

**U.S. Department of Commerce
National Oceanic & Atmospheric Administration**



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

Reviewed by: GRAFF.MARK.HYRUM.151447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2021.02.22 16:13:42 -05'00', 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

GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2021.02.22 16:15:52 -05'00'

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

Date

U.S. Department of Commerce Privacy Impact Assessment

NOAA/NOS/National Centers for Coastal Ocean Science (NCCOS) Research Support System

Unique Project Identifier: NOAA6301

Introduction: System Description

National Centers for Coastal Ocean Science (NCCOS) mission is to deliver ecosystem science solutions for stewardship of the Nation's ocean and coastal resources to sustain thriving coastal communities and economies. NCCOS helps NOAA meet its coastal stewardship and management responsibilities, and provides coastal managers with the scientific information necessary to decide how best to protect environmental resources and public health, preserve valued habitats, and improve the way communities interact with coastal ecosystems.

NCCOS supports 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 *Stressor Impacts & Mitigation (SIM)* program that focuses on ecological forecasting, stressor detection, and an understanding of stressor impacts on coastal resources. NCCOS conducts its research in two SIM sub-priorities:
 - Harmful Algal Blooms
 - Biological Effects of Contaminants and Nutrients
- provides support to the *Marine Spatial Ecology (MSE)* program that integrates a broad spectrum of physical, biological, and social sciences, to inform coastal and marine decision making, and provides unique capabilities to ensure that special places are valued, protected, and preserved, and to assist in growing the economies that are dependent on our nation's maritime resources. NCCOS has identified four MSE sub-priorities:
 - Ecological and Biogeographic Assessments
 - Habitat Mapping
 - Regional Ecosystem Science
 - Coastal Aquaculture Siting and Sustainability
- provides support to the *Coastal Change* program, that seeks to understand the ecosystem services to improve a community's resistance to the impacts of weather and changing climate conditions, and provide timely and actionable scientific assessments, information, and tools

that coastal communities use to make risk management decisions. NCCOS has identified four Coastal Change portfolio sub-priorities:

- Vulnerability and Risk Assessment
- Natural and Nature-Based Features
- Climate Impacts on Ecosystems
- Restoration
- provides support to the *Social Science* programs that focuses on the study of connections between people and the environment and prioritizes investigations into these connections within three interconnected sub-priorities of research:
 - Ecosystem Services Valuation
 - Assessing Human Use
 - Assessing Vulnerability and Resilience
- provides all resources related to data management, electronic file, COTS, printing, computer and software, field data acquisition, backup and restoration, helpdesk, specialty applications for GIS and statistical analysis, moderate programming, Web design and Web product delivery, video conferencing, and other media support services;
- provides LAN and WAN services fully managed by NOAA N-Wave (NOAA0550) for all NCCOS locations. Particularly for Silver Spring MD these services are managed by NOAA0550 through NOAA6001 (NOS).

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.

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

NOAA6301 is a General Support System. NOAA6301 defined as NCCOS Research Support System (N-RSS) is a General Support System for the National Centers for Coastal Ocean Science (NCCOS) Program Office, and provides the infrastructure, hardware and software necessary to enable the mission of NCCOS, the organization.

(b) System location

NOAA6301 has system components in Silver Spring, MD; Charleston, SC; Beaufort, NC; Oxford, MD and Microsoft Azure Cloud.

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

NOAA6301 has interconnections with the following FISMA systems:

- NOAA0100 – NOAA OCIO (NCSC/ESS/NCIRT)
- NOAA0550 – NOAA N-Wave (NOAA Enterprise Network)
- NOAA0700 – NOAA High Availability Enterprise Services (HAES) (EDS/ICAM/NSD)
- NOAA0900 – NOAA Cloud SaaS Applications (ENS/G-Suite/MaaS360/ESRI etc.)

- NOAA6001 – NOS Enterprise Information System

Note: No PII/BII is shared with any of the FISMA systems listed above. NOAA0100, NOAA0550, NOAA0700 and NOAA0900 do not issue interconnection agreements. See available references below. SLAs with NOAA0550 for NCCOS Silver Spring MD location only is managed through NOAA6001, where as for other NCCOS locations (Oxford MD, Beaufort NC and Charleston SC) it is managed by NOAA6301.

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

NOAA6301 is a logical interconnection of system components (Network Devices, Servers, Workstations, Printers, Storage, Applications, Databases and Miscellaneous Devices) residing in four NCCOS research facilities (Silver Spring, MD; Charleston, SC; Beaufort, NC; and Oxford, MD) and in Microsoft Azure Cloud (East US2 and Central US region). Each research facility contributes to the overall mission of the NCCOS Program Office along with unique partnerships and cooperatives established to support and further strategic science goals. The physical and logical connections are managed through NOAA0550 (NOAA N-Wave) and NOAA6001 (NOS Enterprise Information System). All NOAA6301 research facilities are behind NOAA Trusted Internet Connections Access Provider (NOAA N-Wave). Virtual Routing & Forwarding (VRFs) allow for both the internet connections and private network connections, which is managed through NOAA6001 by NOAA0550. All NOAA6301 on-prem IT components exist behind firewalls or on firewalled networks. NOAA6301 IT components in Microsoft Azure Cloud are configured utilizing Azure identity management and networking features but are currently not TIC compliant (work in progress with NOAA N-Wave). NOS domain services are implemented entirely within the security boundary provided by NOAA6001. NOAA6301 follows the Firewall Policy as defined by NOAA6001. VPN services are provided by the NOAA0550 through the management of NOAA6001. Private IP address space is supported by network address translation. This level consists of devices which can initiate connections to outside networks. No public access to the private network is permitted. Direct inbound access from the Internet is not allowed. The public network is designed to support services that must be accessible to NOAA collaborators and partners outside the Trusted Private Network. All NOAA6301 applications (except COTS Helpdesk Track-It System) and databases are hosted in Microsoft Azure Cloud utilizing Platform-as-a-Service (PaaS) deployment model.

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

Access to all information (including limited PII/BII) is stored on restricted access file storage available only to the specific employee(s) following principle of least privilege, separation of duties and on a need to know basis, by permissions settings and/or passwords. Any data stored on a laptop, is encrypted utilizing full device encryption. NOAA/NCCOS public-facing websites accessible to the general public provide information meant for public to use.

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

Scientific information is collected from scientific equipment, other government/non-government entities and partners and from the field. All information is scanned prior to being stored on restricted file storage and transmitted only using NOS/NOAA/DOC managed enterprise solutions (e.g. NOAA Google Suite, DOC Accellion KiteWorks, NOS File Storage, NOAA-managed FTP, NCCOS/NOAA Websites etc.). As a part of the HR, Acquisition and Badging process sensitive information containing PII/BII is transmitted

(only if needed) securely only to the concerned via DOC-managed secure file collaboration tool (*Accellion Kiteworks*).

(g) Any information sharing conducted by the system

In the event of a security incident involving privacy, information will be shared with NOAA N-CIRT and if required with DOC and other federal agencies (e.g., Department of Justice). Just like DOC, NOAA and NOS internal/public-facing websites, NCCOS internal/public-facing websites also have photographs of NCCOS staff involved in research and/or educational programs/activities, voluntarily submitted with implied consent to serve a purpose, reviewed, verified and managed through NCCOS website content managers prior to publishing them on the websites. Publicly accessible information is shared via NCCOS/NOAA public facing websites.

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

- 5 U.S.C. § 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.
- 5 USC 552a (b) & (e)(3) – Records Maintained On Individuals, (b) Conditions Of Disclosure and (e)(3) Agency Requirements
- 15 CFR Part 4 Subpart A § 4.1-4.11 – Freedom of Information Act (FOIA)
- 15 CFR Part 4 Subpart B § 4.21-4.34 – Privacy Act
- 15 U.S.C CHAPTER 91 – Children's Online Privacy Protection (COPPA)
- 16 CFR Part 312 – Children's Online Privacy Protection (COPPA) Rule
- 15 U.S.C. § 1512 is an Organic Law which confers general powers and duties authority to executive agencies, vesting jurisdiction and control of departments, bureaus, offices and branches.
- *Authorities from DEPT-2:* 28 U.S.C. 3101-3105, Debt Collection Act of 1982 (Pub. L. 97-365); 26 U.S.C. 6402(d); and 31 U.S.C. 3711.
- *Authorities from DEPT-6:* 5 U.S.C. 301; 44 U.S.C. 3101.
- *Authorities from DEPT-9:* Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966.
- *Authorities from 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; and Equal Employment Act of 1972.
- *Authorities from DEPT-18:* 5 U.S.C. 301; 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.
- *Authorities from DEPT-29:* Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (Feb. 15, 2015); National Marine Sanctuaries Act, 16 U.S.C. 1431 et seq.; Marine Debris Act, 33 U.S.C. 1951 et seq.; Coast and Geodetic Survey Act, 33 U.S.C. 883a et seq.; Coastal Zone Management Act, 16 U.S.C. 1451 et seq.; Coral Reef Conservation Act, 16 U.S.C. 6401 et seq.; National Historic Preservation Act, 16 U.S.C. 470 et seq.; Ocean Pollution Act, 33 U.S.C. 2701 et seq.; Comprehensive Environmental Response, Compensation and Liability Act, 42 U.S.C. 9601 et seq.; Clean Water Act, 33 U.S.C. 1251; 47 CFR parts 80, 87, and 95. The system is also authorized by the U.S. Office of Management & Budget (OMB) Circular A-130; the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 et seq. (Magnuson-Stevens Act); High Seas Fishing Compliance Act of 1995, 16 U.S.C. 5501 et seq.; International Fisheries Regulations: Vessels of the United States Fishing in Colombian Treaty Waters: 50 CFR 300.120; the FAA Modernization and Reform Act of 2012 (Pub. L. 112-95); the American Fisheries Act, Title II, Public Law 105-277; the Atlantic Coastal Fisheries Cooperative

Management Act of 1993, 16 U.S.C. 5101–5108, as amended 1996; the Tuna Conventions Act of 1950, 16 U.S.C. 951–961; the Atlantic Tunas Convention Authorization Act, 16 U.S.C. Chapter 16A; the Northern Pacific Halibut Act of 1982, 16 U.S.C. 773 et seq. (Halibut Act), the Antarctic Marine Living Resources Convention Act of 1984, 16 U.S.C. 2431–2444; the Marine Mammal Protection Act, 16 U.S.C. 1361; and the Debt Collection Improvement Act, 31 U.S.C. 7701.

- *Authorities from GSA-GOVT-9:* For the Entity Management functional area of SAM, 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 are FAR Subparts 9.4 and 28.2, Executive Order 12549 (February 18, 1986), Executive Order 12689 (August 16, 1989).
- *Authorities from GSA-GOVT-10:* E-Government Act of 2002 (Pub. L. 107–347) Section 204; Davis-Bacon and Related Acts: 40 U.S.C. 3141–3148 40 U.S.C. 276a; 29 CFR parts 1, 3, 5, 6 and 7; Section 5 of the Digital Accountability and Transparency Act (DATA Act), Public Law 113–101.

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

FIPS 199 Security Categorization of 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): N/A			

- 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 or 01-2017).
- 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 01-2019 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.)

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport	X	k. Financial Transaction	
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify): N/A					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: N/A					

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

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address	X	g. Work History	X	k. Procurement/contracting records	X
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		
l. Other work-related data (specify): N/A					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording	X	i. Height		n. Retina/Iris Scans	
e. Photographs	X	j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify): N/A					

NOAA6301 Comments: Unintentional/accidental collection of PII may occur during the utilization of NOAA-approved Uncrewed Aerial Systems (UAS) for NCCOS's coastal ecology research activity to collect imagery and spatial data in remote areas with uneven topography and/or for measuring the performance of Natural and Nature Based Features (NNBF). As a part of post-flight procedures, data collected is reviewed and PII if identified any is deleted immediately. NCCOS adheres to the privacy requirements established by *NOAA UAS Privacy Policy* at all times. No PII will be collected utilizing NOAA-approved UAS without prior notice covering the purpose of the collection and the use of identifiable information will be provided. Information from video surveillance and building

card readers is temporarily acquired as a part of facilities safety and security process/procedures is stored within NCCOS Facility Access Control Systems (ACS), accessible only to authorized Facility Managers, to support incident response and review process and is deleted immediately (if not related to any security incidents) after review. Just like DOC, NOAA and NOS internal/public-facing websites, NCCOS internal/public-facing websites also have photographs of NCCOS staff involved in research and/or educational programs/activities, voluntarily submitted with implied consent to serve a purpose, reviewed, verified and managed through NCCOS website content managers prior to publishing them on the websites. NCCOS staff can anytime request the removal/update of a photograph through NCCOS website content managers.

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

Other Information (specify)
Pre and Post Acquisition. BII information would be obtained and utilized during the pre/post acquisition activities 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.)

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

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

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

NOAA6301 Comments: 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 Describe how the accuracy of the information in the system is ensured.

Accuracy of the information in the system is ensured through access control mechanisms (ensuring the confidentiality of the data) and proper handling/storage techniques and methods (ensuring the integrity of the data).
--

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 Number: 0648-0342, NOAA Website Satisfaction Survey - OMB Control Number: 0648-0308, 2006 NOAA Coastal Services Center Coastal Resources Management Customer Survey renewal
	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.)

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

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

Section 3: System Supported Activities

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

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

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

NOAA6301 Comments: Unintentional/accidental collection of PII may occur during the utilization of NOAA-approved Uncrewed Aerial Systems (UAS) for NCCOS’s coastal ecology research activity to collect imagery and spatial data in remote areas with uneven topography and/or for measuring the performance of Natural and Nature Based Features (NNBF). As a part of post-flight procedures, data collected is reviewed and PII if identified any is deleted immediately. Information from video surveillance and building card readers is temporarily acquired as a part of facilities safety and security process/procedures, and is stored within NCCOS Facility Access Control Systems (ACS) as a part of facilities safety and security process/procedures to support incident response and review process. The information is accessible only to authorized Facility managers and is deleted (if not related to any security incident) immediately after review.

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	
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)	X
Other (specify): N/A			

NOAA6301 Comments: BII would be collected as a part of pre/post acquisition activities and information extracted from *NOAA Grants Online (NOAA1101)* system to support NCCOS Grants Management Program. PII would be collected for administrative actions, for HR and Workforce management.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO. The Federal CIO provides the mandate (<https://policy.cio.gov/web-policy/analytics>) to use tier-2 multi-session cookies and/or other technologies for tracking analytics, and states:

- All agencies must participate in the General Service Administration’s (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs; and
- Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies;

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).

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.

PII Information (from video surveillance and building card readers) temporarily acquired as a part of facilities safety and security process/procedures is stored within NCCOS Facility Access Control Systems (ACS), accessible only to authorized Facility Managers, to support incident response and review process and is deleted immediately (if not related to any security incidents) after review.

Imagery and spatial data is collected from the utilization of NOAA-approved Uncrewed Aerial System (UAS) for conducting coastal ecology research in remote areas with uneven topography and/or for measuring the performance of Natural and Nature Based Features (NNBF) such as salt marshes, nearshore subtidal habitats, emergent vegetation, elevation and nearshore vegetative communities). The data collected is reviewed as a part of post-flight procedures and any unintentional/accidental collection of PII is deleted immediately. NCCOS adheres to the privacy requirements established by *NOAA UAS Privacy Policy* at all times. No PII will be collected utilizing NOAA-approved UAS without prior notice covering the purpose of the collection and the use of identifiable information will be provided.

Just like DOC, NOAA and NOS internal/public-facing websites, NCCOS internal/public-facing websites also have photographs of NCCOS staff involved in research and/or educational programs/activities, voluntarily submitted with implied consent to serve a purpose, reviewed, verified and managed through NCCOS website content managers prior to publishing them on the websites. NCCOS staff can anytime request the removal/update of a photograph through NCCOS website content managers.

BII information would be obtained and utilized during the pre/post acquisition activities (obtained through deliverable BIDS package and contain specific company information) and from information extracted via *NOAA Grants Online system* (NOAA1101) to support NCCOS Grants Management Program. 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.

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.)

Potential threats to privacy as a result of use of NCCOS’s use of information would come from improper handling, retention, sanitization and/or disposal of data. This is mitigated by ensuring that all NCCOS staff completes the mandatory annual IT security awareness training. DOC Access & Use Policy (DOC IT Security Baseline Policy Annex C-8), NOAA Rules of Behavior, NOAA Rules of Behavior for Mobile Devices, and User agreements as well outline the acceptable use and handling of information. Proper sanitization and destruction of media is ensured following NOAA media sanitization processes.

Section 6: Information Sharing and Access

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

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

* Just like DOC, NOAA and NOS internal/public-facing websites, NCCOS internal/public-facing websites also have photographs of NCCOS staff involved in research and/or educational programs/activities, voluntarily submitted with implied consent to serve a purpose, reviewed, verified and managed through NCCOS website content managers prior to publishing them on the websites.

** During a security incident involving privacy

	The PII/BII in the system will not be shared.
--	---

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:</p> <p>NOAA6301 connects to the NOS Line Office information system NOAA6001 and other NOAA information systems (NOAA0100, NOAA0550, NOAA0700 and NOAA0900) for VPN, IT, Security and Network Operations. NCCOS has 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> <p>NOAA6301 receives BII when information is extracted from <i>NOAA Grants Online</i> (NOAA1101) system to support NCCOS Grants Management Program.</p>
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 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): N/A			

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:</p> <ul style="list-style-type: none"> https://coastalscience.noaa.gov/privacy-policy/

	<ul style="list-style-type: none"> • https://oceanservice.noaa.gov/privacy.html • https://www.noaa.gov/protecting-your-privacy
X	<p>Yes, notice is provided by other means.</p> <p>Specify how: PII: Individuals are verbally informed by administrative staff or supervisor that they can decline to provide voluntary PII (including information captured via video surveillance supporting facility safety procedures) and/or are directed to review the NOAA/NOS/NCCOS privacy policies at the below addresses where it is stated that all information collected is voluntary:</p> <ul style="list-style-type: none"> • https://coastalscience.noaa.gov/privacy-policy/ • https://oceanservice.noaa.gov/privacy.html • https://www.noaa.gov/protecting-your-privacy <p>Video surveillance warning and/or notice signs are also posted at entry/exit points. No PII is collected utilizing NOAA-approved UAS. Just like DOC, NOAA and NOS internal/public-facing websites, NCCOS internal/public-facing websites also have photographs of NCCOS staff involved in research and/or educational programs/activities, voluntarily submitted with implied consent to serve a purpose, reviewed, verified and managed through NCCOS website content managers prior to publishing them on the websites.</p> <p>BII is provided for the purpose of acquisition consideration through government managed acquisition processes and forms only. BII received when information is extracted from <i>NOAA Grants Online</i> system is not mandatory and can be restricted at NOAA level. NCCOS does not generate or maintain additional forms or processes to support acquisition and grant related activities.</p>
	<p>No, notice is not provided.</p> <p>Specify why not:</p>

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

X	<p>Yes, individuals have an opportunity to decline to provide PII/BII.</p> <p>Specify how: PII: Individuals are verbally informed by administrative appointed staff or supervisor that they can decline to provide voluntary PII (including information captured via video surveillance supporting facility safety procedures) and/or are directed to review the NOAA/NOS/NCCOS privacy policies at the below addresses where it is stated that all information collected is voluntary:</p> <ul style="list-style-type: none"> • https://coastalscience.noaa.gov/privacy-policy/ • https://oceanservice.noaa.gov/privacy.html • https://www.noaa.gov/protecting-your-privacy <p>Video surveillance warning and/or notice signs are also posted at entry/exit points. No PII is collected utilizing NOAA-approved UAS. NCCOS staff can anytime request the removal/update of a photograph, voluntarily submitted by them with implied consent in the past and still published on NCCOS internal/public-facing websites, through NCCOS website content managers.</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. BII received with information extracted from <i>NOAA Grants Online</i> system is not mandatory and can be restricted at NOAA level. NCCOS does not generate or maintain additional forms or processes to support acquisition and grant related activities.
	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: Individuals and/or Applicants have the opportunity to consent to only particular uses of their PII (including information captured via video surveillance supporting facility safety procedures), in writing, to the administrative staff or HR representative or their supervisor. If a request to collect PII is declined, then, it may affect the overall processing of their employment or access to certain services may be limited or denied. There is only one specific use for each PII collection. No PII is collected utilizing NOAA-approved UAS. Just like DOC, NOAA and NOS internal/public-facing websites, NCCOS internal/public-facing websites also have photographs of NCCOS staff involved in research and/or educational programs/activities, voluntarily submitted with implied consent to serve a purpose, reviewed, verified and managed through NCCOS website content managers prior to publishing them on the websites. For BII received as a part of pre/post acquisition activities, consent is implied with the submittal of the acquisition package. BII received with information when extracted from <i>NOAA Grants Online</i> system, consent is implied with the submission of information under the NOAA Grants Management Program.
	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: PII: Individuals or NCCOS employees can contact administrative/HR staff or the federal employee personnel page to update the PII information as it was submitted and also provide the reason for review or update. Information captured via video surveillance and supporting facility safety procedures is only stored temporarily and is deleted immediately after review by facility managers. No PII is collected utilizing NOAA-approved UAS. NCCOS staff can anytime request the removal/update of a photograph, voluntarily submitted by them
---	---	--

		<p>with implied consent in the past and still published on NCCOS internal/public-facing websites, through NCCOS website content managers.</p> <p>BII is provided for the purpose of acquisition/grants through government-managed acquisition/grants processes and forms only. NCCOS does not generate or maintain additional forms or processes to support acquisition activities.</p> <p>Regarding contracts that are in process or awarded, the applicants 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	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access to storage folders are restricted by ACLs but since PII/BII is not centralized in a database it cannot be easily monitored for access.
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>1/29/2021</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
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. *(Include data encryption in transit and/or at rest, if applicable).*

<p>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</p>

authorization and mission ‘need-to-know’ requirement prior to implementation. Separation of Duties and 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 Kiteworks 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.

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

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

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

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

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

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. (<i>list all that apply</i>): DEPT-2 , Accounts Receivable; DEPT-6 , Visitor Logs and Permits for Facilities Under Department Control; DEPT-9 , Travel Records (Domestic and Foreign) of Employees and Certain Other Persons; DEPT-13 , Investigative and Security Records; DEPT-18 , Employees Personnel Files Not Covered By Notices of Other Agencies; DEPT-29 , Unmanned Aviation Systems; GSA/GOVT-9 , System for Award Management; GSA/GOVT-10 , FAR Data Collection System;
	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>Chapters 1601 and 1607 of NOAA’s Records Schedules, 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>Chapter 2200 (Records of the Chief Information Officer) of NOAA’s Records Schedules, provides disposal authorization for certain records created and maintained by Federal Chief Information Officers (CIO) and their program offices.</p> <p>Chapter 2300 (General Information Technology Management Records) of NOAA’s Records Schedules, provide guidance on records created and maintained by NCCOS Research Support System and related to technology management, system development and system maintenance.</p> <p>Chapter 2400 (Information System Security Records) of NOAA’s Records Schedules, provide guidance on records created and maintained by NCCOS Research Support System and related to protecting the security of IT systems and data, and responding to computer security incidents.</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) (see https://www.archives.gov/records-mgmt/grs.html) to provide disposition authorization for records common to several or all agencies of the federal government. In accordance with NARA GRS Title 3.1, 3.2, 4.1, 5.1 and 5.2 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.</p> <p>In accordance with NARA GRS Title 3.1, 3.2, 4.1, 4.2, 5.1 and 5.2, 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:</p> <ul style="list-style-type: none"> • 3.1 General Technology Management Records • 3.2 Information Systems Security Records • 4.1 Records Management Records • 4.2 Information Access and Protection Records • 5.1 Common Office Records • 5.2 Transitory and Intermediary Records
	<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	<p>Yes, retention is monitored for compliance to the schedule.</p>
	<p>No, retention is not monitored for compliance to the schedule. Provide explanation:</p>

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

Disposal			
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.
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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: Evaluated how easily PII could be used to identify a specific individual. Based on information collected through video surveillance (stored temporarily), contact information and/or photographs published on NCCOS websites, 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.
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 from video surveillance (acquired temporarily as a part of facility safety/security and Incident Response process/procedures) and contact information (acquired for administrative, HR, badging and/or COOP purposes), is restricted to specific individuals, stored for a limited amount of time reducing the breach impact. Just like DOC, NOAA and NOS internal/public-facing websites, NCCOS internal/public-facing websites have photographs of NCCOS staff involved in research and/or educational programs/activities, voluntarily submitted with implied consent to serve a purpose, reviewed, verified and managed through NCCOS website content managers prior to publishing them on the websites.
	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. Information from video surveillance is also stored temporarily within the facility access control systems with access restricted to facility managers only and deleted immediately after review. Photographs of NCCOS staff involved in research and/or educational programs/activities, voluntarily submitted by them with implied consent to serve a purpose on NCCOS internal/public-facing websites is reviewed, verified and managed through NCCOS website content managers prior to publishing them on the websites. NCCOS staff can anytime request the removal/update of a photograph through NCCOS website content managers.
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 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.)

NCCOS primary mission is to support NOAA’s environmental and economic missions by providing valuable scientific information to its constituents.

NCCOS utilizes the NOAA Office of Human Capital Services and collects, stores and maintains employee data for internal COOP, Human Resources, and workforce planning purposes only. NCCOS collects BII during the pre and post activities associated with the acquisition and management of contracts.

Potential threats that exist for information collected include data exfiltration and improper handling, retention, sanitization and/or disposal of data.

NCCOS follows and implements principle of least privilege and separation of duties (RBAC) in combination with rule-based access control. Only authorized individuals with a need to know will have access to data.

All NCCOS components are configured following secure baselines and are continuously monitored through weekly/monthly vulnerability scans and log reviews. All NCCOS staff completes the mandatory IT security awareness training every year.

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

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

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

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