

# U.S. Department of Commerce NOAA



## Privacy Impact Assessment for the National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301)

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  
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary,  
cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743  
Date: 2018.02.12 18:25:52 -05'00'

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

Date

## **U.S. Department of Commerce Privacy Impact Assessment National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301)**

**Unique Project Identifier: 006-00-02-00-01-0511-00**

### **Introduction: System Description**

The NOAA6301 NCCOS Research Support System provides the network infrastructure, hardware and software necessary to enable the mission of NCCOS, the organization. NCCOS's mission is to provide coastal managers with scientific information and tools needed to balance society's environmental, social, and economic goals.

NCCOS is passionate about supporting NOAA's environmental and economic missions by providing valuable scientific information to its constituents. NCCOS's fundamental principles are:

- To deliver high-quality science in a timely and consistent manner using productive and strong partnerships.
- To develop and maintain relevant research, long-term data collection and analyses, and forecasting capabilities in support of its customers, stakeholders, and partners.
- To build capacity in the private, local, state, and tribal sectors by transferring technology and providing technical assistance and knowledge to its customers and partners.
- To conduct the anticipatory science necessary to manage potential impacts of multiple stressors on coastal ecosystems.

The NOAA6301 system:

- provides support to the program areas which are responsible for conducting research in the areas of marine bio-toxins; eco-toxicology; forensics; biotechnology; marine mammal stranding and necropsies; risk analysis; DNA sequencing; and marine related viruses and pathogens;
- provides an operational environment supporting the mission and staff of the program offices located on the Silver Spring Metro Center Campus - NCCOS Head Quarters (HQ), Center for Sponsored Coastal Ocean Research (CSCOR), and Center for Coastal Monitoring and Assessment (CCMA); Beaufort, NC - Center for Coastal Fisheries and Habitat Research (CCFHR); Charleston, SC – Center for Coastal Environmental Health and Biomolecular Research (CCEHBR) and Hollings Marine Laboratory (HML); and Oxford, MD – Cooperative Oxford Laboratory (COL);
- provides all resources related to data management, electronic file, COTS, printing, computer and software, field data acquisition, backup and restoration, LAN, helpdesk, specialty applications for GIS and statistical analysis, moderate programming, Web design and Web product delivery, video conferencing, and other media support services; and
- Provides continued service to the local area network (LAN) connections for non-SSMC locations.

In addition to the general purposes office automation support (file/printer sharing, application

hosting, collaboration, etc.) provided by NOAA6301, the system provides help desk services and supports a number of web sites and internal minor applications, one of which stores PII for the purpose of conducting the external grant review process as defined within the NOAA Grants Online System, (FISMA system ID, NOAA1101, PIA signed 7/6/2017). Grant applications are downloaded from Grants Online on a case by case basis, for review. They are stored by opportunity or grant number.

As detailed in the information sharing section below, NCCOS gathers and stores PII related to employees and contractors for Human Resource-related issues such as the hiring process as well as workforce planning, COOP Operations, and documentation. The NCCOS collects BII during the pre and post activities associated with the acquisition and management of contracts.

### **Information Sharing**

NOAA6301 NCCOS Research Support System General Support System (GSS) collects and collects and stores limited PII, specifically, names, telephone numbers and email addresses (voluntarily submitted by staff, partners, volunteers, and government and non-government collaborators) to facilitate internal and external communications to facilitate business and collaborative functions. This is not a central collection, but rather separated by function or individual project or person.

NOAA6301 is a general support system for NCCOS and stores information about individuals during the application and hiring of (electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase), including standard HR information (such as Travel authorization and vouchers, passports and international travel forms (completed by the employee through the travel portal), information for security badging process (contact information only – the employee completed the badge application on paper forms, which are taken to the NOAA Office of Security), and performance appraisal ranking).

NCCOS' employee data is collected, stored and maintained for internal COOP, Human Resources, and workforce planning purposes (federal employee/contractor).

NCCOS collects BII during the pre and post activities associated with the acquisition and management of contracts. The storage is in the form of PDF forms or MS Word documents. There is no major application or database used to collect or store BII or employee PII information. NCCOS does not have a separate HR division since NCCOS utilizes the NOAA Workforce Management Office.

With exception of the CSCOR Review Application, all information is stored on supervisors' and acquisition managers' restricted access file storage available only to the specific employee(s). Access is restricted to those on a need to know basis, by permissions settings and/or passwords. The data is access controlled when on a supervisor's desktop machine or file share; if stored on a supervisor's laptop, the data is encrypted since all mobile devices have full encryption. The CSCOR Review Application although managed by NCCOS, is hosted by an NOAA6001 NOS Enterprise Services server and is restricted by username and password.

CSCOR Review Application – Information in identifying form is made available by NOAA Grants Online (FISMA system ID, NOAA1101, PIA signed 7/6/2017) to NCCOS to accomplish Independent Individual Merit Reviews supporting the NOAA Grants Online system and process.

Information about the NOAA Grants Program may be found at: <http://www.corporateservices.noaa.gov/~grantsonline/index.html>. This is a non-public system. Information extracted from NOAA Grants Online to support the Independent Individual Merit Reviews is temporarily stored to facilitate the review process lifecycle. This information can include any general personal information and work related information. Although it is not the intent to extract PII information from the NOAA Grants Online system, it is possible the information could contain the Employer Identification Number (EIN). The EIN is a non-mandatory field which may be populated on the grants information made available by federal forms not managed by NCCOS. The NCCOS information system does not collect this identifying information directly.

**A citation of the legal authority to collect PII and/or BII**

The general legislation supporting the system is 5 U.S.C.301, one of the statutes concerning government organization and employees.

Additional authorities from DEPT-2, Accounts Receivable: H.R. 4613 (97<sup>th</sup>): Debt Collection Act of 1982, a bill to increase the efficiency of Government-wide efforts to collect debts owed the United States and to provide additional procedures for the collection of debts owed the United States and 5 U.S.C. 5701-09; 31 U.S.C. 951-953, 4 CFR 102.4, FPMR 101-7; Treasury Fiscal Requirements Manual.

Additional authorities from GSA/GOVT-9, System for Award Management: Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204, and 40 U.S.C. 121(c), Regulations by Administrator. For the Entity Management functional area of Systems Award Management, the authorities for collecting the information and maintaining the system are the Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204 and 2 CFR, Subtitle A, Chapter I, and Part 25, as well as 40 U.S.C. 121(c). For the exclusions portion of the Performance Information functional area, the authorities for collecting the information and maintaining the system are FAR Subparts 9.4 and 28.2, Executive Order 12549 (February 18, 1986), Executive Order 12689 (August 16, 1989).

**The Federal Information Processing Standard (FIPS) 199 security impact category for NOAA6301 is moderate.**

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

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

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

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	

b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

X This is an existing information system in which changes do not create new privacy risks.

## **Section 2: Information in the System**

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

<b>Identifying Numbers (IN)</b>					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID	X**	f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport	x	k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					
** Same data element checked for Grants Online, as in the NOAA1101 PIA.					

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

<b>Work-Related Data (WRD)</b>					
a. Occupation	x	d. Telephone Number	x	g. Salary	x
b. Job Title	x	e. Email Address	x	h. Work History	x
c. Work Address	x	f. Business Associates			
i. Other work-related data (specify):					

<b>Distinguishing Features/Biometrics (DFB)</b>					
a. Fingerprints		d. Photographs		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): NCCOS does not capture photographs for badging since it is performed and stored by the NOAA badging office of security.					

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

<b>Other Information (specify)</b>
<b>Pre and Post Acquisition.</b> This BII information would be obtained and utilized during the pre acquisition obtained through deliverable BIDS package and contain specific company information. BII information would be maintained on specific secure network folders during the execution of awarded contract and other information from companies not receiving awards would be deleted, when appropriate. This information is protected under 41 USC 253, the FOIA Exemption 3 statute for contract proposals and collections associated with them.

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	
Telephone		Email	x		
Other (specify):					

<b>Government Sources</b>					
Within the Bureau	x	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify): NOAA Grants Online <a href="http://www.corporateservices.noaa.gov/~grantsonline/index.html">http://www.corporateservices.noaa.gov/~grantsonline/index.html</a> .					

<b>Non-government Sources</b>					
Public Organizations	x	Private Sector	x	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): NCCOS does not acquire PII from other non-government sources other than associated through formal partnership agreements and for the purpose of facilities safety, security, and COOP. Other non-government sources would be only for BII associated with Pre/Post Acquisition Sensitive Information obtained through delivered bids on NCCOS Acquisitions.					

2.3 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):					

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

**Section 3: System Supported Activities**

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

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

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

**Section 4: Purpose of the System**

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

Purpose			
To determine eligibility		For administering human resources programs	x
For administrative matters	x	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session )		For web measurement and customization technologies (multi-session )	
Other (specify): Collected BII would be associated with determine qualification/eligibility for open acquisitions. PII would be collected for administrative actions, for HR and Workforce management. PII/BII: NOAA Grants Online - Grant Merit Reviews			

**Section 5: Use of the Information**

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

In general, the laws that created the various NOS programs, specifically NCCOS, include provisions for the program to accomplish a mission. The mission may involve partnerships and educating the public. The collection and storage of information is part of accomplishing the legislated mission of the NCCOS, the NOS, and NOAA (members of the public and federal employees).

NOAA6301 stores PII on an ad hoc basis as part of the application and hiring of employees, including electronic copies of resumes and the processing of HR data about employees including hiring ranking. This information is stored temporarily during the hiring phase, as well as standard HR information such as travel authorization and vouchers, passports and international travel forms, information for the security badging process (name, work email address and work telephone number, and performance appraisal ranking).

NCCOS stores limited PII and potentially an EIN (BII), for grant review only, on an ad hoc basis about individuals or entities that are providing information in support of a grant application submitted through NOAA Grants Online which is retained for the review process lifecycle only.

BII – Pre and Post Acquisition. This BII information would be obtained and utilized during the pre-acquisition obtained through deliverable BIDS package and contain specific company information. BII information would be maintained on specific secure network folders during the execution of awarded contract and other information from companies not receiving awards would be deleted, when appropriate.

**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			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

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



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

X	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.</p> <p>Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NOAA6301 connects to the NOS Line Office information system NOAA6001 and other NOAA information systems for VPN, Security and Network Operations. NCCOS established security permissions based on NOS Active Directory Network account (enforced 2FA when possible), restrictions in firewall ACL and security permissions on specific network folders where documentation is stored.</p>
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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

Class of Users			
General Public		Government Employees	x
Contractors	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	<p>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://coastalscience.noaa.gov/contact/privacy">https://coastalscience.noaa.gov/contact/privacy</a>.</p> <p>A PAS for Grants Online has been finalized and has been posted at: <a href="https://grantsonline.rdc.noaa.gov/">https://grantsonline.rdc.noaa.gov/</a></p>	
x	Yes, notice is provided by other means.	<p>Specify how: (Specific to PII) Verbally by administrative appointed staff or supervisor OR this address is referenced: <a href="https://coastalscience.noaa.gov/contact/privacy">https://coastalscience.noaa.gov/contact/privacy</a>. This is an NOS standard privacy policy and not specific to NCCOS.</p> <p>BII is provided for the purpose of acquisition consideration only through government managed acquisition processes and forms only. NCCOS does not generate or maintain additional forms or processes to support acquisition activities. BII provided within NOAA Grants Online utilized within the CSCOR Review Application is managed through the NOAA Grants Online application only.</p>

	No, notice is not provided.	Specify why not:
--	-----------------------------	------------------

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

x	Yes, individuals have an opportunity to decline to provide PII/BII.	<p>Specify how: PII: No information collected is mandatory. Individuals are verbally told by administrative appointed staff or supervisor that they can decline or individuals are directed to review the privacy policy at this address: <a href="https://coastalscience.noaa.gov/contact/privacy">https://coastalscience.noaa.gov/contact/privacy</a>, where it is stated all information collected is voluntary. This is an NOS standard privacy policy and not specific to NCCOS.</p> <p>BII provided for acquisition consideration is not mandatory. However, declining to provide the information necessary to evaluate them for an acquisition could result in non-award.</p> <p>PII provided within NOAA Grants Online, utilized within the CSCOR Review Application, is managed through the NOAA Grants Online application only. Completion of the Grants Online application would be needed for award consideration.</p>
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	<p>Specify how: Applicants for positions are providing their personal information on a voluntary basis through their resumes. There is only one use for this information. The employment application contains the Privacy Act notice. Applicants have the opportunity to consent to only particular uses of their PII, in writing, to the HR representative or their supervisor, but it may affect the overall processing of their employment.</p> <p>For ongoing employee business, such as travel, there is only one specific use for each PII collection.</p> <p>BII is submitted for a specific purpose which consent is implied with the submittal of the package. BII provided within NOAA Grants Online utilized within the CSCOR Review Application is managed through the NOAA Grants Online application only.</p>
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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

x	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: (Specific to PII) NCCOS employees can contact HR staff or the federal employee personnel page to update their information, as they are informed as part of new employee
---	---	--

		<p>orientation.</p> <p>BII is provided for the purpose of acquisition consideration through government managed acquisition processes and forms only. NCCOS does not generate or maintain additional forms or processes to support acquisition activities. BII provided within NOAA Grants Online utilized within the CSCOR Review Application is managed through the NOAA Grants Online application only.</p> <p>Regarding contracts and grants that are in process or awarded, the applicants or awardees would send updates to the stated NOAA contact.</p>
	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	<p>Access to the PII/BII is being monitored, tracked, or recorded.</p> <p>Explanation: With exception to the CSCOR Review Application, access to storage folders are restricted by ACL and since PII/BII is not centralized in a database it cannot be easily monitored for access. The CSCOR Review Application has a database which is monitored, tracked and recorded.</p>
x	<p>The information is secured in accordance with FISMA requirements.</p> <p>Provide date of most recent Assessment and Authorization (A&amp;A): 3/23/2017. Next one is no later than 3/22/2018.</p> <p><input type="checkbox"/> This is a new system. The A&amp;A date will be provided when the A&amp;A package is approved.</p>
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
x	Other (specify): All appropriate contractors and contract clauses include non-disclosure, but not all federal employees sign a confidentiality agreement or non-disclosure agreement.

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

All information is stored within the accredited boundaries of NOAA6301 in network data shares controlled by established permission based on the organizational, project, or employee access rights. Any access to specific restricted files or folders must be requested through an access change request which is reviewed and documented by the NOAA6301 Information System Security Officer for authorization and mission ‘need-to-know’ requirement prior to implementation. Least privilege is implemented through file share permissions to ensure privacy and open only to those demonstrating a “need to know.”

Any PII information which is transmitted electronically must follow the federal government and NOAA standard procedure of secure packaging such as utilization of Department of Commerce (DOC) Accellion for encryption in transit.

NCCOS implements security controls listed in NIST Special Publication 800-53 R4 required for a moderate system. In compliance with NIST Special Publication 800-53 rev 4, NCCOS has a security program, with performance measures and goals, in order to complete continuous monitoring activities, which include annual security control reviews, quarterly vulnerability scanning, monthly review of security access control list, weekly review of audit logs, handling of access change requests and change control board activities. The risk assessment includes the possible threats and vulnerability to the confidentiality, integrity, and availability of mission and sensitive PII data along with the countermeasures.

The controls supporting the use of Microsoft Azure FedRamp approved system as a customer are in place in NOAA6301. There are currently Web applications, with no PII, hosted on Microsoft Azure. As noted in Section 12.2, we are transitioning CSCOR to Azure prior to December 2018. The same sharing controls that are in place currently for CSCOR will apply when it is moved to Azure.

Every year the IT system undergoes a thorough continuous monitoring for the assessment and authorization (A&A) process that is performed by an independent. The A&A process ensures that the security plan and operational, management, and technical controls meet Department of Commerce (DOC) and NOAA guidelines for continued operation.

**Section 9: Privacy Act**

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C.

§ 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

x	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number ( <i>list all that apply</i> ): <a href="#">COMMERCE/DEPT-18</a> - Employees Personnel Files Not Covered By Notices of Other Agencies; <a href="#">DEPT-2</a> , Accounts Receivable; <a href="#">GSA/GOVT-9</a> , System for Award Management.
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created:

**Section 10: Retention of Information**

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

x	<p>There is an approved record control schedule.                  Provide the name of the record control schedule: Chapters 1601 and 1607 of NOAA’s Records Schedules, <a href="http://www.corporateservices.noaa.gov/audit/records_management/schedules/">http://www.corporateservices.noaa.gov/audit/records_management/schedules/</a>, provide supplemental record retention guidance for the NCCOS Research Support System. Chapter 1601 pertains to general administration for the National Ocean Service and Chapter 1607 pertains to specific records managed by the NCCOS Research Support System. Specifically, 1601-02 Grants Working Files (N1-370-02-5), 1601-04 Electronic Copies (N1-370-02-5), 1601-05 NOS Annual Operating Plan (AOP) Information Tracking Systems (N1-370-04-4), 1609-06 in the NOAA Disposition Handbook and 1607-04 Program Funding Database.</p> <p>The retention period for these records is guided by the General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the federal government. In accordance with GRS 20, item 3, electronic versions of records scheduled for disposal may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. In accordance with GRS 20, item 3, the data is presently being retained indefinitely.</p> <p>For NCCOS administrative PII data, the records would be covered under the following NARA general records schedules:                  GRS 2 – payroll and pay administrative records                  GRS 20 – electronic records                  GRS 23 – records common to most offices within agencies</p> <p>NCCOS’ contact information (contractor and partner) is collected to provide a means for the Office of Coast Survey to communicate and respond to needs and requests. This data would be retained as long as the individual continued to request contact and information. It is technologically possible to delete information at the request of the individual. There is no scheduled records retention for this information.</p>
	<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:</p>
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): Compliant sanitization methods.			

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

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

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	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: Evaluated how easily PII could be used to identify a specific individual. Based on contact information, individuals can be identified.
X	Quantity of PII	Provide explanation: Considered how many individuals can be identified from the PII. The PII is only temporarily stored for a limited amount of individuals, therefore reducing the breach impact.
X	Data Field Sensitivity	Provide explanation: Data fields are limited and only used when absolutely required. SSN is not one of these data fields. EIN is a field which can be populated within NOAA Grants Online, however, is not required and is not utilized. This field will not be extracted from NOAA Grants Online in the future revision of the CSCOR Review Application.
X	Context of Use	Provide explanation: Evaluated the context of use—the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated. The use of the PII is restricted to specific individuals, stored for a limited amount of time and is not utilized in more than one way reducing the impact.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: The PII is only temporarily stored in a protected location for a limited amount of individuals, therefore reducing the breach impact.
X	Other:	Provide explanation: The loss of a single individual's PII would have an impact on that individual through possible identify theft and NCCOS as a government identity BUT it would not have an impact on the NCCOS mission or have a serious impact on reputation.

**Section 12: Analysis**

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

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

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

x	Yes, the conduct of this PIA results in required technology changes. Explanation: NOAA6301 is utilizing Azure SQL in the Microsoft Azure PaaS environment to store web application data. Although there is currently no PII/BII associated with the web/apps and transitioning to the new environment is not expected prior to December 2018, controls are already in place to encrypt at rest data through the Azure SQL TDE capability: <a href="https://msdn.microsoft.com/en-us/library/dn948096.aspx">https://msdn.microsoft.com/en-us/library/dn948096.aspx</a> . All SQL databases will have this feature turned on at inception and it will remain on. This storage is currently planned only for CSCOR and will further secure the CSCOR Review Application Database.
	No, the conduct of this PIA does not result in any required technology changes.