

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



**Privacy Impact Assessment**  
**for the**  
**NOAA2220 Fleet Support Service (FSS)**

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

**CATRINA PURVIS** Digitally signed by CATRINA PURVIS

Date: 2020.09.30 19:10:58 -04'00'

09/21/2020

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

Date

## U.S. Department of Commerce Privacy Impact Assessment

### NOAA / Fleet Support System (FSS)

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

#### **Introduction: System Description**

*Provide a description of the system that addresses the following elements:*

*The response must be written in plain language and be as comprehensive as necessary to describe the system.*

The NOAA2220 Fleet Support System (FSS) comprises of sensors, computers, and networked devices that are located on NOAA Office of Marine and Aviation Operations' (OMAO) ships, aircraft, unmanned platforms and at NOAA's Marine and Aircraft Operations Centers that help facilitate OMAO's mission of remote data collection. The NOAA2220 Fleet Support System provides remotely deployable networks, computer systems, and sensors to support and facilitate all aspects of the collection of Oceanographic, Meteorologic, Atmospheric, and Topographical data and transmits the data to other NOAA Line Offices for processing and distribution.

*(a) Whether it is a general support system, major application, or other type of system*

The NOAA2220 Fleet Support System (FSS) is identified as a general support system of computers, sensors, and networked devices most known for collecting scientific data. However, in support of OMAO operations, potential privacy and business sensitive information can exist within some of the functions of the General Support Enclave and Research and Development (R&D) Science Enclave. See figure 1 below.

*(b) System location*

Systems are primarily located onboard NOAA OMAO ships, aircraft, unmanned vehicles, and in the cloud (Azure). However there is a very small number of support systems located at OMAO's Marine and Aircraft Operations Centers 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; and Ford Island, Hawaii. Limited pier-side support is also provided to ships in Newport, Rhode Island and Kodiak, Alaska, though there is no IT equipment located at these locations.

*(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*

The NOAA2220 system is designed to operate in a stand-alone environment and does not require any connections to perform its core requirements. However, during optimal operations, NOAA2220 interconnects with the NOAA NOC/NWAVE for trusted interconnection pathways to the NOAA2220 cloud environment and cyber, marine, and aircraft operations centers. This remotely

deployed system is broken down into enclaves that facilitate all aspects of OMAO's mission operations (see figure 1, privacy view of enclaves and data, next page). There are four main enclaves. Two that cover Operational Technology (OT) and two that cover Information Technology (IT). The OT enclaves are Marine Operational Technology (MOT) and Aviation Operational Technology (AOT). The MOT and AOT enclaves largely consist of navigation, mechanical, propulsion, as well as unmanned command and control systems and present very limited privacy risk in the form of video surveillance and video and photographic imagery from the unmanned functions.

There are two Information Technology (IT) enclaves: the General Support and the R&D Science. The General Support enclave privacy concerns exist within the corporate, medical and public facing web functions. The R&D Science enclave has a very limited privacy risk in the form of video and photographic imagery in the sensors, temp data store, and workstation functions.

## NOAA 2220 Enclave Privacy View

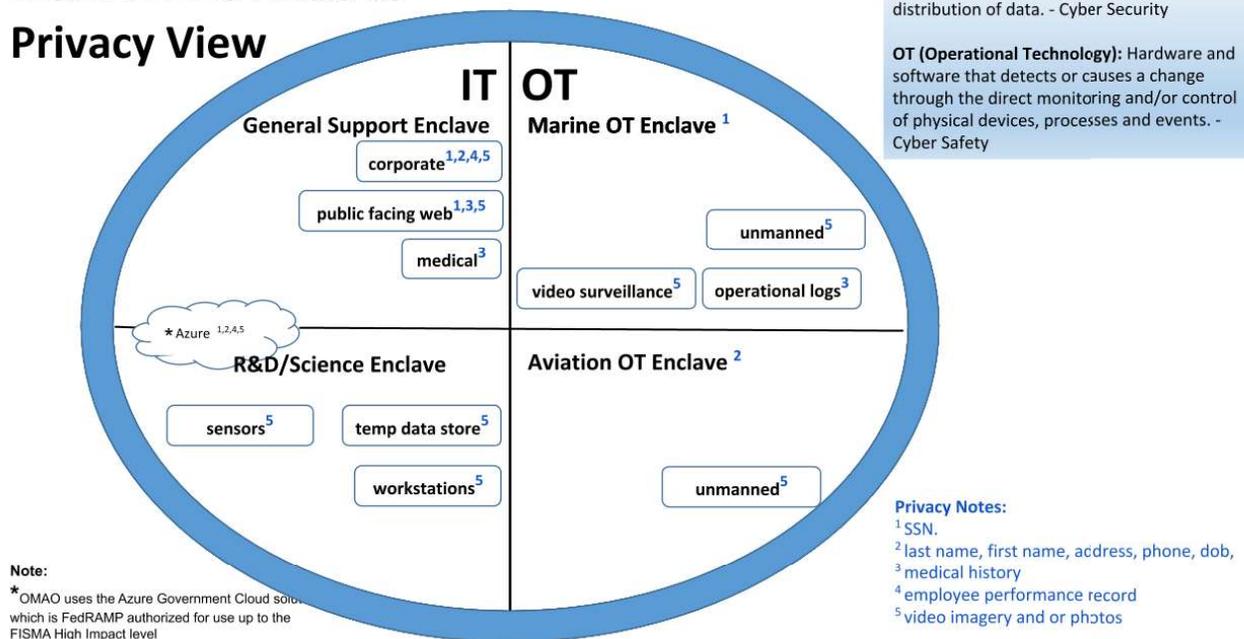


Figure 1

(d) *The way the system operates to achieve the purpose(s) identified in Section 4*

Though the original purpose of the NOAA2220 was to facilitate the remote collection and distribution of raw data, over the years its role has expanded to support many aspects of mission operations. Through this and due to the nature of shipboard operations, the potential to collect sensitive personal and Personally Identifiable Information (PII) exists. IT General Support systems onboard may carry a limited amount of administrative PII to carry out the necessary human resource management. Manning ships and aircraft require personnel meeting certain health and safety standards, therefore health and medical records are also stored and handled to determine crew fitness as well as to treat medical emergencies while underway. Also there is a need to monitor some locations and spaces on ships for personnel safety, therefore a video surveillance system is used to monitor those spaces so images and video of personnel is collected on Marine Operation Technology (MOT). Further incidental personal information in the form of video imagery can be potentially

within the IT R&D Science Enclave under the sensors, data, and display functions (see figure1).

*(e) How information in the system is retrieved by the user*

Users are able to retrieve information from the system by accessing files from computers, laptops, and portable USB devices.

*(f) How information is transmitted to and from the system*

At its core, the purpose of NOAA2220 Fleet Support Systems is to collect scientific data and position marine and airborne assets in the locations of interest. However as described above the purpose of the NOAA2220 system has expanded over time to meet OMAO needs. As it pertains to sensitive business and personal information where the transmission of within the IT General Support Enclave sub-functions), data are transferred to and from the system via computers, USB portable drives, network connections, scanners, and video cameras. The IT R&D Science Enclave sub-function can ingest information from video cameras to the system and this information is transmitted from this Enclave via computers, USB portable drives, and network connections.

*(g) Any information sharing conducted by the system*

Below is a breakdown of the various PII collected including how it is collected and shared.

**Enclave (General Support) Function (corporate)**

**Purpose:** The corporate function of the General Support enclave can span ships, centers, and the cloud and supports fleet corporate and administrative functions. OMAO actions like hiring, payroll, professional review, fitness for duties to act as aircrew members and ship crew members, travel authorizations and clearances. Typical PII transactions within the NOAA2220 boundary collect, store and/or disseminate information with the NOAA Office of Human Capital Services to facilitate Human Resources (HR) actions like Applicants for the NOAA Corps (Name, date of birth, place of birth, country of citizenship (if U.S., how citizenship acquired), mailing address, physical address, telephone numbers, email addresses, social security number, selective service registration, educational information (names and locations of schools, graduation dates, areas of study, years attended, degrees), GPAs for undergraduate and graduate programs, courses (and credit hours) in progress or proposed prior to graduation, college transcripts, credit hours in applicable fields of study, work experience (name and location of company, position title, supervisor contact information, description of work, hours, salary and reason for leaving, whether employment is/was at a professional level), letters of reference, physical examinations, statements of prior military service (rejections, conscientious objector status, type of discharge, current obligations), recruiting officer's interview evaluation form, personal resumes, special qualifications and skills, and names of references. For HR actions like payroll, NOAA2220 collects: name, work and home addresses, telephone numbers and email addresses; and passport number for travel purposes. Also, NOAA2220 collects two forms of photo identification (Commerce ID, Driver's license number and/or passport number) in order to issue a Common Access Card (CAC) or Alt Tokens. The system also collects user-id and date-time access information for federal employees and contractors with a valid CAC at MOC-P and MOC-A. The form used to collect this information is DD-2841. These forms are stored on shipboard NOAA2220 file server once received by Local Registration

Authority (LRA). Health Records are also maintained on ships and at centers to determine fitness for duty and safety for aircrew and ship crew as well as to provide for emergency care while underway. HIPAA information consists of health records of NOAA employees and guests who sail on a NOAA vessel, as well as for contractors who will be on board for more than 24 hours. Further infectious disease testing may be required to allow for crew safety prior to anyone coming onboard ships or aircraft. OMAO requires all health related PII that is transmitted to and from external healthcare or testing providers to be transmitted via secure encrypted means (ssl/https). Also where information is to be emailed OMAO requires the use of Accellion Kiteworks. Fax (with notification to the recipient so he/she will be standing at the fax machine) can be used as a fall-back for emergency situations. There are multiple medical officers who share responsibility for collecting and transmitting HIPAA information. Any medical officer who has this responsibility is trained and aware of how to handle such information. All primary handlers of OMAO HIPAA are PHS officers and take one time HIPAA training from PHS and all are required to have a medical license. These PHS officers also provide one hour annual HIPAA training to OMAO Medical Person In Charge MIPIC's. The Executive Office of each ship also has access to the Medical Records in case of an emergency and there is not a Medical Officer or MIPIC onboard.

**Retention:** Human Resource records are retained indefinitely and ten (10) years after separation records are sent to NRC for archival purposes. OMAO personnel Health and HIPAA records are transferred to the National Archive immediately upon separation from the Agency and local copies are deleted. Guest Health records are kept for 4 years and then local copies deleted.

**Disclosure:** Employees are aware that these are being kept at the time of creation and are not given the option to opt out. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice OPM GOV-1 and DEPT-1,7,9,18,25 and NOAA-1,2,3,4,10,13,14.

---

#### **Enclave (General Support) Function (video surveillance)**

**Purpose:** There is also a small amount of video of PII as associated with cameras on board ship and in secure spaces in OMAO Port offices. The video captured is stored on a secure computer and only accessed by authorized personnel. Ships have a Closed Circuit Television (CCTV) system that is used to record video throughout the ship for the purpose of safety. Ships' personnel are notified by signs located throughout the ship that state that these premises are under video surveillance and cameras in use.

**Retention:** On average records are only retained 30 days due to limited hard drive space. Files are overwritten and are therefore not maintained indefinitely.

**Disclosure:** Crew members are notified of capture of the information in the orientation packet given to those traveling on the ships. Secure spaces with video cameras are marked. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies

---

#### **Enclave (General Support) Function (public facing website)**

**Purpose:** NOAA2220 has 4 public facing websites that deal with PII for Human Resource management: The Commissioned Personnel Center ([CPC application suite](#)<sup>1</sup> which comprises the E-Recruit - NOAA Corps Recruiting application, OPF Online Self Service website for NOAA Corps Officers and the Virtual Board application to assist in Personnel Boards; The Wage Mariner Hiring Portal WMHP<sup>2</sup> aka WMMS (recruiting, hiring, maintaining qualifications of wage mariner employees); The Medical Readiness Tracking Tool MRTT<sup>3</sup> (health records used for fitness determinations for aircraft and ship crew) first name, last name, position, location, physical exam results, vaccinations, email address; The aircraft science data website<sup>5</sup> (aircraft externally mounted video cameras, aircraft mission manifest) all broken down in more detail in follow on sections.

**Retention:** Records are retained indefinitely and are slowly cycled to the NRC site for archival

purposes.

**Disclosure:** Passengers and crew are notified that the manifest is maintained on the public sites and are given the option to opt out. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice OPM GOV-1 and DEPT-1,7,9,18,25 and NOAA-1,2,3,4,10,13,14, MRTT<sup>3</sup> OMAO medical personnel follow the HIPAA notification and disclosure requirements.

---

### **Enclave (General Support) Function (cloud/Azure)**

**Purpose:** The CPC application suite<sup>1</sup> Sites and servers supporting human resource, corporate, and administrative functions rely on cloud-based servers within the NOAA2220 boundary in Azure. These applications and supportive sites are not public facing. Commissioned Personnel Center Human Resource Management System (CPC HRMS) is a back office application for all HR functions of NOAA Corps officers except payroll which is only accessible within OMAO Network and uses oracle access manager for authentication and authorization. Segmentation provides least privilege security and access to the applicable information. The CPC (E-Recruit Application) is used to recruit, hire, and manage all administrative actions for NOAA Commissioned Officers. The CPC Database (CPC HRMS, OPF Online and VirtualBoard Applications) contains the following PII for NOAA Corps officers, their dependents, and NOAA Corps applicants: Name, address, dependent names, dependent addresses, date of birth, and social security numbers of NOAA Corps Officers and their dependents and NOAA Corps Applicants. Further, NOAA Corps officers Security Clearance Details, Medical Fitness Details and Performance Evaluations. Personnel actions for NOAA Corps (CPC) Subject individual, official correspondence and forms generated by routine personnel actions, previous employers, prior military service, Selective Service System, Federal Housing Administration, Social Security Administration, and similar sources, benefits for' wage mariners, and continuation of medical care for sick and injured mariners, and as required by other government agencies and industry. The Wage Mariner Hiring Portal WMHP<sup>2</sup> aka WMMS (recruiting, hiring, qualification of wage mariner employees). The Wage Mariner Hiring Portal (WMHP) system is designed to allow an applicant to apply for a "wage mariner" position within the National Oceanic and Atmospheric Administration (NOAA) fleet of maritime vessels. NOAA will use this information in hiring federal wage mariner employees. The information is used to determine if the applicant meets the basic job qualifications. If the applicant meets the qualifications the applicant's information is then passed on to the hiring official or it is placed in a pool of prospective candidates for future openings. The WMHP system collects basic user information, wage mariner licensing, certifications, and relevant current and or past work history. Applicants fill out basic personal, licensure, and work history information into a profile resume. Once their basic profile is complete, applicants can submit this resume to available wage mariner positions as shown on the WMHP web site. Application information includes: first and last name, contact number and email address, wage mariner licenses and certifications, relevant work history. <sup>3</sup>Medical Readiness Tracking Tool. OMAO uses information in this application to determine fitness of duty for aircrew and ship crew members as well for the emergency treatment of ship crew while deployed. NDL NOAA Dive Logs have personal information like name, telephone, address, and date of birth. The Medical Readiness Tracking Tool MRTT<sup>3</sup> (health records used for fitness determinations for aircraft and ship crew) first name, last name, position, location, physical exam results, vaccinations, email address. Shipboard Automated Maintenance Management System SAMMS belongs to a broader category of software called CMMS (Computerized Maintenance Management Systems) of which ABS's Nautical Systems Enterprise and SpecTech's AMOS among others belong. The SAMMS Sybase Sql database can contain general personal data like firstname, lastname, system administration and audit data like userId and password, as well as some work-related data, i.e., billet assignments and details. SAMMS data is encrypted at rest and while in motion. There are no public facing aspects to this application.

**Retention:** CPC<sup>1</sup> employee records are retained in DB indefinitely. Ten years after separation,

records are sent to NRC for archival purposes. WMHP<sup>2</sup> resumes are purged once a year. MRTT<sup>3</sup> HIPAA health records are sent to the National Archive immediately upon separation from the Agency. Guest health records are kept for four years. SAMMS information is retained only while the employee duties line up with the ship maintenance requirement.

**Disclosure:** Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice OPM GOV-1 and DEPT-1,7,9,18,25 and NOAA-1,2,3,4,10,13,14; The use of this system is mandatory. The failure to use the WMHP<sup>2</sup> system and provide the information will prevent applicants from being evaluated for positions as federal wage mariner employees. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among OMAO Administrative staff for evaluation and hiring purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies. MRTT<sup>3</sup> OMAO medical personnel follow the HIPAA notification and disclosure requirements. Ship maintenance personnel are aware that their information is being stored and used in the SAMMS application.

---

#### **Enclave (R&D Science) Functions (sensors, data, display)**

**Purpose:** Aircraft externally mounted cameras<sup>4</sup> on research aircraft. OMAO assets primarily operate in un-populated areas although on occasion can be called to assist in capturing disaster recovery images. Due to the use of externally mounted video cameras there is a potential to capture accidental video and imagery of people. Aircraft video is published on the public science website with the other aircraft data. Due to the speed of the aircraft, operational altitudes, and resolutions of the down-looking camera, it is likely that it would be possible to identify a person from the video.

**Retention:** This information is only temporarily captured and stored in the science enclave long enough to publish on the public facing website.

**Disclosure:** Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice DOC approved the SORN coverage to be as to subject matter - DOC DEPT-29.

---

#### **<sup>4</sup>Aircraft Science Website (<https://seb.noaa.gov/pub>)**

**Purpose:** Video from aircraft externally mounted cameras<sup>4</sup> on aircraft. OMAO assets primarily operate in un-populated areas although on occasion can be called to assist in capturing disaster recovery images. Due to the use of video cameras there is a potential to capture accidental video and imagery of people. Crew manifest information consisting of first name, last name, and affiliation is published with the flight data. Aircraft mounted Scientific Cameras used to share aircraft meteorological data with the public can include crew manifests which contain a minor amount of PII as part of the scientific crew manifests required during preflight to account for the number of souls on board during aircraft missions. This data may consist of first name, last name, and their flight position (i.e., pilot, navigator, chief scientist, observer, guest). As part of the preflight brief procedures guests and non-NOAA personnel are notified and given the option to opt out. This information is transmitted with the raw data off the aircraft. The raw data set is publically available on the web server.

**Retention:** Files are kept indefinitely.

**Disclosure:** Crew members are notified of capture of the information. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice DOC approved the SORN coverage to be as to subject matter - DOC DEPT-29.

---

#### **Enclave R&D Science Function (unmanned)**

**Purpose:** OMAO uses UxS for imagery in support of NOAA's scientific mission. The data gathered from UxS is initially reviewed by OMAO and then transferred to end users (other NOAA

Line Office scientists) following standard procedures. Use of unmanned systems creates the potential for inadvertent collection of PII, such as images of individuals along the coastlines that are within the area of study by unmanned vehicles. To mitigate this risk, no deliberate retrieval of information using any unique identifier within UxS datasets will be conducted, and any PII inadvertently collected will be deleted within 30 days of identification. NOAA2220 follows policy posted on the [uas.noaa.gov](http://uas.noaa.gov) site along with the NOAA Unmanned Aircraft System Privacy Policy. This policy serves as an application of existing law and policy, and also includes new constraints unique to UAS operations contained in a February 15, 2015, Presidential Memorandum, Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems. OMAO requires users to ensure that all UxS activities adhere to the existing laws and policies regarding PII collection, use, storage, and transmission, as well as to verify that the additional duties outlined in the Presidential Memorandum which have been set forth in the NOAA policy are properly executed. If an aerial drone goes down during flight operations, the retrieval of the unit would be at the discretion of the operator based on the feasibility of retrieval and any safety issues involved in recovery. While recovery is likely during operations over land, the chance of recovery is significantly reduced when operating over open water. If recovery is not possible, there is the possibility that any inadvertently-obtained PII could be recovered by others. Recovery efforts by others would be complicated by the same safety and feasibility concerns that prevented OMAO from recovering the drone, and water damage (possibly including corrosion by salt water) would make data recovery even more difficult. Given the non-sensitive nature of OMAO drone operations, and the fact that most operations are conducted in areas with little or no public presence, OMAO believes the risk is very slight.

**Retention:** Any PII found in drone data is deleted.

**Disclosure:** Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice DOC SORN, DEPT-29.

*(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*

NOAA'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 1966, Title 33 U.S.C. 853i; 853j-1; 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. | Human Resource Information: as outlined in The Department of Commerce (DOC), through NOAA, Office of Marine and Aviation Operations (OMAO) has special hiring authority under Code of Federal Regulations |(CFR), Title 5, Chapter 1, Subchapter A, Part 3, §3.2 and under the DOC Department Administrative Order (DAO) 202-302 Section 2; Subsection .02a. specific to the hiring of federal wage mariner employees | [COMMERCE/NOAA-1, Applicants for the NOAA Corps](#) | [COMMERCE/NOAA-3, NOAA Corps Officer Official Personnel Folders](#) | COMMERCE/DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons | [NOAA-10, NOAA Diving Program File](#); COMMERCE/DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons | COMMERCE/DEPT-7, Employee Accident Records | COMMERCE/DEPT-18, Employees Information Not Covered by Other Agencies | [COMMERCE/NOAA-22, NOAA Health Services Questionnaire \(NHSQ\) and Tuberculosis Screening Document \(TSO\)](#) | OPM/GOVT-1, General Personnel Records | OPM-2, Employees Performance File Records apply. COMMERCE/ DEPT-29, Unmanned Aircraft Systems

*(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system*

FISMA Moderate impact level.
------------------------------

### **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.)*

<b>Changes That Create New Privacy Risks (CTCNPR)</b>					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	X
c. Significant System Management Changes	X	f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): Potential sensitive video can exist within the IT R&D Science enclave under the Sensors, Data and Display functions due to the potential to capture personal imagery through unmanned aerial systems. COMMERCE/DEPT-29					

This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015).

This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

### **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.)*

<b>Identifying Numbers (IN)</b>					
a. Social Security*	X	f. Driver's License	X	j. Financial Account	
b. Taxpayer ID		g. Passport	X	k. Financial Transaction	
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m. Medical Record	X
e. File/Case ID					
n. Other identifying numbers (specify):					

\*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: OMAO CPC applications may collect and maintain SSN, EmployerID, EmployeeID, Driver's License, Passport, and Health Records for Human Resource functions like hiring, payroll, proof of residency, proof of identity for marine and aircraft facility locations, clearance to travel, fitness for duty requirements associated with both aircrew and ships' crew, treatment of medical emergencies onboard vessels at sea. NOAA Medical Providers responsible for the medical care of employees working throughout NOAA may disclose employee HIPAA and other protected information such as a SSN to facilitate medical care in the best interest of the employee.

<b>General Personal Data (GPD)</b>					
a. Name	X	h. Date of Birth	X	o. Financial Information	
b. Maiden Name	X	i. Place of Birth	X	p. Medical Information	X
c. Alias	X	j. Home Address	X	q. Military Service	X
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity		m. Education	X	t. Mother's Maiden Name	
g. Citizenship	X	n. Religion			
u. Other general personal data (specify):					

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

<b>Distinguishing Features/Biometrics (DFB)</b>					
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): (d.)The above identified PII is associated with OMAO. Potentially during operations an Unmanned Aerial System (UAS) may collect video imagery and aerial photos. Any "PII" collected is incidental, unintentional, and not retained.					

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

<b>Other Information (specify)</b>					
Video from a crew safety camera system located on ships. Video for surveillance cameras in secure spaces. Video from externally mounted cameras on manned aircraft. Video cameras mounted on unmanned aircraft.					

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): As selected above OMAO can get Human Resource records due to NOAA employees who transfer within the DOC to other offices such as the 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 Kiteworks. Further OMAO Medical Providers responsible for the medical care of employees working throughout OMAO may send and receive employee HIPAA and other protected information such as a SSN to facilitate medical care in the best interest of the employee, OMAO utilize kiteworks or fax to facilitate this.					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): As selected above OMAO can get sensitive BII information associated with procurements OMAO uses Kiteworks to transfer sensitive BII. Further OMAO Medical Providers responsible for the medical care of employees working throughout OMAO may send and receive employee HIPAA and other protected information such as a SSN to facilitate medical care in the best interest of the employee, OMAO utilize kiteworks or fax to facilitate this.					

## 2.3 Describe how the accuracy of the information in the system is ensured.

As information is entered
<p>OMAO personnel who enter PII check the information for quality and accuracy as they enter the information to ensure that it is correct. Also OMAO application developers code data validation features into the software. JavaScript query validation client side and several features programmed in on the server side including c# custom validation in the mid tier, then database restrictions (length limits, referential integrity, etc.) as the final check input interfaces that validate input of the data. Applications also feature double check (summary page) before submit allowing the OMAO users of sensitive data verify the data as they enter prior to submit. OMAO users make efforts to remove duplicate data. Further NOAA2220 applications that store sensitive information have regular period backups. Applications and file servers utilize NOAA CAC, OMAO Alt Tokens and ICAMS authentication methods to prevent unauthorized access. NOAA2220 uses ADAudit to provide a file access audit tool to monitor access of sensitive files and directories.</p>

## 2.4 Is the information covered by the Paperwork Reduction Act?

X	<p>Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB 0648-0047 Application for Appointment in the NOAA Commissioned Officer Corps OMB 0648-0790 Wage Mariner Hiring Portal COMMERCE/DEPT-18</p>
	No, the information is not covered by the Paperwork Reduction Act.

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

<b>Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)</b>			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify): UAS (drones) are used to gather video imagery and aerial photos for meteorologic, atmospheric, topographic, oceanographic, marine mammal population and damage response. The UAS has the potential to temporarily contain PII.			

<input type="checkbox"/>	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.)*

<b>Activities</b>			
Audio recordings		Building entry readers	
Video surveillance	X	Electronic purchase transactions	
Other (specify): SSN's in Electronic Health Records and Electronic Human Resources records			

- NOAA2220 ships have a Closed Circuit Television (CCTV) system that is used to record video throughout the ship for the purpose of safety as well as for monitoring secured spaces. Ships' personnel are notified by signs located throughout the ship that state that these premises are under video surveillance and cameras in use. Least privileges are enforced for access to the video surveillance data. Only authorized personnel will have access. The NOAA2220 System Owner will be responsible for granting access and controlling who has access to this information. The orientation packet given to those traveling on the ships includes a vessel orientation and a statement about safety compliance.

<input type="checkbox"/>	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.)*

<b>Purpose</b>			
For a Computer Matching Program		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): Unintentional/incidental image or video capture as a result of video camera used on UAS.			

## **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).

In order to support normal business processes, NOAA2220 gathers PII as necessary in order to facilitate the HR activities, provide continuity, and perform administrative functions such as the training and relocation of employees (Federal employees/contractors). For HR actions OMAO collect: name, work and home addresses, telephone numbers and email addresses and passport number for travel purposes. This information is collected through hiring check, mid-term and annual evaluation periods, and awards. In support of missions and operations NOAA2220 collects Health Insurance Portability and Accountability Act (HIPAA) information which consists of medical information (health examination information) for OMAO employees. Any person that is not part of ship's company required to be on board for 24 hours or more will need a medical evaluation. Further infectious disease testing may be required to allow for crew safety prior to anyone coming onboard ships or aircraft. 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, Office of Human Capital Services 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. In support of mission and operations 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 Kiteworks.

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 userid and date-time access information for federal employees and contractors with valid CAC at MOC-P and MOC-A. The form used to collect this information is DD2841. These forms are stored on the Local Registration Authority (LRA) workstation in the HQ OPS center. In support of operations comments from the crew member and or scientists which can be either employee/contractor, member of the public, foreign national, visitor name are saved to the electronic flight jacket and uploaded to Aircraftlogs.com as well crew manifest to the public site. The last name of the commenter is noted. The crew member is typically a Commissioned Officer and or a Civil Servant. The scientist can be a federal employee/contractor, member of the public, foreign national, and or a visitor. As an unintended byproduct of mission operations, video imagery of members of the public may be captured due to manned and unmanned externally mounted video cameras.

- 5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of

information in accordance with the retention schedule, etc.)

There is a potential threat of accidental loss or external threat compromise of PII, medical, HR and video information. There is also a threat insider to unauthorized access and unauthorized modification to PII, medical, HR and video information.

Pertaining to the loss of sensitive information; NOAA2220 has put the following controls in place: OMAO only handles the least amount of PII required in order to operate; laptops and portable devices that contain sensitive information employ FIPS 140-2 validated encryption; all sensitive data in transit within NOAA220 employ FIPS 140-2 validated encryption; NOAA2220 employs multi-factor authentication to restrict access to laptops and portable devices; NOAA2220 regularly scans for vulnerabilities and patches to prevent known threats due to software, hardware, and firmware weaknesses from exploiting potential vulnerabilities; NOAA, OMAO and NOAA2220 train handlers and administrators in the safe handling and threats to sensitive information; When and where possible NOAA2220 leverages NOAA SOC to assist in incidents handling loss or potential loss of sensitive information.

Pertaining to the external threat and compromise of sensitive information; NOAA2220 has put the following controls in place: OMAO only handles the least amount of PII required in order to operate; laptops and portable devices that contain sensitive information employ FIPS 140-2 validated encryption; all sensitive data in transit within NOAA220 employ FIPS 140-2 validated encryption; OMAO uses least privilege principles and follows strict guidelines for limiting access to sensitive information and is restricted to only authorized personnel; NOAA2220 employs multi-factor authentication to restrict access; Sites that are used to gather and process sensitive information are BOD 18-01 compliant and utilize the latest required TDE and ssl encryption modules for information at rest and in motion; NOAA2220 segments, networks, applications, and functions to further isolate and prevent unauthorized access to sensitive information; NOAA2220 employs multi-factor authentication to restrict access to laptops and portable devices; NOAA2220 regularly scans for vulnerabilities and patches to prevent known threats due to software, hardware, and firmware weaknesses from exploiting potential vulnerabilities; OMAO strives to delete and destroy sensitive information when no longer needed; NOAA, OMAO, and NOAA2220 train handlers and administrators in the safe handling and identification of external threats to sensitive information and what to do in case of possible or actual threat; When and where possible, NOAA2220 leverages NOAA SOC to assist in incidents handling evolving the compromise of sensitive information.

Pertaining to the insider threat of unauthorized access and unauthorized modification of sensitive information, NOAA2220 has put the following controls in place: OMAO only handles the least amount of PII required in order to operate, all databases that store sensitive information employ FIPS 140-2 validated encryption. OMAO uses least privilege principles and follows strict guidelines for limiting access to sensitive information and is restricted to only authorized personnel. NOAA2220 employs multi-factor authentication to restrict access. NOAA2220 segments, networks, applications and functions to further isolate and prevent unauthorized access to sensitive information. NOAA2220 employs multi-factor authentication to restrict access to laptops and portable devices. NOAA2220 regularly scans for vulnerabilities and patches to prevent known threats due to software, hardware and firmware weaknesses from exploiting potential vulnerabilities. OMAO strives to delete and destroy sensitive information when no longer needed. NOAA, OMAO and NOAA2220 train handlers and administrators in the safe handling and identification of insider threats to sensitive information and what to do in case of possible or actual threat. When and where possible NOAA2220 leverages also uses NOAA SOC to assist in incidents handling.

## **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			X**
Private sector	X*		
Foreign governments			
Foreign entities			
Other (specify):			

\*\* This only applies to the aircraft mission log. No other PII.

\* To new private physician

	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.

	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	*X	Government Employees	X
Contractors	X		
Other (specify):			

\* This only applies to the aircraft mission log. No other PII.

## **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 Privacy Act statement and/or privacy policy can be found at: <a href="https://www.cio.noaa.gov/itmanagement/pdfs/NOAAPrivacyPolicy_Final_May2017.pdf">https://www.cio.noaa.gov/itmanagement/pdfs/NOAAPrivacyPolicy_Final_May2017.pdf</a> .

X	Yes, notice is provided by other means.	<p>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.</p> <p>For the PII on the aircraft log (passenger's name), the Pilot or Flight Director is required to provide notice to the passengers during the preflight brief. For video surveillance captured onboard ships the ships personnel are notified by signs located throughout the ship that state that these premises are under video surveillance and cameras are in use.</p>
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	<p>Specify how:</p> <p>Human Resource HR information; HR is collected through the employee's application for employment and other requests such as COOP calling tree. The employee is fully informed of how the information will be utilized when collected. The employment application contains the Privacy Act notice. Applicants have the opportunity to decline to provide PII, in writing, to the HR representative or to their supervisors, but it might affect the overall processing of their employment. For hiring websites like the NOAA Corps (CPC applications) and Wage Mariner (WMHP) sites candidates are asked to provide PII. Applicants have the opportunity to decline however that will result in the candidate not being considered for the Federal position. OMAO employees may decline to provide PII information on performance evaluations.</p> <p>Health Insurance Portability and Accountability Act (HIPAA) information; Prior to aircraft and ship departures crew members and guests are required to sign waivers and releases. Crew and guests have the opportunity to decline providing this information however failure to do so may result in the crew member or guest not getting underway with the vessel or aircraft. 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.</p> <p>System Administration and audit information; Users (Privileged/Unprivileged Users) may decline to provide PII info on a DD- 2841 form; however, this will prevent them from receiving an Alt Token and that will prevent them from being HSPD-12 compliant.</p> <p>Crew manifest on the public science website. For the PII on the aircraft log/passenger manifest (passenger's name), the Pilot or Flight Director is required to give guest crew members the opportunity to decline to be reported on the pub website.</p>
---	---	--

		Video safety and security cameras; signs and plaques are posted notifying in areas with cameras allowing personnel to make the choice to enter those spaces prior to being recorded.
	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>Medical: 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 unless it is a medical emergency. This medical information is used only 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> <p>Crew Manifest: Crew manifests are a safety feature required by the USCG and FAA. Individuals are informed of this requirement and consent to this use by boarding a ship or aircraft. If an individual does not consent, s/he is not authorized to board a ship or aircraft.</p> <p>Video Safety &amp; Security Cameras: Signage is posted in all locations containing video cameras. All personnel are informed of the purpose to share the information in the event of a safety/security incident onboard a ship or aircraft. Boarding a ship or aircraft is consent to this use.</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>Healthcare information is updated as new injuries/illnesses 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 check-in 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 Enterprise Services via the web portal to update/review PII pertaining to them in accordance with their guidelines. Otherwise, during each evaluation period each employee will have an opportunity to</p>
---	---	---

		update their PII before signing their evaluation form.  Crew Manifests: Individuals are provided the opportunity to verify the accuracy of the information collected and request changes by notifying the aircraft Flight Director, Pilot, or ships OPS Officer.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Video/Safety Recordings: There is no opportunity to update the video images recorded for safety and security purposes.

### **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 the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): <u>September 25, 2020</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 moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC 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.  
*(Include data encryption in transit and/or at rest, if applicable).*

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). Databases utilize FIPS 140-2 compliant crypto packages provided by Oracle to encrypt the data. The package is called DBMS\_CRYPT0 (AES256, + CHAIN\_CBC, + PAD\_PKCS5. All HR sensitive data in motion utilize https/ssl and all external sites are BOD 18-01 compliant.

For Health Records information, the SQL database utilizes Transparent Data Encryption (TDE(AES256)), encrypts SQL Server, Azure SQL Database, and Azure Synapse Analytics (SQL Data Warehouse) data files. All healthcare sensitive data in motion utilize https/ssl and all external sites are BOD 18-01 compliant. NOAA2220 employs McAfee hard drive encryption for the laptops that OMAO medical staff uses to store employees PII. This encryption is FIPS 140-2 validated. Computers that are issued to the medical staff of the ships are on the OMAO domain. The users are required to log into the computer using a Common Access Card (CAC). •• The web server that stores the mission logs is open to the general public. All public science data websites that may inadvertently collect sensitive data utilize https/ssl and all external sites are BOD 18-01 compliant. The server itself is secured, scanned, and backed up on a regular basis. OMAO uses Kiteworks, external drives, and other DOD encrypted transfer methods to receive and send sensitive PII and BII.

**Section 9: Privacy Act**

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

X  Yes, the PII/BII is searchable by a personal identifier.

No, the PII/BII is not searchable by a personal identifier.

9.2 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, number, and link. <i>(list all that apply):</i> <a href="#">COMMERCE/NOAA-1, Applicants for the NOAA Corps</a> <a href="#">COMMERCE/NOAA-3, NOAA Corps Officer Official Personnel Folders</a> COMMERCE/DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons <a href="#">NOAA-10, NOAA Diving Program File</a> COMMERCE/DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons COMMERCE/DEPT-7, Employee Accident Records COMMERCE/DEPT-18, Employees Information Not Covered by Other Agencies <a href="#">COMMERCE/NOAA-22, NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSO)</a> OPM/GOVT-1, General Personnel Records OPM-2, Employees Performance File Records COMMERCE/ DEPT-29, Unmanned Aircraft Systems
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, this system is not a system of records and a SORN is not applicable.

**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.)*

<b>Disposal</b>			
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 Level**

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. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	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 HR information pertains to personnel and contains names, phone numbers, addresses, qualifications, medical status, payroll, and HR information. The HIPAA information pertains to medical records and all associated medical information.
X	Quantity of PII	Provide explanation: There are approximately 1000 personnel with HR information. There are approximately 900 personnel that are aboard ships and 100 aircrew members.
X	Data Field Sensitivity	Provide explanation: Sensitive data is entered in the system via forms and is stored in a secure manner, the data is only accessible to 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 cases released.
X	Obligation to Protect Confidentiality	Provide explanation: NOAA2220 is obligated under the Health Insurance Portability and Accountability Act (HIPAA) to protect the confidentiality of the PII it stores or transmits and it does so by encrypting data at rest and using access controls
X	Access to and Location of PII	Provide explanation: All PII and HIPAA information are only accessed by Supervisors and Medical staff (Executive Officer (XO) for emergencies) and only with the need to know. HR information is located within the IT Mission Enclave under the Corporate function. Medical information is located within the IT Mission Enclave under the Medical function.
	Other:	Provide explanation:

## **Section 12: Analysis**

- 12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

NOAA2220 collects the least amount of PII required to operate in order to lessen the potential threat of accidental loss of this information or unauthorized internal access. NOAA2220 follows the guidance set forth in NIST 800-53 controls for access control; audit and accountability; identification and authentication; media protection; planning; risk assessment; system and communications protection to ensure that the information is handled, retained, and disposed of appropriately. Further, NOAA2220 follows DOC and NOAA mandates as well as continual training for applicable personnel to ensure that the information is handled, retained, and disposed of appropriately.

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

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

12.3 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.