

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



**Privacy Impact Assessment**  
**for the**  
**Southeast Regional Office Local Area Network**  
**(NOAA4300)**

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: 2020.10.05 15:32:13 -04'00'

09/01/2020

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

Date

**U.S. Department of Commerce Privacy Impact Assessment**  
**National Marine Fisheries Service**  
**NOAA4300 – Southeast Regional Office Local Area Network (SERO)**

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

**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.*

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

NOAA4300 is a general Support System. It supports all offices within the Southeast Region (SER) which include the Regional Administrator's Office; Operations, Management & Information Services Office; State/Federal Liaison Office; Sustainable Fisheries Division; Protected Resources Division; and, Habitat Conservation Division.

The system also supports non-SERO offices located in St. Petersburg including NOAA SE Office of General Counsel (GCSE), Damage Assessment Center (DAC), and NMFS SE Financial Services. The information for these Non-SERO offices is covered by the NOAA4020 Privacy Impact Assessment.

*(b) System location*

NOAA4300 is physically housed in a leased portion of a three story building located within the city limits of Saint Petersburg, Florida. The building is 85% occupied by NOAA and NMFS offices. The network servers, web servers, and network management workstations are located in a secure room on the second floor.

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

NOAA4300 has an interconnection with NOAA4000 (NMFS WAN) for the following purposes:

- NMFS to NMFS network access
- Core backbone network services with Internet connectivity (TICAP)
- Enterprise Active Directory
- Tier 1,2, and 3 technical support
- Coordination of IP address (DNS)
- Real-time network monitoring
- VMS Data for purposes of Catch Shares (IFQ) program and Permits Management System (PIMS)

Upon verification of FIPS199 Moderate system compliance (or SP-171 equivalent), and the sharing of sensitive data has been authorized, a direct connection to ACCSP will be created, with a new Interconnection Agreement between NOAA4300 and ACCSP being created and signed. Starting September 1, 2020, in order to comply with modifications to both the Gulf of Mexico Charter Vessel and Headboat Reporting Requirement Rule

(<https://www.fisheries.noaa.gov/action/gulf-mexico-modifications-charter-vessel-and-headboat-reporting-requirements>) and the South Atlantic Charter Vessel and Headboat Reporting Requirement Rule (<https://www.fisheries.noaa.gov/action/south-atlantic-modifications-charter-vessel-and-headboat-reporting-requirements>), NOAA4300 will be required to share permit holders' date of birth (DOB) and email addresses with ACCSP, **once ACCSP can provide documentation verifying a successful Assessment and Independent Validation and Verification of compliance with all applicable security policies, controls, and requirements of a FIPS199 Moderate (or equivalent) system.** The following timelines are based upon ACCSP's providing proof of compliance (third-party audit/SAR, control queries and artifacts, SSP, etc.) to NOAA4300, and are currently tentative at best. Once compliance is achieved, ACCSP will be required to provide annual verification of Continuous Monitoring methodology practices and current FIPS199 compliance through third party audit results prior to the renewal of any system interconnect or data sharing agreements.

- By June 1<sup>st</sup>, 2020, NOAA4300 plans to begin sharing permit holders' Date of Birth (DOB) with ACCSP.
- By June 30<sup>th</sup>, 2020, NOAA4300 plans to begin sharing electronic logbook and landing data with ACCSP.
- By September 30<sup>th</sup>, 2020, NOAA4300 plans to begin sharing Vessel Monitoring System (VMS) positional data with ACCSP in order to comply with pending regulations.
- By December 30<sup>th</sup>, 2020, in order to comply with pending regulations, NOAA4300 plans to share all for hire permit holder data with ACCSP.

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

NOAA4300 collects and stores information that consists of basic identifying information about employees, contractors, volunteers, and partner agency staff who are facility occupants or system users. The information is maintained as a supplement to other records for purposes of human resource activities (including managing security clearances), Continuity of Operations (COOP) execution, and performing other related administrative tasks, e.g., travel, awards, facility management, and staff training requirements in support of individual job duties and requirements. Information collected to manage security clearances may include: full name, home address, home phone number, e-mail address, educational background, Social Security Number (SSN), and employment history. Information maintained for COOP and other administrative processes includes: full name, grade level and/or position within the organization, role/responsibility, home address, home phone number, and mobile phone number.

NOAA4300 also collects and stores permit-related data. In order to manage U.S. fisheries, the NMFS requires the use of permits or registrations by participants in the United States. The information collected by NMFS SERO includes the contents of permit applications and supporting artifacts. Typical transactions include initial or renewal permit applications. The permit holder or applicant completes a blank application downloaded from the applicable NMFS Web site, received in the mail, or obtained through visiting the Permits office, and submits it to the applicable office via online, or in person, including any required supporting documentation and proof of payment through pay.gov. Approved permits are mailed to applicants. For permit transfers within a family, marriage certificates, divorce decrees, and/or death certificates may be required. Tax Identification Numbers (TINs) allow positive identification and cost recovery billing of Individual Fishing Quota (IFQ) holders.

In addition, information is collected to facilitate public education, outreach, or collaboration with partners on research/conservation projects. For these activities, the name, address, e-mail address, telephone number, and other non-sensitive organizational information may be temporarily stored. These individuals, businesses or organizations may be workshop participants, business contacts, members of mailing lists, etc. In all cases the information is voluntarily submitted.

NOAA4300 employs contractors in a variety of roles in order to support its mission, primarily in the Habitat/Sustainable Fisheries/Protected Resources branches. All contractors undergo the same security clearance process as Federal Government employees. Access to information collected and maintained within the system boundary of NOAA4300 is determined by the individual's job duties and role within the organization. Any request involving the sharing of sensitive data, whether internal or external, must be documented in a Memorandum of Understanding (MoU) or Interconnection Security Agreement (ISA), and approved by each system's Authorizing Official. Information is shared within the Southeast Region 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 (Such as the Office of General Counsel and the Southeast Division of the NMFS Office of Law Enforcement), the U.S. Coast Guard and the Department of Justice. Information will also be shared at the state or interstate level for the purpose of determining an applicant's eligibility when data collected by the state affects permit eligibility.

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

Employees can contact the HR representative for NOAA4300 and review their information, or a personal contact information form can be completed and given to HR, who will then update the information accordingly.

Permits: 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.

Partners for public outreach and education may update their information at any time by contacting the appropriate staff member assigned as their coordinator.

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

Information is manually collected through mail, over the telephone, in person, email, fax, and online.

Information is currently transmitted to and from the system through a network connection internal to the NMFS WAN employing Virtual Private Network encryption (TCP/IP using TLS) to secure the data.

Once ACCSP has achieved FIPS199 (or equivalent) compliance, and direct data sharing has been approved and established, data will be sent via encrypted connection to ACCSP (using AES-256 Encryption over a dedicated connection). Once transferred, authorized SER staff can access the data through the SAFIS web interface, which uses HTTPS to secure the connection.

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

NOAA4300 uses the interconnection with NOAA4000 to share permit related data with NOAA4400 (SEFSC) in Miami, and NOAA4011(NFPLRS).

OLE (NOAA4000) accesses the Permits Information Management System (PIMS) for Fishery Management/Law Enforcement purposes.

NOAA4300 currently leverages its existing Interconnection Agreement with SEFSC to share non-sensitive data with the Atlantic Coastal Cooperative Statistics Program (ACCSP). NOAA4300 sends the IDENT field data to SEFSC,

who then sends it to ACCSP via an encrypted connection. SEFSC currently has an Interconnect Agreement in place with ACCSP. The Interconnect between SEFSC and NOAA4300 is reviewed annually. ACCSP requires a unique identifier for each for-hire SER Permit holder in order to validate landing reports. In order to comply with regulations while not disclosing sensitive data, ACCSP provided an algorithm to NMFS, who runs the algorithm for each applicable permit holder to generate the identifier, and then shares the encrypted identifier with ACCSP. Although the identifier is comprised of fragmentary PII (birthdate, email address, and phone number), there is no exploitable data contained in the generated identifier.

Once ACCSP has become compliant with Federal requirements and the sharing of sensitive data has been authorized, a direct connection to ACCSP will be created, with a new Interconnection Agreement between NOAA4300 and ACCSP. Starting September 1, 2020, in order to comply with modifications to both the Gulf of Mexico Charter Vessel and Headboat Reporting Requirement Rule (<https://www.fisheries.noaa.gov/action/gulf-mexico-modifications-charter-vessel-and-headboat-reporting-requirements>) and the South Atlantic Charter Vessel and Headboat Reporting Requirement Rule (<https://www.fisheries.noaa.gov/action/south-atlantic-modifications-charter-vessel-and-headboat-reporting-requirements>), NOAA4300 will be required to share permit holders' date of birth (DOB) and email addresses with ACCSP, **once ACCSP can provide documentation verifying a successful Assessment and Independent Validation and Verification of compliance with all applicable security policies, controls, and requirements of a FIPS199 Moderate (or equivalent) system.** The following timelines are based upon ACCSP's providing proof of compliance (third-party audit/SAR, control queries and artifacts, SSP, etc.) to NOAA4300, and are currently tentative at best. Once compliance is achieved, ACCSP will be required to provide annual verification of Continuous Monitoring methodology practices and current FIPS199 compliance through third party audit results prior to the renewal of any system interconnect or data sharing agreements. As a non-federal system receiving sensitive federal data (and federal funding for that purpose), the system in question is required to possess a security categorization equal to (FIPS) or equivalent (such as SP-171) to the system(s) providing the data. In this case, the security categorization baseline requirement is Moderate. Based upon an audit performed in April 2019, this system was not compliant with the requirements for a system collecting, storing, processing, or disseminating sensitive data from federal sources. There is currently an effort underway to certify compliance of this system through a vendor other than the one who performed the initial audit in 2019.

- By June 30<sup>th</sup>, 2020, NOAA4300 plans to begin sharing electronic logbook and landing data with ACCSP.
- By September 30<sup>th</sup>, 2020, NOAA4300 plans to begin sharing Vessel Monitoring System (VMS) positional data with ACCSP in order to comply with pending regulations.
- By December 30<sup>th</sup>, 2020, in order to comply with pending regulations, NOAA4300 plans to share all for hire permit holder data with ACCSP.

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

5 U.S.C. § 301, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

FOIA-related authorities: 5 U.S.C. 552 and 552a, 15 CFR Part 4.

Permit and registration data 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, 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 is 31 U.S.C. 7701.

From: COMMERCE/DEPT-13: Executive Orders 10450, 11478, 12065, [5 U.S.C. 301](#) and 7531-

332; [15 U.S.C. 1501](#) *et seq.*; [28 U.S.C. 533-535](#); [44 U.S.C. 3101](#); Equal Employment Act of 1972; and all existing, applicable Department policies, and regulations.

From: COMMERCE/DEPT-14: 5 U.S.C. 301; 44 U.S.C. 31101; 42 U.S.C. 3211; 31 U.S.C. 240; 28 U.S.C. 533-535 and 1346(b); 15 U.S.C. 277 and 278e(b); E.O. 10450; E.O. 11478, as amended and all other authorities of the Department.

From: COMMERCE/DEPT-18: 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

From: COMMERCE/DEPT-25: 5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075.

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

NOAA4300 is a FIPS199 Moderate system.

**Section 1: Status of the Information System**

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

This is a new information system.

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

<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	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. j. Other changes that create new privacy risks (specify): <b>Pending connection/data sharing with ACCSP (upon 3<sup>rd</sup> party verification and validation of ACCSP obtaining FIPS199 moderate compliance).</b>					
<b>Video Camera System at all facility entrance and exit points, and in parking lot for safety and security purposes.</b>					

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	X
b. Taxpayer ID	X	g. Passport	X	k. Financial Transaction	X
c. Employer ID	X	h. Alien Registration	X	l. Vehicle Identifier	X
d. Employee ID	X	i. Credit Card	X	m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
<p>*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: Tax Identification Numbers/Social Security Numbers are collected to allow positive identification for cost recovery billing of Individual Fishing Quota holders.</p> <p>For Permits: 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.</p> <p>The credit card and financial account data contained in the system is for Federal purchase and travel cards, and travel accounts. No personal financial data or credit card information is collected, maintained, or disseminated.</p>					

<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	
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	X
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	
g. Citizenship	X	n. Religion			
u. Other general personal data (specify): Permit applicant, permit holder, permit transferor/transferee, vessel owner, vessel operator, dealer applicant, dealer permit holder, spouse, former spouse, or decedent.					

<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	X
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):					

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

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

<b>Other Information (specify):</b> 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, Catch/Observer Discard Data, Quota Share/Quota Pound Transfer Data, Business Operation Information (Business Processes, Procedures, Physical Maps).
---

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

<b>Directly from Individual about Whom the Information Pertains</b>					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X*	Email	X		
Other (specify):					
* For clarification of previously submitted information only					

<b>Government Sources</b>					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify):					

<b>Non-government Sources</b>					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

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

--

Employees can contact the HR representative for NOAA4300 and review their information, or a personal contact information form can be completed and given to HR, who will then update the information accordingly.

Permits: 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.

Partners for public outreach and education may update their information at any time by contacting the appropriate staff member assigned as their coordinator.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB Control Nos: 0648- 0013, 0648-0016, 0648-0205, 0648-0358. 0648-0543, 0648-0551, 0648-0703.
	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):			
<b>Video Camera System at all facility entrance and exit points, and in parking lot for facility safety and security purposes.</b>			

	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	X*
Video surveillance	X	Electronic purchase transactions	
Other (specify): The facility housing NOAA4300 maintains a video surveillance system, which is used only for the purposes outlined in DEPT-13 Routine Uses (security-related and law enforcement records access requirements).			

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

**Section 4: Purpose of the System**

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

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation	X	For criminal law enforcement activities	X
For civil enforcement activities	X	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):			

**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).

For PII/BII in reference to federal employees, contractors, foreign national guest/visitors, student interns, and volunteers:

The information required for determining Security Clearance by DOC Security for federal employees, contractors, interns, and volunteers may include full name, home address, home phone number, e-mail address, educational background, SSN, and employment history. The SERO Security Officer collects information in-person, via telephone (for clarifications/corrections on completed forms), via email/fax and submits forms for clearance process. A security clearance is required to gain access to the SERO facility. This information is collected from the individual requesting the clearance (employee, contractor, foreign national guest/visitor, student intern, or volunteer).

The information is maintained as a supplement to other records for purposes of human resource activities, Continuity of Operations (COOP) execution, and performing other related administrative tasks includes full name, grade level and/or position within the organization, role/responsibility, home address, home phone number, and mobile phone number. This information is collected from the individual employee, contractor, student intern, or volunteer. Information is also used by Human Resources regarding current employees and job applicants for administrative purposes. This information is collected from the individual employee or applicant.

For Permit-related PII/BII: 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 posts 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. This information is considered to be part of the public domain.

Tax Identification Numbers allow positive identification for cost recovery billing of IFQ holders. Also, as stated in the routine uses of COMMERCE/NOAA-12 and COMMERCE/NOAA-19, a Tax Identification Number 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.

Information will also be collected to facilitate public education, outreach, or collaboration with partners on research/conservation projects. For these activities, the name, address, e-mail address, telephone number, and other non-sensitive organizational information may be temporarily stored. These individuals, businesses or organizations may be workshop participants, business contacts, members of mailing lists, etc. In all cases, the information is voluntarily submitted by the individuals or representative of the business or organization.

NOAA4300 currently has a data sharing agreement with ACCSP. The ACCSP requires the generation of a unique identifier made up of fragmentary data drawn from the name, email address, telephone number, and birthdate of all for-hire SER Permit holders in order to validate landing reports. ACCSP will collect the unique identifier of SERO permit holders through an interconnection agreement with NOAA4400, Southeast Fisheries Science Center.

Once ACCSP is certified as a FIPS199 Moderate/equivalent system, PII/BII as specified in Part G of the System Description Section will be shared to most accurately match entities between systems, and a system interconnect agreement between ACCSP and NOAA4300 will be drafted and implemented. Annual Assessment and Independent Validation and Verification of continued compliance will be a critical condition of all data sharing and interconnect agreement renewals.

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.)

Disclosure of data from an internal source is considered the biggest potential threat to the PII/BII contained within NOAA4300. To mitigate this threat, the following measures are in place:

- All users are subject to a Code of Conduct that includes the requirement for confidentiality.
- All staff (employees and contractors) receive training on privacy and confidentiality policies and practices.
- Access to the PII/BII is restricted to authorized personnel only.
- The information is secured in accordance with FISMA requirements for a Moderate System.
- 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).

- A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
- Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.

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

\*Case by case with DOJ and U.S. Coast Guard if applicable (criminal enforcement leading to litigation).  
 \*\*The PII/BII in the system will not be shared unless required and authorized to do so on a case by case basis, such as with ACCSP, after successfully achieving FIPS199/equivalent requirements for a Moderate system.

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.

X	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: Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:  <b><u>NMFS Office of Law Enforcement (OLE)</u></b> All applicable controls are in place, including encryption of data at rest and during transfer.  <b><u>Atlantic Coastal Cooperative Statistics Program (ACCSP)   Atlantic Coastal Fisheries Information Network (ACFIN) - (Pending system interconnection)</u></b> All applicable controls reported as in place by ACCSP, including encryption of data at rest and during transfer.
	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.)*

<b>Class of Users</b>			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

### **Section 7: Notice and Consent**

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

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: <a href="https://www.fisheries.noaa.gov/national/fisheries-observers/privacy-act-statement">https://www.fisheries.noaa.gov/national/fisheries-observers/privacy-act-statement</a>	
X	Yes, notice is provided by other means.	Specify how: Notice is provided on the applicable employee forms.  Permits: Notice is provided on the permit or related application.  Outreach: Notice is given in the email response to the individual's email. Video Surveillance: Signs are posted at all points of entry to the facility and at vehicle entrances.
	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.	Specify how:  Information submitted for security clearances for access to federal networks/facility access is voluntary (may be declined, in writing, to the supervisor) but is required by federal regulations. Therefore, if the information is not provided, no access will be granted.  Information submitted for Human Resource activities such as hiring is voluntary (may be declined, in writing, to the supervisor), but if the required information is not provided, employment cannot be granted. Once employed, information is kept on file with Human Resources for COOP and other administrative purposes.  Permits: 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.
---	---	---

		Information for public outreach and education is strictly voluntary, by an email request. If information is not provided, it may affect the level or amount of services requested.
	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.	Specify how:  Security Clearance: Information is used solely for security clearance, and is only accessible to those employees whose job duties require access to this information. This information is usually submitted by completion of a form. The form outlines the <a href="#">NOAA Privacy Policy</a> , linked to NOAA web pages, which states that “Submitting voluntary information constitutes your consent to the use of the information for the stated purpose.” Information submitted for Human Resource activities such as hiring by completing a form. The form outlines the NOAA Privacy Policy, which states that “Submitting voluntary information constitutes your consent to the use of the information for the stated purpose.”  Employee information is kept on file with Human Resources for COOP and other administrative purposes.
	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.	Specify how:  Employees can contact the HR representative for NOAA4300 and review their information, or a personal contact information form can be completed and given to HR, who will then update the information accordingly.  Permits: 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.  Partners for public outreach and education may update their information at any time by contacting the Southeast Regional Office.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

**Section 8: Administrative and Technological Controls**

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

	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: Access to PII is tracked through database/application logging. Network administrators can track user access through these logs
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>3/11/2020</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 a moderate or higher. NOAA4300 is a FIPS199 Moderate System
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.
X	Contracts with customers establish DOC ownership rights over data including PII/BII.
X	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).

There is no public access to NOAA4300. Users are only allowed access to information that is required for them to fulfill their job duties. All portable computers are encrypted with McAfee Disk Encryption.

Access to PII is controlled through access control policies and access enforcement mechanisms. Separation of duties is strictly enforced for duties involving access to PII.

Least privilege is enforced for all NOAA4300 users, enforcing 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.

Access to information system media containing PII, including digital media, is restricted to authorized personnel. Users are uniquely identified and authenticated through either 2 factor authentication or USGCB compliant passwords before accessing PII.

PII, both in paper and digital forms, is securely stored until destroyed or sanitized using approved equipment, techniques, and procedures.

Removable media and mobile devices containing PII that are transported outside the organization’s controlled space are protected using both physical methods and data encryption.

The confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape, is protected through full disk/tape encryption. Any printed output containing PII/BII is secured

in a locked file cabinet or drawer.

**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	<p>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></p> <p>DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons DEPT-5, Freedom of Information and Privacy Request Records  DEPT-18, Employees Personnel Files Not Covered By Notices of Other Agencies DEPT-19, Department Mailing Lists  DEPT-20, Biographical Files  NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA’s Mission.</p> <p>Permits:  COMMERCE/DEPT-13, Investigative and Security Records.  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</p> <p>COMMERCE/DEPT-14, Litigation, Claims, and Administrative Proceeding Records. COMMERCE/DEPT-25, Access Control and Identity Management System  GSA/GOVT-7, Federal Personal Identity Verification Identity Management System (PIV IDMS)</p>
	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	<p>There is an approved record control schedule. Provide the name of the record control schedule:</p> <p>NOAA Chapter 100: Enterprise-Wide Functions  Electronic Records schedule: NARA General Records Schedule 20, Electronic Records.  Individual records are removed manually from the system at personnel separation</p> <p>Permits: There are approved record control schedules for both Sustainable Fisheries and Marine Mammal Protection permits.  NOAA 1504-11  NOAA 1514-01</p>
---	--

	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	X	Deleting	X
Other (specify):			

**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 information contained within the system could be used to identify individuals, and potentially verify their identity to third parties. Compromise of PII could result in adverse effects on individuals (Identity Theft), as well as a loss of public trust in the organization, which would hinder the agency's overall mission.
X	Quantity of PII	Provide explanation: full name, home address, home phone number, e-mail address, educational background, SSN, and employment history. Any or all of these could be used to the detriment of the individual to whom they belong.
X	Data Field Sensitivity	Provide explanation: Data field sensitivity ranges from moderate to high value PII/BII.
	Context of Use	Provide explanation:

X	Obligation to Protect Confidentiality	Provide explanation: Magnuson-Stevens Fishery Conservation and Management Act
	Access to and Location of PII	Provide explanation:
	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.)

As information is collected from the individual, little to no threat to privacy exists at point of collection. All information collected is the minimum required by policy or statute to accomplish the agency's mission and/or fulfill the purpose the information is being collected for.

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

X	Yes, the conduct of this PIA results in required business process changes.
	<p>Explanation: In order to comply with the Social Security Number Fraud Prevention Act of 2017, which restricts the inclusion of SSN on Federal Government mailed correspondence, Federal Agencies will not be allowed to include a full SSN on mailed items. By 2022, there will be no more mailing of completed Permit applications from applicants to NOAA, unless the head of the agency deems it necessary to include the complete SSN on a mailed application.</p> <p>Ensuring annual FIPS199 Moderate (or equivalent SP-171) compliance of ACCSP in order to renew any ISA and data sharing agreements to support pending regulations will require hard and enforceable deadlines to be placed upon ACCSP to provide sufficient documentation prior to renewal of the PIA, ISA, and any other interconnect agreements. This will require coordination between NMFS OCIO, ACCSP, and NOAA4300 IT Staff.</p>
	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.

## **APPENDIX A: NOAA4300 ISSO Findings with ACCSP Control Statements Based Upon Requested Artifacts and Clarifications**

(Note: These findings are current as of 5/21/2020. No new artifacts have been submitted to NOAA4300 from ACCSP. NMFS OCIO provided notification on the evening of 5/26/2020 that new artifacts were sent to them regarding some of these findings. Updates to this appendix will follow via email once the artifacts have been reviewed.)

Additional information was requested from ACCSP staff to clarify some of the privacy control statements submitted for the NOAA4300 PIA (Section 6.2).

Red text is what was sent to ACCSP as a request for additional information.

Blue text is the response from ACCSP to the request for additional information/artifacts.

*Italicized black text is the conclusion reached, based upon the information/artifacts provided.*

### **Least Privilege (AC-6) SP800-171 Rev. 2 – CUI 3.1.5: Employ the principle of least privilege, including for specific security functions and privileged accounts.**

Role Based access control is employed to ensure that privileges associated with each account type is the minimum needed for access to ACCSP resources to accomplish their assigned tasks. However, even though specific privileged roles and responsibilities are defined, the limited ACCSP staffing levels does not permit a total division of duties. Least privilege is implemented as a means to allocate the use of existing resources to their assigned account and reduces operational risk and maintains the integrity of the information. All administrative actions are subject to being audited. All user actions are subject to auditing. Logging or auditing of successful or blocked privileged access is only implemented on Oracle database, with only minimal (only SSH attempts) auditing at operating-system level. See extract from ACFIN POAM document to cover AC-6(9) and AC-6(10).

*The POAM [referenced above] states “Prevent non-privileged users from executing privileged functions and audit the execution of such functions.” Are any interim measures being taken to mitigate this risk until this POAM can be completed? For example, are there any mechanisms in place to alert administrators of these actions until the POAM can be completed?*

*The underlined text in the statement above states that all user and administrative actions are subject to auditing. What sort of auditing are they currently subject to, based on the system’s current audit capability? Please provide an artifact showing what events are or can currently be audited, both within Oracle and at the OS level. The more detail provided in each artifact, the better.*

*Database changes are logged and saved with user and timestamp.*

*No logs or additional artifacts to support or clarify the audit capability statement were provided, although it is reasonable to accept the time/date stamp assertion, as that is industry standard in most cases. What remains in question is the actual content of the audit capability in place now, as the POAM statement indicates a large amount of data is currently not auditable.*

*The text below is an excerpt from the POAM (2020-1) which indicates the scope of current*

*deficiencies in ACCSP's audit capability:*

1. *Develop and document a more formal audit review process.*
2. *Expand audit review to more system devices and processes.*
3. *Enhancements to auditing including the addition of the following audit events:*
  - *Successful and unsuccessful logons and logoffs*
  - *Successful and unsuccessful attempts to access security relevant files and utilities*
  - *Operations performed to read, modify or destroy audit information*
  - *Modifications to the audit configuration that occur while the audit functions are operating*
  - *Unsuccessful revocation of security attributes*
  - *Modifications to the group of users that are part of a role*
  - *Changes to the system time*

*The most recent update to the POAM by ACCSP indicates the implementation of Netflow as an interim solution. Despite the above request for an audit log example, none were provided. The only response to the request was “**Database changes are logged and saved with user and timestamp.**” Another critical concern is the SAR finding indicating the presence of administrator level accounts on ACCSP workstations. There is a POAM in place to remove these privileges (POAM 2020-6), with a completion date of 7/31/2020. This was not initially disclosed to NOAA4300, nor was it stated in the submitted control text in the PIA.*

**Remote Access (AC-17) SP800-171 Rev. 2 – CUI 3.1.12: Monitor and control remote access sessions.**

ACFIN is a LAN infrastructure with some public-facing services (DNS, Tomcat) hosted on Amazon Web Services (AWS). Privilege users access servers by first connecting through SSL VPN followed by either SSH or RDP to specific servers. Management of AWS is done via HTTPS. In order to gain access to ACCSP resources, a user must first connect to the VPN using CISCO AnyConnect.

**SERVERS:** Remote access to servers is only allowed by admins and they must use the ACCSP VPN.

**DESKTOPS:** Remote access to desktops is only allowed with special permission from Management and those who are allowed must use the ACCSP VPN.

**APPLICATIONS:** Remote access to internal applications is only allowed with the use of the ACCSP VPN.

*According to the ACCSP Remote Access Policy, personally owned devices are allowed to connect to the ACCSP internal network, is this correct? Is there an AV requirement or patch level baseline for BYOD that is currently enforced? I see that requirement #6 states “Personal computer devices must meet the requirements for remote access which generally includes all Windows, MacOS, or Linux operating systems still receiving current security updates.” Is there an auditing or enforcement policy in place to validate personal devices meet these requirements? Is there a mechanism to warn ACCSP system administrators of personal devices connecting to the system that are missing 1 or more critical patches, or have potential malware installed?*

*Added the need for BYOD security policy and requirements to POAM list in accordance with NIST SP800-46r2 and NIST SP800-114r1.*

*BYOD POAM (2020-34) set to complete 7/31/2020. – Complete POAM text follows.*

*“Develop, share and enforce the Bring Your Own Device security policy and requirements to allow usage of these devices on ACFIN.  
Add the BYOD policy as an appendix to the to the remote access policy for ACFIN.”*

*I see the [ACCSP Remote Access] policy states “The ACFIN Information Security Team reserves the right to verify compliance through methods including, but not limited to, network-traffic monitoring and device inspections.” Is there a template or SOP for these actions in place, or is there a previous instance of audit/network traffic monitoring you can provide (username redacted)?*

*No artifact/clarification was provided for this request, further indicating a lack of control or monitoring of remote access to the system.*

*What documented actions are taken if an unauthorized user’s presence or activity is discovered?  
Can you provide any examples of this?*

*No artifact/clarification provided.*

## **Auditable Events (AU-2)**

### **SP800-171 Rev. 2 – CUI 3.3.1**

Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

This control is partially met. ACFIN has operating and database system audits with email notifications sent to the system administrators as daily system summaries, and when major system-health incidents occur. Audited events cover all critical systems, i.e. account access, operating systems, web apps and databases. See extract from ACFIN POAM document.

The ACFIN POAM includes enhancements to auditing including the addition of the following audit events:

- Successful and unsuccessful logons and logoffs
- Successful and unsuccessful attempts to access security relevant files and utilities
- Operations performed to read, modify or destroy audit information
- Modifications to the audit configuration that occur while the audit functions are operating
- Unsuccessful revocation of security attributes
- Modifications to the group of users that are part of a role
- Changes to the system time
- Denial of access resulting from an excessive number of logon attempts
- Uses of privileged account

Audit records containing this information are deemed to be adequate to support after-the-fact investigations of security incidents. Audit logs will be used to help troubleshoot related system problems.

*Please provide an example of a current audit log and its content to demonstrate what information is auditable at this time.*

*Until the referenced POAM is completed, are there any interim measures or practices in place to mitigate the risk of the current information gap? If so, please provide an artifact detailing these interim measures.*

*It is unclear what can be audited – it is stated that “Audited events cover all critical systems, i.e. account access, operating systems, web apps and databases. See extract from ACFIN POAM document”, but the POAM states that enhancements will include critical information/events such as:*

- Successful and unsuccessful logons and logoffs*
- Successful and unsuccessful attempts to access security relevant files and utilities*
- Operations performed to read, modify or destroy audit information*
- Modifications to the audit configuration that occur while the audit functions are operating*
- Unsuccessful revocation of security attributes*
- Modifications to the group of users that are part of a role*
- Changes to the system time*
- Denial of access resulting from an excessive number of logon attempts*
- Uses of privileged account*

*Each of these are account access and action items that are critical to successful auditing. An artifact detailing what can currently be audited would clarify this issue, as without the information listed above, it is difficult if not impossible to track activities in the system in such a way that they can be attributed to an individual.*

*The statement for AC-6 indicates, “Logging or auditing of successful or blocked privileged access is only implemented on Oracle database, with only minimal (only SSH attempts) auditing at operating-system level. See extract from ACFIN POAM document to cover AC-6(9) and AC-6(10).” With this statement in evidence, what measures and capabilities are currently in place for auditing activity on the critical (non-Oracle) systems specified in the statement above with regard to account access, operating systems, and web apps, other than SSH attempts (as indicated in the statement for AC-6)? Please provide an artifact to support the clarification.*

*Modified SSP CUI 3.3.1:*

*“ACFIN records all database session activity using Oracle Enterprise Manager (OEM). Access to individual production database systems and changes made to mission critical data are logged. Logs are retained within system backups. At the database level, database transactions and standard CRUD operations are stored in audit fields (user\_entered, user\_changed, date\_entered, date\_changed). Audit logs also track data changes to critical tables.*

*Operating system monitoring and session activity is logged and system administrators are notified of any unauthorized system login attempts by unknown users and IPs. Access to individual production database systems and changes made to mission critical data are logged. All logs are retained within the system indefinitely. Operating system logging and monitoring is covered by RHEL Logwatch monitoring and email notifications. Enterprise Manager host monitoring is also enabled to provide supplemental critical service alerts on RHEL hosts. Our Tomcat host is monitored using AWS CloudWatch configured to sent system-health alerts and failures.”*

*artifacts added:*

*Artifact\_ACCSP\_unathorized\_activity\_notification\_scup\_server.jpg.(1)*

*Artifact\_ACCSP\_OracleEnterpriseManager\_OEM\_session\_client\_activity\_Apr19\_Apr20\_2020 (2)*  
*AU-6\_Artifact\_Audit\_Logging\_Apps\_APEX\_access\_log.jpg. (3)*

*No artifacts were submitted to support the text of the response. No logs have been submitted to demonstrate the current audit capability of ACCSP.*

*The 3 artifacts referenced were numbered and are described below.*

*Artifact 1 is an email alert of an event, not an audit log.*

*Artifact 2 is a screenshot of the Oracle Cloud Control console, and shows no evidence of audit events or logfile review. It is showing load and usage activity, not individual user activity, which does nothing to enforce individual accountability.*

*Artifact 3 is an authentication log, not an event log. This shows who logged on, but nothing past that (actions taken, files altered, etc.)*

**Audit Review, Analysis, and Reporting (AU-6) SP800-171 Rev. 2 – CUI 3.3.2:** Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Audit reporting and reviewing will entail audit record analysis to identify inappropriate or unusual activity. Unusual, suspicious, or unauthorized activity is to be reported to the ISSO and/or system owner as soon as possible. If warranted, the ISSO will initiate investigation into the suspicious activity and document suspected violations. See extract from ACFIN POAM document.

*Please provide an artifact showing any interim measures to audit or review account activity, if any. Is there or will there be a mechanism in place to detect unusual activity, or will there be a required frequency for manual review of system logs? Will there be an SOP detailing these procedures?*

*The statement for AU-2 indicates that some auditing is performed – please include an artifact to support this and demonstrate current capabilities within the system, at all levels of operation.*

*Added artifacts of logs that identify user and page access:*

*AU-6\_Artifact\_Audit\_Logging\_Apps\_APEX\_access\_log.jpg*

*The artifact provided shows login activity, but no access or action events (files copied, deleted, renamed, etc.) Is this the current level of logging available, or is there anything more detailed? Repeated requests for detailed examples of audit logs have gone unanswered. No answer to the SOP or planned review frequency was given.*

**Media Access (MP-2) SP800-171 Rev. 2 – CUI 3.8.1:** Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.

The organization restricts access to system and end user media, both paper and digital. All server disk drives and backup tape media are physically protected in the locked server room, to which only authorized personnel have key access. Quarterly offsite tapes are transported by the system administrator to the storage facility and old media rotated back into server room use the next day. Upon end of life of, media is physically destroyed / shredded and recycled at appropriate electronics recycling facilities. Staff desktop and laptop computers follow established password and lock screen security. Staff are not permitted to share CUI outside of the organization. Media are securely stored in a fireproof Cabinet accessible by keys. Only authorized personnel have access to the keys.

*Are the quarterly backup tapes stored in a safe or other locked container at the storage facility?*

*Is this storage facility a specialized IT media storage facility, such as Iron Mountain, or is it a “regular” storage facility?*

*Safe at a “regular” storage facility, covered under existing POAM 2020-29.*

*The “regular” storage facility being referred to is the IT Director’s home. The backups are kept in a portable file strongbox at his residence. This was documented as a finding in the SAR that was not shared with NOAA4300; instead, the Authorizing Official chose to use the text in the PIA and refer to the IT Director’s residence as a “regular” storage facility.*

*Are the backup tapes encrypted? If so, please provide an artifact verifying this.*

*Yes. See: MP-2\_artifact\_ACCSP\_BackupExec\_media\_encryption.jpg*

*The artifact provided indicates the backup tapes are encrypted – it does not show the algorithm, or whether it is a FIPS 140 compliant encryption solution.*

*how are they [offsite quarterly backups] stored/secured at the facility? Please provide an artifact showing how the quarterly backups are secured at the offsite facility.*

*Out of scope / not necessary. The pictured safe is used at a Regular storage facility over 50 miles from the office in a climate controlled environment to address disaster recovery concerns.*

*A POAM (2020-29) is now in place to acquire the services of a secure IT storage facility for storing ACCSP backup media, rather than the IT Director’s home.*

**Media Storage (MP-4) SP800-171 Rev. 2 – CUI 3.8.2: Limit access to CUI on information system media to authorized users.**

All network tapes and drives are physically protected in the locked server room, to which only authorized personnel have key access. ACCSP staff PCs use established password and lock screen security. Staff are instructed to refrain from storing sensitive CUI on paper, DVD, external drive or other media, in their possession. Sensitive CUI must be on encrypted media only.

*Is this staff instruction documented or made available to users in a published policy or ROB other than on the ACCSP account form? Do users receive a copy of this form?*

*The ACCSP account form serves that purpose as all end-users have access to it. Internal ACCSP policies are not published.*

*Other than the initial form an employee signs when they are hired, there are no reminders of ACCSP’s policy to safeguard CUI. Given the fact that remote users are not trained in proper handling of CUI (SAR finding), there is no background screening of new hires included in the hiring process (SAR finding), and no mobile devices used by ACCSP are encrypted (SAR finding), this lack of documentation or reminder is a point of concern.*

**Protection of Information at Rest (SC-28) SP800-171 Rev. 2 – CUI 3.13.16: Protect the confidentiality of CUI at rest.**

Data at rest on ACCSP/ACFIN servers is defined as the secure baseline configuration, the firewall rule set, and authenticator content. To meet the PII/PIA requirement, data are encrypted at-rest in ACFIN Oracle databases. Data is encrypted at-rest PII (e.g. birth dates) using Oracle's transparent data encryption (TDE). TDE uses AES 192 bit encryption.

*What other data is encrypted at rest within the system? Please provide an artifact for each type, or if possible, a report showing all encrypted data tables. This is a critical factor, and each data type/table that is encrypted must be documented with an artifact.*

*PII in the context of SERO-ACFIN data sharing was defined earlier as only birth dates. OMB Memorandum M-07-1616 does not classify email address as PII, however we have encrypted it. Any other data encrypted within the system, and the associated artifacts, are outside the scope of this agreement and therefore not applicable.*

*Added artifact: SC-28\_Artifact\_ACCSP\_Oracle\_TDE\_at\_rest\_encrypted\_pii\_columns.jpg  
MP-2\_Artifact\_ACCSP\_BackupExec\_media\_encryption.jpg*

*All data provided to ACCSP by NOAA4300 is within the scope of this document, and has been discussed in meetings prior to this request. Position reports, landing reports, logbook reports, etc. are BII/Trade Secret data and are required to be listed on the host system's PIA, and protected accordingly. The latest PIA for ACCSP states that DOB is the only PII in the system – this is completely incorrect. NOAA4300 will be sharing logbook reports, landing reports, vessel location data, and other for-hire permit holder data, which includes PII, BII, and Trade Secret information. ACCSP has not provided an artifact demonstrating that the applicable data is not properly encrypted despite multiple requests. The only artifact provided by ACCSP showed the DOB table was encrypted; no other tables or data types were referenced.*

*The NMFS CIO has stated that the Oracle TDE 192 bit encryption is sufficient for safeguarding sensitive government data within ACCSP. There is no artifact describing or detailing exactly what data is encrypted in the database, despite multiple requests.*

Other significant security concerns of this system (listed as significant vulnerabilities in the ACFIN SAR) include:

- 1) **ACCSP does not encrypt mobile devices.** There is a POAM in place (2020-11) to be completed by 9/30/2020. Complete POAM text follows:

“Determine if ACCSP mobile devices require encrypting, if CUI is present on mobile devices or if this is acceptable risk.”

*(Note: this does not indicate the testing or implementation of encryption; merely the consideration of whether or not encryption is required.)*

- 2) **Screening of individuals is not included in the hiring process.** – POAM in place (2020-07) planned completion 9/30/2020

- 3) **ACCSP does not periodically scan for vulnerabilities to the ACFIN network.** - POAM in place (2020-06) planned completion 9/30/2020
- 4) **An incident response capability has not been established.** - POAM in place (2020-01) planned completion 8/17/2020
- 5) **Malicious code protection is not deployed on the Linux servers.** – POAM in place (2020-14), completion date 5/15/2020. No completion artifact submitted or update regarding implementation provided.

*ACCSP has made progress toward compliance with OMB/FISMA requirements, but still has much to accomplish before reaching what would normally be considered a compliant posture. The following issues have POAMs in place, but some of them (particularly the encryption of mobile devices, vulnerability scanning, and malicious code protection) stand out as major shortcomings that may not be addressed with the appropriate degree of alacrity, given the amount of sensitive government data contained within the system.*

*ACCSP collects, stores, processes and disseminates PII, BII, and Trade Secret data from multiple government agencies, and:*

- 1) *Does not encrypt any mobile devices that have access to this data. Furthermore, ACCSP will not determine whether or not it is necessary to do so until September 30, 2020, despite these devices having access to sensitive government data.*
- 2) *Does not have malicious code protection in place on their Linux servers. The current POAM completion date has passed, and may have been completed – no artifacts or updates have been provided at the time of this writing.*
- 3) *Does not perform routine vulnerability scanning of the system, and will not have the capability to do so until September 30, 2020.*
- 4) *Does not have the audit capability to ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions, and despite multiple requests, will not provide a detailed artifact or example (such as an audit log) to demonstrate what capabilities are currently in place.*
- 5) *Allows personal devices to connect to the network through VPN, with no baseline configuration or scanning capability to monitor or enforce compliance with any BYOD requirements.*
- 6) *Allows Administrator level access on workstations, despite a documented lack of audit capability.*
- 7) *Has no incident response procedure documented or implemented – multiple requests for an artifact showing some level of capability in terms of incident response have never been answered.*

