U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for
Permits and Registrations for NMFS Commercial and Recreational Fisheries and Protected Resources

Reviewed by: Sarah Brabson, Bureau Privacy Officer or Designee and Rob Swisher, Acting NOAA Privacy Officer

Approved by: _____, DOC Chief Privacy Officer

Date approved: _____

U.S. Department of Commerce Privacy Impact Assessment

NOAA/ Permits and Registrations for NMFS Commercial and Recreational Fisheries and Protected Resources

Unique Project Identifier: 006-48-01-14-02-3305-00

OMB Control No.	Title of Collection	NOAA Security System Number
0648-0013	Southeast Region Dealer Permit Family of Forms	NOAA4300
0648-0084	Basic Requirements for Special Exception Permits and Authorizations to Take, Import, and Export Marine Mammals and Endangered and Threatened Species and for Maintaining a Captive Marine Mammal Inventory Under the Marine Mammal Protection Act, the Fur Seal Act, and the Endangered Species Act	NOAA4500
0648-0151	Applications and Reporting Requirements for Small Take of Marine Mammals by Specified Activities Under the Marine Mammal Protection Act	NOAA4500
0648-0194	Antarctic Marine Living Resources Conservation and Management Measures	NOAA4020
0648-0202	Northeast Region Permit Family of Forms	NOAA4100
0648-0203	Northwest Region Permit Family of Forms (now part of West Coast Region)	NOAA4600
0648-0204	Southwest Region Permit Family of Forms (now part of West Coast Region)	NOAA4010
0648-0205	Southeast Region Permit Family of Forms	NOAA4300
0648-0206	Alaska Region Permit Family of Forms	NOAA4700
0648-0218	South Pacific Tuna Act Permit Applications	NOAA4010
0648-0229	Northeast Region Dealer Permit Family of Forms	NOAA4100
0648-0230	Permits for Incidental Taking of Endangered or Threatened Species	NOAA4500
0648-0272	Individual Fishing Quotas for Pacific Halibut and Sablefish in the Alaska Fisheries	NOAA4700
0648-0304	High Seas Fishing Permits	NOAA4010
0648-0309	Scientific Research, Exempted Fishing, and Exempted Activity Submissions	NOAA4500
0648-0316	Prohibited Species Donation Program	NOAA4700
0648-0327	Atlantic Highly Migratory Species Vessels Permits	NOAA4011
0648-0334	Alaska License Limitation Program for Groundfish, Crab, and Scallops	NOAA4700

0648-0345	Southeast Region Bycatch Reduction Device Certification Family of Forms	NOAA4300
0648-0387	International Dolphin Conservation Program	NOAA4010
0648-0393	American Fisheries Act: Vessel and Processor Permit Applications	NOAA4700
0648-0402	Application and Reports for Scientific Research and Enhancement Permits Under the Endangered Species Act	NOAA4500
0648-0463	Pacific Islands Region Coral Reef Ecosystems Permits	NOAA4010
0648-0471	Highly Migratory Species Scientific Research Permits, Exempted Fishing Permits, and Letters of Authorization	NOAA4011
0648-0490	Pacific Islands Region Permit Family of Forms	NOAA4010
0648-0495	Atlantic Highly Migratory Species Vessel Chartering Permits	NOAA4011
0648-0514	Alaska Region Bering Sea and Aleutian Islands Crab Permits	NOAA4700
0648-0545	Alaska Rockfish Pilot Program	NOAA4700
0648-0551	Southeast Region Gulf of Mexico Red Snapper Individual Fishing Quota Program	NOAA4300
0648-0565	Amendment 80 Permits and Reports	NOAA4700
0648-0569	Alaska Individual Fishing Quota Temporary Transfers	NOAA4700
0648-0577	Non-Commercial Permit and Reporting Requirements in the Main Hawaiian Islands Bottomfish Fishery	NOAA4010
0648-0578	National Saltwater Angler Registry and State Exemption Program	NOAA4020
0648-0586	Permitting, Vessel Identification, and Reporting Requirements for Deepwater Shrimp Fisheries in the Western Pacific Region	NOAA4010
0648-0589	Permitting, Vessel Identification and Reporting Requirements for the Pelagic Squid Jig Fishery in the Western Pacific Region	NOAA4010
0648-0595	Western and Central Pacific Fisheries Convention Vessel Information Family of Forms	NOAA4010
0648-0620	Pacific Coast Groundfish Trawl Rationalization Program Rule Permit and License Information Collection	NOAA4600
0648-0664	Permit and Reporting Requirements for Non-Commercial Fishing in the Rose Atoll, Marianas Trench and Pacific Remote Islands Marine National Monuments	NOAA4010
0648-0665	Alaska Community Quota Entity (CQE) Program	NOAA4700
0648-0673	American Lobster Limited Entry Program and an Individual Trap Transfer (ITTP) Program	NOAA4100
0648-0674	Atlantic Herring Amendment 5 Data Collection	NOAA4100

Introduction: System Description

In order to manage U.S. fisheries, the NOAA National Marine Fisheries Service (NMFS) requires the use of permits or registrations by participants in the United States. Applications for permits and registrations are collected from individuals under the authority of the Magnuson-Stevens Fishery Conservation and Management Act, the High Seas Fishing Compliance Act, the American Fisheries Act, the Tuna Conventions Act of 1950, the Atlantic Coastal Fisheries Cooperative Management Act, the Atlantic Tunas Convention Authorization Act, the Northern Pacific Halibut Act, the Antarctic Marine Living Resources Convention Act, the Western and Central Pacific Fisheries Convention Implementation Act (WCPFCIA; 16 U.S.C. 6901 et seq), international fisheries regulations regarding U.S. Vessels Fishing in Colombian Treaty Waters, the Marine Mammal Protection Act, the Endangered Species Act and the Fur Seal Act. The authority for the mandatory collection of the Tax Identification Number (Employer Identification Number or Social Security Number) is 31 U.S.C. 7701.

NMFS has established the National Permits System (NPS) to accept and maintain all Sustainable Fisheries permit applications and related data. All regional and other program systems are either housed within this system, with mirror sites available at the region/program sites (Southwest Region and Pacific Islands Region), are in the process of being linked with NPS or have, or are developing, parallel applications. Research permit application data is mainly housed within NOAA4500, the Seattle, WA Local Area Network.

Information in the systems consists of contents of permit applications and related documents such as permit transfers and percentage of ownership in a corporation. A typical transaction is an initial or renewal permit application: the permit holder or applicant completes an application downloaded from the applicable NMFS Web site or obtained through the NPS, submits it to the applicable office along with any required supporting documentation and/or required fee payment, and receives a new permit. For permit transfers within a family, marriage certificates, divorce decrees, and/or death certificates may be required.

NPS, as well as other permits applications in development or in use, provide the option of online submission of permit applications and related information, via secure Web pages.

Information Sharing:

Information is shared within NMFS offices, in order to coordinate monitoring and management of sustainability of fisheries and protected resources. Sources of information include the permit applicant/holder, other NMFS offices, the U.S. Coast Guard and State or Regional Marine Fisheries Commissions.

NMFS may post non-sensitive permit holder, vessel-related, and/or IFQ information for the public, via Web sites and Web Services, per notice given on permit applications.

The SORNs listed in Section 7 provide, where applicable, that the records may be shared under the following circumstances:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the Department of Commerce (Department). These records or information contained therein may specifically be disclosed as a routine use as stated below. The Department will, when so authorized, make the determination as to the relevancy of a record prior to its decision to disclose a document.

1. In the event that a system of records maintained by the Department to carry out its functions indicates a violation or potential violation of law or contract, whether civil, criminal or regulatory in nature and whether arising by general statute or particular program statute or contract, rule, regulation, or order issued pursuant thereto, or the necessity to protect an interest of the Department, the relevant records in the system of records may be referred to the appropriate agency, whether Federal, State, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute or contract, rule, regulation, or order issued pursuant thereto, or protecting the interest of the Department.

2. A record from this system of records may be disclosed in the course of presenting evidence to a court, magistrate, hearing officer or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations, administrative appeals and hearings.

3. A record in this system of records may be disclosed to a Member of Congress submitting a request involving an individual when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed to the Department of Justice in connection with determining whether the Freedom of Information Act (5 U.S.C. 552) requires disclosure thereof.

5. A record in this system will be disclosed to the Department of Treasury for the purpose of reporting and recouping delinquent debts owed the United States pursuant to the Debt Collection Improvement Act of 1996.

6. A record in this system may be disclosed to the Department of Homeland Security for the purposes of determining the admissibility of certain seafood imports into the United States (NOAA-19) or for the purposes of determining the admissibility of certain marine mammal or threatened or endangered species or species parts imports into the United States (NOAA-12).

.

7. A record in this system of records may be disclosed to a contractor of the Department *(in actuality, NOAA only)* having need for the information in the performance of the contract but not operating a system of records within the meaning of 5 U.S.C. 552a(m).

(#s 8-11 apply only to NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries)

8. A record in this system of records may be disclosed to approved persons at the state or interstate level within the applicable Marine Fisheries Commission for the purpose of co-managing a fishery or for making determinations about eligibility for permits when state data are all or part of the basis for the permits.

9. A record in this system of records may be disclosed to the applicable Fishery Management Council (Council) staff and contractors tasked with the development of analyses to support Council decisions about Fishery Management Programs.

10. A record in this system of records may be disclosed to the applicable NMFS Observer Program for purposes of identifying current permit owners and vessels and making a random assignment of observers to vessels in a given fishing season.

11. A record in this system of records may be disclosed to the applicable regional or international fisheries management body for the purposes of identifying current permit owners and vessels pursuant to applicable statutes or regulations and/or conservation and management measures adopted by a regional or international fisheries management body, such as: the Food and Agriculture Organization of the United Nations, Commission for the Conservation of Antarctic Marine Living Resources, Inter-American Tropical Tuna Commission, International Pacific Halibut Commission, and International Commission for the Conservation of Atlantic Tunas.

12. Disclosure to appropriate agencies, entities, and persons when (1) it is suspected or determined that the security or confidentiality of information in the system of records has been compromised; (2) it is determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identify theft or fraud, or harm to the security or integrity of this system or other systems or programs that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

All systems in this PIA are moderate impact, except for NOAA4700, which has a POA&M to become a moderate system, to be completed 1/1/2015.

Section 1: Information in the System

1.1 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*	x	e. Alien Registration		i. Financial Account	x

b. Taxpayer ID	x	f. Driver's License		j. Financial Transaction	x
c. Employee ID	x	g. Passport		k. Vehicle Identifier	
d. File/Case ID	x	h. Credit Card		l. Employer ID Number	x
m. Other identifying numbers (specify): Captain's license, State and Federal Dealer Numbers (if applicable), permit or license numbers for Federal or state permit/licenses issued and start and end dates and other permit status codes, vessel registration number					

*If no Employer ID Number, required for Individual Fishing Quota holders, to ensure correct identification for cost recovery payment to NMFS. Also, as stated in both SORNs' routine uses, a Tax Identification Number (EIN or SSN) is required on all permit applications other than research or exempted fishing permits, under the authority 31 U.S.C. 7701. For purposes of administering the various NMFS fisheries permit and registration programs, a person shall be considered to be doing business with a Federal agency including but not limited to if the person is an applicant for, or recipient of, a Federal license, permit, right-of-way, grant, or benefit payment administered by the agency or insurance administered by the agency pursuant to subsection (c) (2) (B) of this statute.

General Personal Data (GPD)					
a. Name	x*	g. Date of Birth	x	m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	x
c. Alias		i. Home Address	x	o. Medical Information	x
d. Gender		j. Telephone Number	x	p. Military Service	
e. Age	x	k. Email Address	x	q. Physical Characteristics	x
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): *Permit applicant, permit holder, permit transferor/transferee, vessel owner, vessel operator, dealer applicant, dealer permit holder, marriage certificate, divorce decree, death certificate.					

Work-Related Data (WRD)					
a. Occupation	x	d. Telephone Number	x	g. Salary	
b. Job Title	x	e. Email Address	x	h. Work History	x
c. Work Address	x	f. Business Associates	x		
Other work-related data (specify): Vessel name, vessel length overall. Name of corporation, state and date of incorporation of business and articles of incorporation.					

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): Height, weight, hair and eye color, medical records for permit disputes					

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

Other Non-sensitive Information (specify): Species, aggregate catch data and statistics, quota share balance, quota pound balance, quota pound limits, listings of endorsements and designations (i.e., gear endorsement, size endorsement, sector endorsement, permit tier) associated with the permit, name of physical IFQ landing site, Exemptions (i.e., Owner on Board - Grandfathered Exemption, Owner on Board, as stated in code of federal regulations) and exemption status, contact persons.
Other Sensitive Information (specify): Catch/Observer Discard Data, Quota Share/Quota Pound Transfer Data, Business Operation Information (Business Processes, Procedures, Physical Maps)

1.2 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	x
Telephone	x	Email	x		
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	x
State, Local, Tribal		Foreign			
Other (specify): Other federal agencies: U.S. Coast Guard vessel registration data.					

Non-government Sources					
Public Organizations		Public Media, Internet		Private Sector	x*
Commercial Data Brokers					
Other (specify): *State or Regional Marine Fisheries Commission's Data					

Section 2: Purpose of the System

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

Purpose			
To determine eligibility	x	For administering human resources programs	
For administrative matters	x	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	x
For civil enforcement activities	x	For intelligence activities	
Other (specify):			

Section 3: Use of the System

3.1 Provide an explanation of how the bureau will use the PII/BII to accomplish the checked purpose(s), e.g., to verify existing data. Describe why the PII/BII that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and further the mission of the bureau and/or the Department. Indicate if the PII/BII identified in

Section 1.1 of this document is in reference to a federal employee/contractor, member of public, foreign national, visitor or other (specify).

This information will allow NMFS to identify owners and holders of permits and non-permit registrations and vessel owners and operators for both civil and criminal enforcement activities, evaluate permit applications, and document agency actions relating to the issuance, renewal, transfer, revocation, suspension or modification of a permit or registration. NMFS may use lists of permit holders or registrants as sample frames for the conduct of surveys to collect information necessary to the administration of the applicable statutes. NMFS may post non-sensitive permit holder, vessel-related, and/or IFQ information for the public, via Web sites and Web Services, per notice given on permit applications. Tax Identification Numbers (EIN, SSN) allow positive identification for cost recovery billing of IFQ holders. All PII/BII are in reference to members of the public.

Section 4: Information Sharing

4.1 Indicate with whom the bureau intends to share the PII/BII in the system and how the PII/BII will be shared.

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

Section 5: Notice and Consent

5.1 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 6.	
x	Yes, notice is provided by other means.	Specify how: Notice is provided on the permit or related application.
	No, notice is not provided.	Specify why not:

5.2 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.	Specify how: The personal information is collected when the individual completes the appropriate application. On the application, the individual is advised that NMFS will not be able to issue a permit if the individual does not provide each item of information requested. The individual may choose to decline to provide the required personal information at that time, but will not be able to receive a permit.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

5.3 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.	Specify how: The individual may choose to decline consent to the particular use of his/her personal information (for permit application) when completing the application; however, he will not receive a permit.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

5.4 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.	Specify how: Information may be reviewed/updated when completing or renewing a permit application or supporting document, or by calling or emailing the applicable NMFS office at any time. Permits are completed on line, or in the case of paper applications, by reviewing and updating the application pre-filled by NMFS permit office staff with their most recent information on the permit holder.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 6: Administrative and Technological Controls

6.1 Indicate the administrative and technological controls for the system. Check all that apply.

x	All users signed a confidentiality agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff received training on privacy and confidentiality policies and practices.
x	Access to PII/BII is restricted to authorized personnel only.
x	The information is secured in accordance with FISMA requirements. Provide dates of most recent

	Assessment and Authorization: NOAA4010: 7/1/2014 NOAA4011: 8/6/2014 NOAA4020: 3/19/2014 NOAA4100: 3/18/2014 NOAA4300: 8/14/2014 NOAA4500: 4/23/2014 NOAA4600: 4/23/2014 NOAA4700: 3/28/2014
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher ***
x	NIST 800-122 recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM). See Appendix A.
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Other (specify):

*** One system, NOAA4700, has a low impact category, but the moderate level controls are in place, with tailoring per FIPS 200. An upgrade to moderate is expected to be completed 1/1/2015 (see Appendix A for NOAA4700).

Section 7: Privacy Act

7.1 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, these systems are covered by an existing system of records notice. Provide the system name and number: COMMERCE/NOAA #19, Permits and Registrations for United States Federally Regulated Fisheries COMMERCE/NOAA #12, Marine Mammals, Endangered and Threatened Species, Permits and Exempted Applicants
x	Yes, UPDATED system of records notices were submitted to the Department for approval on May 30, 2013 for NOAA #19 and #12.
	No, a system of records is not being created.

Section 8: Retention of Information

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

x	There are approved record control schedules for both Sustainable Fisheries and Marine Mammal Protection permits. Provide the names of the record control schedules: NOAA 1504-11; NOAA 1514-01.
	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:

Appendix A for NOAA4010, NMFS Headquarters Local Area Network

In the first column, please complete as "in place", "POAM ID # ____", "NA" or "RA (Risk Accepted)

In Place	**Access Enforcement (AC-3)**. Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists).
In Place	**Separation of Duties (AC-5).** Organizations can enforce separation of duties for duties involving access to PII.
In Place	**Least Privilege (AC-6).** Organizations can enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.
In Place	**Remote Access (AC-17).** Organizations can choose to prohibit or strictly limit remote access to PII.
In Place	**User-Based Collaboration and Information Sharing (AC-21).** Organizations can provide automated mechanisms to assist users in determining whether access authorizations match access restrictions, such as contractually-based restrictions, for PII.
In Place	**Access Control for Mobile Devices (AC-19).** Organizations can choose to prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).
In Place	**Auditable Events (AU-2).** Organizations can monitor events that affect the confidentiality of PII, such as unauthorized access to PII.
In Place	**Audit Review, Analysis, and Reporting (AU-6)**. Organizations can regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.
In Place	**Identification and Authentication (Organizational Users) (IA-2).** Users can be uniquely identified and authenticated before accessing PII.
In Place	**Media Access (MP-2).** Organizations can restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm).
In Place	**Media Marking (MP-3).** Organizations can label information system media and output containing PII to indicate how it should be distributed and handled.
In Place	**Media Storage (MP-4).** Organizations can securely store PII, both in paper and digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
In Place	**Media Transport (MP-5).** Organizations can protect digital and non-digital media and mobile devices containing PII that is transported outside the organization's controlled areas.
In Place	**Media Sanitization (MP-6).** Organizations can sanitize digital and non-digital media containing PII before it is disposed or released for reuse.
In Place	**Transmission Confidentiality (SC-9).** Organizations can protect the confidentiality of transmitted PII.
In Place	**Protection of Information at Rest (SC-28).** Organizations can protect the confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape.
In Place	**Information System Monitoring (SI-4).** Organizations can employ automated tools to monitor PII internally or at network boundaries for unusual or suspicious transfers or events.

This page is a supplement for Section 6, Technological Controls. Upon final approval, this page must be removed prior to publication of the PIA.

Appendix A for NOAA4011, National Fishing Permit and Landings Reporting System

In the first column, please complete as "in place", "POAM ID # ____", "NA" or "RA (Risk Accepted)

In Place	**Access Enforcement (AC-3)**. Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists).
NA*	**Separation of Duties (AC-5).** Organizations can enforce separation of duties for duties involving access to PII.
In Place**	**Least Privilege (AC-6).** Organizations can enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.
In Place	**Remote Access (AC-17).** Organizations can choose to prohibit or strictly limit remote access to PII.
NA	**User-Based Collaboration and Information Sharing (AC-21).** Organizations can provide automated mechanisms to assist users in determining whether access authorizations match access restrictions, such as contractually-based restrictions, for PII.
In Place	**Access Control for Mobile Devices (AC-19).** Organizations can choose to prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).
In Place	**Auditable Events (AU-2).** Organizations can monitor events that affect the confidentiality of PII, such as unauthorized access to PII.
In Place	**Audit Review, Analysis, and Reporting (AU-6)**. Organizations can regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.
In Place	**Identification and Authentication (Organizational Users) (IA-2).** Users can be uniquely identified and authenticated before accessing PII.
In Place	**Media Access (MP-2).** Organizations can restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm).
NA***	**Media Marking (MP-3).** Organizations can label information system media and output containing PII to indicate how it should be distributed and handled.
NA***	**Media Storage (MP-4).** Organizations can securely store PII, both in paper and digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
NA***	**Media Transport (MP-5).** Organizations can protect digital and non-digital media and mobile devices containing PII that is transported outside the organization's controlled areas.
In Place	**Media Sanitization (MP-6).** Organizations can sanitize digital and non-digital media containing PII before it is disposed or released for reuse.
In Place	**Transmission Confidentiality (SC-9).** Organizations can protect the confidentiality of transmitted PII.
In Place	**Protection of Information at Rest (SC-28).** Organizations can protect the confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape.
NA****	**Information System Monitoring (SI-4).** Organizations can employ automated tools to monitor PII internally or at network boundaries for unusual or suspicious transfers or events.

***** This is in place on the application. However, the system administration and database management functions are performed by one individual. We will be drafting a FIPS200 to seek risk acceptance; *this document should be approved by 1/31/2015.*

**Revised to “in place”: Customer PII is only accessible only to team members that require access to perform their job functions.

*** NOAA4011 does not utilize external media in its operations.

**** NOAA4011 monitors for external access to PII. However, the current application does not have the capability to monitor internal user that access PPI. As a compensation control, access to PII is restricted to only team members that require it.

This page is a supplement for Section 6, Technological Controls. Upon final approval, this page must be removed prior to publication of the PIA.

Appendix A for NOAA4020, Headquarters, Silver Spring Shark

In the first column, please complete as "in place", "POAM ID # ____", "NA" or "RA (Risk Accepted)

In Place	**Access Enforcement (AC-3)**. Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists).
In Place	**Separation of Duties (AC-5).** Organizations can enforce separation of duties for duties involving access to PII.
In Place	**Least Privilege (AC-6).** Organizations can enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.
In Place	**Remote Access (AC-17).** Organizations can choose to prohibit or strictly limit remote access to PII.
In Place	**User-Based Collaboration and Information Sharing (AC-21).** Organizations can provide automated mechanisms to assist users in determining whether access authorizations match access restrictions, such as contractually-based restrictions, for PII.
In Place	**Access Control for Mobile Devices (AC-19).** Organizations can choose to prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).
In Place	**Auditable Events (AU-2).** Organizations can monitor events that affect the confidentiality of PII, such as unauthorized access to PII.
In Place	**Audit Review, Analysis, and Reporting (AU-6)**. Organizations can regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.
In Place	**Identification and Authentication (Organizational Users) (IA-2).** Users can be uniquely identified and authenticated before accessing PII.
In Place	**Media Access (MP-2).** Organizations can restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm).
In Place	**Media Marking (MP-3).** Organizations can label information system media and output containing PII to indicate how it should be distributed and handled.
In Place	**Media Storage (MP-4).** Organizations can securely store PII, both in paper and digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
In Place	**Media Transport (MP-5).** Organizations can protect digital and non-digital media and mobile devices containing PII that is transported outside the organization's controlled areas.
In Place	**Media Sanitization (MP-6).** Organizations can sanitize digital and non-digital media containing PII before it is disposed or released for reuse.
In Place	**Transmission Confidentiality (SC-9).** Organizations can protect the confidentiality of transmitted PII.
In Place	**Protection of Information at Rest (SC-28).** Organizations can protect the confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape.
In Place	**Information System Monitoring (SI-4).** Organizations can employ automated tools to monitor PII internally or at network boundaries for unusual or suspicious transfers or events.

This page is a supplement for Section 6, Technological Controls. Upon final approval, this page must be removed prior to publication of the PIA.

Appendix A for NOAA4100, NMFS Gloucester, MA Local Area Network

In the first column, please complete as "in place," "POAM ID # ____," "N/A," or "RA (Risk Accepted."

In Place	**Access Enforcement (AC-3)**. Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists).
In Place	**Separation of Duties (AC-5).** Organizations can enforce separation of duties for duties involving access to PII.
In Place	**Least Privilege (AC-6).** Organizations can enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.
In Place	**Remote Access (AC-17).** Organizations can choose to prohibit or strictly limit remote access to PII.
N/A	**User-Based Collaboration and Information Sharing (AC-21).** Organizations can provide automated mechanisms to assist users in determining whether access authorizations match access restrictions, such as contractually-based restrictions, for PII.
In Place	**Access Control for Mobile Devices (AC-19).** Organizations can choose to prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).
In Place	**Auditable Events (AU-2).** Organizations can monitor events that affect the confidentiality of PII, such as unauthorized access to PII.
In Place	**Audit Review, Analysis, and Reporting (AU-6)**. Organizations can regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.
In Place	**Identification and Authentication (Organizational Users) (IA-2).** Users can be uniquely identified and authenticated before accessing PII.
In Place	**Media Access (MP-2).** Organizations can restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm).
In Place	**Media Marking (MP-3).** Organizations can label information system media and output containing PII to indicate how it should be distributed and handled.
In Place	**Media Storage (MP-4).** Organizations can securely store PII, both in paper and digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
In Place	**Media Transport (MP-5).** Organizations can protect digital and non-digital media and mobile devices containing PII that is transported outside the organization's controlled areas.
In Place	**Media Sanitization (MP-6).** Organizations can sanitize digital and non-digital media containing PII before it is disposed or released for reuse.
In Place	**Transmission Confidentiality (SC-9).** Organizations can protect the confidentiality of transmitted PII.
In Place	**Protection of Information at Rest (SC-28).** Organizations can protect the confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape.
In Place	**Information System Monitoring (SI-4).** Organizations can employ automated tools to monitor PII internally or at network boundaries for unusual or suspicious transfers or events.

This page is a supplement for Section 6, Technological Controls. Upon final approval, this page must be removed prior to publication of the PIA.

Appendix A for NOAA4300, NMFS St. Petersburg FL Local Area Network

In the first column, please complete as "in place", "POAM ID # ____", "NA" or "RA (Risk Accepted)

In Place	**Access Enforcement (AC-3)**. Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists).
In Place	**Separation of Duties (AC-5).** Organizations can enforce separation of duties for duties involving access to PII.
In Place	**Least Privilege (AC-6).** Organizations can enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.
In Place	**Remote Access (AC-17).** Organizations can choose to prohibit or strictly limit remote access to PII.
In Place	**User-Based Collaboration and Information Sharing (AC-21).** Organizations can provide automated mechanisms to assist users in determining whether access authorizations match access restrictions, such as contractually-based restrictions, for PII.
In Place	**Access Control for Mobile Devices (AC-19).** Organizations can choose to prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).
In Place	**Auditable Events (AU-2).** Organizations can monitor events that affect the confidentiality of PII, such as unauthorized access to PII.
In Place	**Audit Review, Analysis, and Reporting (AU-6)**. Organizations can regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.
In Place	**Identification and Authentication (Organizational Users) (IA-2).** Users can be uniquely identified and authenticated before accessing PII.
In Place	**Media Access (MP-2).** Organizations can restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm).
In Place	**Media Marking (MP-3).** Organizations can label information system media and output containing PII to indicate how it should be distributed and handled.
In Place	**Media Storage (MP-4).** Organizations can securely store PII, both in paper and digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
In Place	**Media Transport (MP-5).** Organizations can protect digital and non-digital media and mobile devices containing PII that is transported outside the organization's controlled areas.
In Place	**Media Sanitization (MP-6).** Organizations can sanitize digital and non-digital media containing PII before it is disposed or released for reuse.
In Place	**Transmission Confidentiality (SC-9).** Organizations can protect the confidentiality of transmitted PII.
In Place	**Protection of Information at Rest (SC-28).** Organizations can protect the confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape.
In Place	**Information System Monitoring (SI-4).** Organizations can employ automated tools to monitor PII internally or at network boundaries for unusual or suspicious transfers or events.

This page is a supplement for Section 6, Technological Controls. Upon final approval, this page must be removed prior to publication of the PIA.

Appendix A for NOAA4500, NMFS Seattle WA Local Area Network

In the first column, please complete as "in place," "POAM ID # ____," "N/A," or "RA (Risk Accepted."

In place	**Access Enforcement (AC-3)**. Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists).
In place	**Separation of Duties (AC-5).** Organizations can enforce separation of duties for duties involving access to PII.
In place	**Least Privilege (AC-6).** Organizations can enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.
In place	**Remote Access (AC-17).** Organizations can choose to prohibit or strictly limit remote access to PII.
In place	**User-Based Collaboration and Information Sharing (AC-21).** Organizations can provide automated mechanisms to assist users in determining whether access authorizations match access restrictions, such as contractually-based restrictions, for PII.
In place	**Access Control for Mobile Devices (AC-19).** Organizations can choose to prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).
In place	**Auditable Events (AU-2).** Organizations can monitor events that affect the confidentiality of PII, such as unauthorized access to PII.
In place	**Audit Review, Analysis, and Reporting (AU-6)**. Organizations can regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.
In place	**Identification and Authentication (Organizational Users) (IA-2).** Users can be uniquely identified and authenticated before accessing PII.
In place	**Media Access (MP-2).** Organizations can restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm).
In place	**Media Marking (MP-3).** Organizations can label information system media and output containing PII to indicate how it should be distributed and handled.
In place	**Media Storage (MP-4).** Organizations can securely store PII, both in paper and digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
In place	**Media Transport (MP-5).** Organizations can protect digital and non-digital media and mobile devices containing PII that is transported outside the organization's controlled areas.
In place	**Media Sanitization (MP-6).** Organizations can sanitize digital and non-digital media containing PII before it is disposed or released for reuse.
In place	**Transmission Confidentiality (SC-9).** Organizations can protect the confidentiality of transmitted PII.
In place	**Protection of Information at Rest (SC-28).** Organizations can protect the confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape.
In place	**Information System Monitoring (SI-4).** Organizations can employ automated tools to monitor PII internally or at network boundaries for unusual or suspicious transfers or events.

This page is a supplement for Section 6, Technological Controls. Upon final approval, this page must be removed prior to publication of the PIA.

Appendix A for NOAA4600, NMFS Seattle WA Local Area Network

In the first column, please complete as "in place", "POAM ID # ____", "NA" or "RA (Risk Accepted)

In Place	**Access Enforcement (AC-3)**. Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists).
In Place	**Separation of Duties (AC-5).** Organizations can enforce separation of duties for duties involving access to PII.
In Place	**Least Privilege (AC-6).** Organizations can enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.
In Place	**Remote Access (AC-17).** Organizations can choose to prohibit or strictly limit remote access to PII.
In Place	**User-Based Collaboration and Information Sharing (AC-21).** Organizations can provide automated mechanisms to assist users in determining whether access authorizations match access restrictions, such as contractually-based restrictions, for PII.
In Place	**Access Control for Mobile Devices (AC-19).** Organizations can choose to prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).
In Place	**Auditable Events (AU-2).** Organizations can monitor events that affect the confidentiality of PII, such as unauthorized access to PII.
In Place	**Audit Review, Analysis, and Reporting (AU-6)**. Organizations can regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.
In Place	**Identification and Authentication (Organizational Users) (IA-2).** Users can be uniquely identified and authenticated before accessing PII.
In Place	**Media Access (MP-2).** Organizations can restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm).
In Place	**Media Marking (MP-3).** Organizations can label information system media and output containing PII to indicate how it should be distributed and handled.
In Place	**Media Storage (MP-4).** Organizations can securely store PII, both in paper and digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
In place	**Media Transport (MP-5).** Organizations can protect digital and non-digital media and mobile devices containing PII that is transported outside the organization's controlled areas.
In Place	**Media Sanitization (MP-6).** Organizations can sanitize digital and non-digital media containing PII before it is disposed or released for reuse.
In Place	**Transmission Confidentiality (SC-9).** Organizations can protect the confidentiality of transmitted PII.
In Place	**Protection of Information at Rest (SC-28).** Organizations can protect the confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape.
In Place	**Information System Monitoring (SI-4).** Organizations can employ automated tools to monitor PII internally or at network boundaries for unusual or suspicious transfers

	or events.

This page is a supplement for Section 6, Technological Controls. Upon final approval, this page must be removed prior to publication of the PIA.

Appendix A for NOAA4700, NMFS Juneau AK Local Area Network

POA&M for upgrade to moderate level, per FIPS 199 assessment: #60583. Completion expected 1/1/2015. *But currently, all controls below are in place.*

In the first column, please complete as "in place", "POAM ID # ____", "NA" or "RA (Risk Accepted)

In Place	**Access Enforcement (AC-3)**. Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists).
In Place	**Separation of Duties (AC-5).** Organizations can enforce separation of duties for duties involving access to PII.
In Place	**Least Privilege (AC-6).** Organizations can enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.
In Place	**Remote Access (AC-17).** Organizations can choose to prohibit or strictly limit remote access to PII.
In Place	**User-Based Collaboration and Information Sharing (AC-21).** Organizations can provide automated mechanisms to assist users in determining whether access authorizations match access restrictions, such as contractually-based restrictions, for PII.
In Place	**Access Control for Mobile Devices (AC-19).** Organizations can choose to prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).
In Place	**Auditable Events (AU-2).** Organizations can monitor events that affect the confidentiality of PII, such as unauthorized access to PII.
In Place	**Audit Review, Analysis, and Reporting (AU-6)**. Organizations can regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.
In Place	**Identification and Authentication (Organizational Users) (IA-2).** Users can be uniquely identified and authenticated before accessing PII.
In Place	**Media Access (MP-2).** Organizations can restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm).
Partially*	**Media Marking (MP-3).** Organizations can label information system media and output containing PII to indicate how it should be distributed and handled.
In Place	**Media Storage (MP-4).** Organizations can securely store PII, both in paper and digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
In Place	**Media Transport (MP-5).** Organizations can protect digital and non-digital media and mobile devices containing PII that is transported outside the organization's controlled areas.
In Place	**Media Sanitization (MP-6).** Organizations can sanitize digital and non-digital media containing PII before it is disposed or released for reuse.
In Place	**Transmission Confidentiality (SC-9).** Organizations can protect the confidentiality of transmitted PII.
In Place	**Protection of Information at Rest (SC-28).** Organizations can protect the confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape.
In Place	**Information System Monitoring (SI-4).** Organizations can employ automated tools to monitor

	PII internally or at network boundaries for unusual or suspicious transfers or events.

*****NOAA4700 Rules of Behavior prohibit the transfer of PII or sensitive material to removable media this negates the need for media labeling of removable devices. NOAA4700 Media and Physical Protection Policy requires any Hard Disk Drive to be destroyed by proper methods prior to being disposed of or transferred outside of an AKR controlled environment. NOAA4700 Media and Physical Protection also mandates that any HDD used on a device containing PII be labelled and only used on devices containing PII if they are going to be reused.

NOAA4700 reports server creates a warning banner that transfers to the display or printed version of any reports containing PII from the Oracle Database.

This page is a supplement for Section 6. Upon final approval, this page must be removed prior to publication of the PIA.