a significant amount of PII.X
x	Data Field Sensitivity	Provide explanation: The data being entered in the system is entered on forms and is stored in a secure manner, accessible by only approved individuals and saved in .pdf form to limit any alteration.
x	Context of Use	Provide explanation: The release of this information could cause moderate harm to the individuals due to the sensitivity of the PII being collected and in some case released.

x	Obligation to Protect Confidentiality	Provide explanation: NOAA2220 is obligated under the Health Insurance Portability and Accountability Act (HPAA) to protect the confidentiality of the PII is process, stores, or transmits and does so by encrypting data at rest and using access controls.
x	Access to and Location of PII	Provide explanation: The information is accessed by Medical staff and Supervisors only with the need to know. Although in some cases the medical staff and supervisor may have laptops they don't store any PII on them and in the case that they may all laptops are encrypted.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: We are reevaluating what PII we collect for new employees and employee evaluations. For example, SSN is no longer collected on any forms that are stored, processed, and transmitted within NOAA2220.
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

National Oceanic and Atmospheric Administration

U.S. Public Health Service

PRIVACY ACT STATEMENT FOR CLIENTS

The following information is provided in order to comply with the requirements of the Privacy Act of 1974, and is consistent with the provisions of 5 CFR Parts 293 and 297.

1. The health services you receive through this program result in the gathering and recording of information that is personal and confidential. Your employing agency serves as a custodian of your records. Upon termination of employment the original documents or copies of your records will be transferred to your Employee Medical Folder (EMF) in the agency's Employee Medical File System (EMFS). These records are stored as a distinct and separate part of your Official Personnel Folder. **Your records are collected and maintained for a variety of purposes, including:**

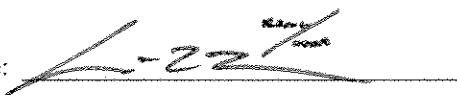
- (a) to meet the mandates of law, Executive order, or regulations;
- (b) to provide data necessary for proper medical evaluations, treatment for the continuity of medical care;
- (c) to provide an accurate medical history and treatment and/or hazard exposures and health monitoring;
- (d) to enable the planning for further care;
- (e) to provide a record of communications among members of the health care team;
- (f) to provide a legal document describing the health care administered and exposure incidents;
- (g) to provide a method of evaluating the quality of health care rendered as required by professional standards and legislative authority;
- (h) to ensure that all relevant, necessary, accurate, and timely data are available to support any medically-related employment decisions;
- (i) to document claims filed with and the decisions reached in OWCP cases;
- (j) to document employee's reporting of occupational injuries, unhealthy and/or unsafe working conditions;
- (k) to ensure proper and accurate operation of the agency's employee drug testing program under Executive Order 12564.

2. **If you do not wish to participate in these services, or to provide the requested information, you are not required to do so. However, if you decline the health services required for job-related clearances, the absence of documented medical clearances will impact your employer's authority to permit you to perform certain functions of your position. You should consult with your supervisor in this matter.**

3. Specified reasons for disclosure of information are identified in the Privacy Act; some, but not all, of the more routine uses are listed below. **The information in your EMF may be disclosed;**

- (a) to a Federal, State, or local agency in compliance with laws governing reporting of communicable disease;
- (b) to a Federal agency, court, or party in litigation when the Government is a party to the proceeding;
- (c) to a Federal, State, or local agency responsible for investigating, prosecuting and enforcing laws and/or regulations;
- (d) to a Federal agency, in connection with the retention of an employee, the issuance of a security clearance, job suitability, classification, letting of a contract, issuance of a license, grant, or other benefit by the requesting agency;
- (e) to a congressional office made at the request of that individual;

Points of Contact and Signatures

<p>Information System Security Officer or System Owner Name: LCDR Ansaruddin Hasan Office: NOAA OMAO Phone: 301-713-7660 Email: ansaruddin.hasan@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: right;"> <small>Digitally signed by HASAN.ANSARUDDIN SA.1376816210 DN: cn=SA.1376816210, o=U.S. Government, ou=NOAA, email=ansaruddin.hasan@noaa.gov, c=US Date: 2016.09.19.09:51:57-0400</small> </p> <p>Signature: <u>HASAN.ANSARUDDIN SA.1376816210</u></p> <p>Date signed: <u>9/19/2016</u></p>	<p>Information Technology Security Officer Name: Darryl Badley Office: NOAA OMAO Phone: 301-713-7734 Email: Darryl.badley@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: right;"> <small>Digitally signed by BADLEY.DARRYL.DUA NE.1077291896 DN: cn=NE.1077291896, o=U.S. Government, ou=NOAA, email=DARRYL.DUA@NOAA.NMFS, c=US Date: 2016.09.13.11:54:47-0400</small> </p> <p>Signature: <u>BADLEY.DARRYL.DUA NE.1077291896</u></p> <p>Date signed: <u>9/13/2016</u></p>
<p>Authorizing Official Name: RDML Anita L. Lopez Office: NOAA OMAO Phone: 301-713-7700 Email: anita.lopez@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u></u></p> <p>Date signed: <u>9/13/16</u></p>	<p>Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>Signature: _____</p> <p>Date signed: _____</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.