

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



Privacy Impact Assessment
for the
NOAA6001
National Ocean Service Enterprise Information System (NOSEIS)

Reviewed by: Robin Burress for 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

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2025.06.10 12:44:57 -04'00'

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

Date

U.S. Department of Commerce Privacy Impact Assessment NOAA/NOS/Enterprise Information System (NOSEIS)

Unique Project Identifier: NOAA6001

Introduction: System Description

Provide a brief description of the information system.

The National Ocean Service Enterprise Information System (NOSEIS); identified as NOAA6001, is classified as a general support system. The NOAA6001 system is a collection of integrated components, consisting of hardware, software, data, telecommunications and personnel that is architected for providing the National Ocean Service (NOS) organization IT services. NOAA6001 provides NOS staff and program offices technology-based solutions for logical access control, office automation, network connectivity, data storage, and various cloud-based services.

The NOAA6001 system is utilized for collecting and processes Controlled Unclassified Information (CUI), Business Identifiable Information (BII) and Personally Identifiable Information (PII) information types on behalf of Assistant Administrator and Management and Budget (AAMB) and U.S. Integrated Ocean Observing System (IOOS), in support of business functions and coastal economies and their contribution to the national economy and advancing the priorities of the NOS. For information that clarifies the priorities of NOS program and staff offices for which NOAA6001 is architected to support, navigate to <https://oceanservice.noaa.gov/programs/welcome.html>.

Address the following elements:

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

NOAA6001 is classified as a general support system.

(b) System location

The components of the NOAA6001 system are physically and logically located both in contiguous United States (CONUS) and outside the contiguous United States (OCONUS) locations. The CONUS locations include the Silver Spring Metro Campus (SSMC) buildings in Silver Spring, MD, the NOAA Enterprise Data Center (EDC), in Ashburn, VA, and several NOS program office locations. The OCONUS locations comprise of network infrastructure components that provide connectivity to NOS program and staff offices.

NOAA6001 system component locations:

- NOAA Government Building, Norfolk, VA 23510
- Avaya, Columbia, MD 21046
- Channel Islands National Marine Sanctuary, Santa Barbara, CA 93101
- Cordell Bank National Marine Sanctuary, Point Reyes Station, CA 94956
- NOAA Enterprise Data Center (EDC), Ashburn, VA, 20147

- Nancy Foster Florida Keys Environmental Complex, Key West, FL 33040
- Key Largo Office, Key Largo, FL 33037
- NOAA Restoration Center, Galveston, TX 77551
- GovDelivery Communications Cloud (GovDelivery) Software as a Service (SaaS), Saint Paul, MN 55102
- Gray's Reef National Marine Sanctuary, Savannah, GA 31411
- Greater Farallones National Marine Sanctuary, San Francisco, CA 94129
- Hawaiian Islands Humpback Whale National Marine Sanctuary, Kihei, HI 96753
- Monitor National Marine Sanctuary, Newport News, VA 23606
- Monterey Bay National Marine Sanctuary, Monterey, CA 93940
- National Centers for Coastal Ocean Science (NCCOS) Beaufort Laboratory, Beaufort, NC 28516
- Hollings Marine Laboratory (HML), Charleston, SC 29412
- Cooperative Oxford Laboratory, Oxford, MD 21654
- Adobe, San Jose, CA 95110
- Microsoft Azure Central, VA
- Microsoft Azure East, VA
- Microsoft Azure East 2, VA
- Microsoft Azure West, CA
- NOS SSMC 3, Silver Spring, MD 20910
- NOS SSMC 4, Silver Spring, MD 20910
- Office for Coastal Management (OCM) Charleston Office, Charleston, SC 29405
- Olympic Coast NMS Headquarters, Port Angeles, WA 98362
- Papahānaumokuākea Marine National Monument, Hilo, HI 96720
- Stellwagen Bank National Marine Sanctuary, Scituate, MA 02066
- Thunder Bay National Marine Sanctuary, Alpena, MI 49707
- NOAA Western Regional Center, Seattle, WA 98115

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

NOAA6001 is interconnected with the following systems in concurrence with CSAM:

- NOAA N-Wave (NOAA0550)
- NOAA Cyber Security Center (NCSC) (NOAA0100)
- Office of Coastal Management General Support System (NOAA6101)
- Center for Operational Oceanographic Products and Services (CO-OPS) PORTS and NWLON (NOAA6205)
- National Centers for Coastal Ocean Science Research Support System (NOAA6301)
- National Geodetic Survey (NGS) General Support System (NOAA6401)
- Office of Coast Survey (OCS) Nautical Charting System (NOAA6501)
- Office of National Marine Sanctuaries (ONMS) (NOAA6602)
- Office of Response and Restoration (OR&R) Local Area Network (NOAA6701)
- NOAA EDC (NOAA0520)
- NOAA Consolidated Cloud Applications (NOAA0900)

NOAA6001 implements NIST Moderate level physical, technical and administrative controls for protecting interconnected system communication and data.

NOAA6001 information system assets are protected in organizational facilities that employ card readers and additional accesses restrictions based on a need-to-know and/or business requirement (physical access control list). Building card readers are under the control of the Department of Commerce (DOC) Office of Security (OSY) and this information is not stored within the boundary of NOAA6001.

Logical access control is facilitated by established access control lists (ACL), enforcing authorized access for subjects and objects. These ACLs are architected to prevent unauthorized accesses for all data types, including CUI, PII and BII. In addition, NOAA6001 leverages data loss prevention tools provided at the NOAA level to assist mitigating potential spillage of sensitive CUI/PII/BII through NOAA Data Loss Prevention tool (DLP).

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

The Information System Manager (ISM) for NOAA6001 also serves as Chief Technology Officer (CTO) for the NOS. The responsibility of the ISM is to oversee and manage the day-to-day operation of NOAA6001.

The operations manager for NOAA6001 is tasked with supervising the Domain Infrastructure Team (DIT) activities and responsible for overseeing operations and maintenance of the NOAA6001 enterprise services and systems.

The network manager for NOAA6001 is tasked with supervising not only the activities of the Network Infrastructure Team (NIT) and the network infrastructure for NOAA6001, but overseeing some elements of the network infrastructure for the NOS.

The NIT is tasked with managing the NOS network infrastructure, ensuring network connectivity and its operation. This is an enterprise-level responsibility of NOAA6001. The NIT responsibility is all aspects of managing the NOS network including configuration management, tuning, troubleshooting and installation and maintenance activities for the network infrastructure.

The DIT is tasked with managing the operation of the various NOS enterprise services (e.g., identity management, Windows & MacOS configuration management, Windows & MacOS patch management, data storage, data backup and anti-virus) supporting on-premise and cloud solutions that consist of server, specialized appliances, enterprise Windows & MacOS systems configuration and patch management services and endpoint security components residing within NOAA6001 boundary. DIT responsibilities include all aspects of on-premise and cloud system administration and management for servers, enterprise Windows & MacOS systems configuration and patch management services, identity management (e.g., on-premise Active Directory (AD), Azure AD), printer management, database services, storage and backup services and endpoint security (e.g., anti-virus, anti-malware, DLP).

The NOS Help Desk is tasked with providing NOAA6001 users with Windows and MacOS endpoints technical assistance and troubleshooting. NOS Help Desk is responsible for all aspects of user and endpoint authentication, endpoint troubleshooting,

endpoint deployment, endpoint system administration, endpoint configuration management, endpoint patch management and endpoint vulnerability remediation.

The following technologies are the major components of the NOAA6001 information system:

- Microsoft Azure Commercial Cloud (Azure) is a FedRAMP Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) cloud computing platform that enables the back-end infrastructure supporting NOS-related mission/business content. Azure also serves the organization as the long-term and offsite data storage solution.
- GovDelivery Communications Cloud (GovDelivery) is a FedRAMP approved SaaS subscription that provides the Communication and Education Division (CED) with optimized features that facilitate efficient communications of information to the general public. Access to manage data and its content is limited to only CED employees. GovDelivery is used by CED to deliver email, campaigns and Short Message Service (SMS) content to government and non-government users that have specifically requested NOS content. GovDelivery is only accessible by NOAA6001 authorized users. CED leverages GovDelivery for processing and transmitting PII containing email addresses of users requesting NOS content.
- Adobe Connect is a SaaS application managed and used by CED for recording video conferences (e.g., NOS All Hands meetings, etc.) and sharing/streaming CED developed video/audio content that supports NOS-related mission/business goals. The application can receive data via upload into an interface that then is capable of being displayed during the teleconference. The information processed by the application and transmitted in video format is for both internal (bureau) and external (public) consumption. PII/BII in the form of digital images, audio/video is transmitted by the application.
- The CED is authorized to develop and post NOS and NOAA related information onto publicly accessible information systems (e.g., NOS web site(s)) and social media platforms (e.g., Facebook, VIMEO, Twitter/"X", Flickr, Instagram, YouTube). Digital files are produced and can be obtained by vetted partners of the organization (e.g., museums, science foundations). CED developed content is made available on interactive kiosks owned/operated by non-NOAA entities that reside at remote locations around the world and facilitates public consumption of CED outreach programmatic information. The physical devices (kiosks) presenting this information do not reside within NOAA6001, but are under the control of the local institution partnered with CED. These systems display organizational BII/PII information types in the form of images and audio/video formats authorized for public consumption.
- Digital data storage services provided by NOAA6001 to NOS program and staff offices is delivered via network connectivity to the Cohesity DataProtect application. Cohesity is an appliance that leverages software-defined solution for protecting and digitally storing NOS data. The enclave operates on a cluster of virtualized hosts managed by the DIT. Cohesity provides short term storage, recovery vitality in the event of a disruption and serves as the conduit for the long-

term storage service provided by the Commercial Azure component of NOAA6001. The Quantum StorNext (Quantum) combines a Storage Area Network (SAN) file system with a policy-based storage manager that provides access, management and protection of digital media data.

- The Quantum Corporation's CatDV solution is an internal digital asset management and workflow platform that provides asset management, cataloging, video workflow automation, and collaboration to NOAA's video production teams. CatDV is our internal video catalog and stores all video production assets, including thumbnails, audio, project files and their associated metadata. CatDV also stores information pertaining to rights management associated with clips such as copyright or source of stock footage. This enables optimization of media analysis and custom search engines of very large databases. CatDV only stores data associated with video production assets (title, description, location, summary, etc.). This also provides full audit capability, analytics, and asset control rules for digital media data.
- Avaya Cloud Secure (Avaya) is a Federal Risk and Authorization Management Program (FedRAMP) approved SaaS subscription that provides the NOS basic Voice over Internet Protocol (VoIP), Voice Messaging, Instant Messaging, mobility support and some audio conferencing.
- The U.S. Integrated Ocean Observing System (IOOS) Ocean Enterprise Study consists of a contractor to originally develop and maintain two spreadsheets. The first spreadsheet contains details of 2020 Ocean Enterprise survey respondents and the information they provided in their survey instrument (PRA OMB Control # 0648-0712) responses. The second spreadsheet comprises details of businesses determined to be active in the provision of Ocean Enterprise products and services together with details concerning their business activity collated from their websites and from other public (e.g., USASpending.gov, www.thomasnet.com, market and analyst reports and generalized web research, email blasts/newsletters/websites Ocean Enterprise relevant organizations) and proprietary sources (e.g., Ocean Enterprise related conferences, IOOS presentations at relevant events, ERISS Corporation research team, IOOS personnel), which is used as the list of individuals receiving the email the complete the optional Ocean Enterprise survey.
- The Cisco Webex Meetings is a cloud-based and video conferencing solution managed and used by IOOS for recording audio, any screen shared (i.e., slides) images and chat logs including names that appear in chat (e.g., IOOS Advisory Committee Public Meeting, etc.) and that supports NOS-related mission/business goals. Webex Meetings service receives and transmits audio and video information during the teleconference. The recordings only capture PII of federal staff and contractors or a speaker's prepared presentation; the recording feature is turned off before the public may provide comments. The information is processed by the application and transmitted in video format for internal (bureau) consumption. Written consent will be collected from the owner of any slides that are being recorded. NOAA is in the process of creating a records retention schedule for Webex recordings. Once the retention schedule has been completed and approved by the National Archives and Records Administration (NARA), all

audio, any screen shared (i.e., slides) images and chat log recordings from WebEx will be deleted as soon as the minutes have been completed and certified for the Federal Advisory Committee Act (FAC) meetings. Internal office presentation videos will be retained for one year before being deleted. Until the retention schedule is approved by NARA, all records must be treated as permanent.

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

- Microsoft Azure Commercial Cloud: AAMB federal and contractor employees that possess privileged level access can retrieve information by leveraging logical access applied to the Azure environment.
- Websites: AAMB federal and contractor employees that possess privileged and non-privileged access can retrieve information by leveraging logical access within the Google Sites environment. Google Sites functionality and hosting resides within the boundary of NOAA0900. This system is not a child system of NOAA6001 and is described as an accessible resource by AAMB employees, utilizing services for uploading mission-related CUI/BII/PII data types to Intranet websites. Non-privileged individuals are only NOAA federal and contractor employees who do possess the ability to change content hosted by Google Sites. These internal facing websites possess CUI/BII/PII in the form of names, email addresses and images. These websites are not publicly facing/accessible. These websites possess CUI/BII/PII in the forms of names, email addresses and images. Similar to the internal facing websites, the Google website function is managed by NOAA0900 and the content hosted on the websites is managed by NOAA6001.
- GovDelivery Communications Cloud: AAMB federal and contractor CED employees that possess privileged access can retrieve information by leveraging logical access enforced by Max.gov, for accessing the SaaS. The data stored within the application is only accessible to privileged users that must be connected to the NOAA6001 network for access. The application contains BII/PII in the form of email addresses. Non-privileged individuals (i.e., public) are not capable of accessing the application.
- Adobe Connect: AAMB federal and contractor employees that possess privileged access can access information by leveraging logical access controls provided by the service. NOS federal and contractor employees that possess non-privileged with read only access and view information by participating in the meetings/webinars being recorded by the application. The application records information from NOS all hands meetings and webinars and could present BII/PII in the form of names, email addresses, images and digital audio and video recordings of stakeholders talking about NOS-related topics. The application back end is not publicly accessible; however, the content is shared publicly via social media and other publicly accessible platforms (i.e., YouTube). NOAA6001 transferred NOAA6001 public access information to NOAA6301 managed web sites, which facilitates uploading NOAA6001 public information to the NOAA6301 hosted web sites and to the above identified commercial social media sites.
- Kiosks: AAMB federal and contractor employees that possess privileged account

access to the Kiosks Management Console can manage information and content made available to the kiosks. Access to the content is controlled by CED and non-privileged individuals (e.g., public), are permitted view only access when the content is presented on the digital kiosk. The kiosks display BII/PII in the form of digital images and audio and videos recordings of NOS federal and contractor employees that are speaking to NOS-related topics.

- Government Furnished Equipment (GFE): AAMB federal and contractor employees are issued GFE client systems (e.g., laptops and mobile devices) for the purpose of performing assigned roles and responsibilities in support of NOS mission and business functions. The GFE component enables AAMB employees the ability to access NOAA6001 resources based on role-based access controls. CUI/PII/BII can be stored on local hard drives of these systems.
- Enterprise storage (Cohesity) and databases are data management components, that support some NOS staff and program offices. The Cohesity application and databases provide data storage and short-term backup of data. Access to the components is enforced utilizing a role-based access schema. Only staff and program office employees that possess authorization, are capable of accessing data. This action can be performed using a GFE. Privileged access to both components is limited to the DIT. CUI/BII/PII could be in the form of email addresses, names and digital audio and videos recordings of stakeholders talking about NOS-related topics, human resources data, credit card information, passport information, contracting data, etc. Refer to the information types listed in section G of this document.
- Avaya Cloud Secure (Avaya) is a FedRAMP approved SaaS subscription that provides basic VoIP, Voice Messaging, Instant Messaging, mobility support to various personnel devices, and Collaboration including basic and advanced audio and web conferencing. PII/BII can be relayed via audio and video conversations.
- Social media: Social media services are leveraged by staff and program office business units for the purpose of extending a communications and outreach platform. These are services that relay information to the public for purpose of information sharing and consumption. Some of this information could be in the form of non-sensitive BII and PII. These resources do not operate or reside within the boundary of NOAA6001.
- IOOS Ocean Enterprise Study spreadsheets are restricted to IOOS federal and contractor personnel. The contractor performs manual collection and incorporates into the content into the appropriate spreadsheets that is shared with IOOS. The results from SurveyMonkey are restricted to IOOS contractor developing the report. Final IOOS Ocean Enterprise Study are posted to <https://ioos.noaa.gov/project/ocean-enterprise-study/>.

- The Cisco Webex Meetings recordings/videos are only available to IOOS federal and contractor employees who possess privileged access. The application back end is not publicly accessible and the content of the recordings are not shared outside of IOOS federal and contractor employees who possess privileged access. The application records information from IOOS Advisory Committee Public Meetings and could present BII/PII in the form of audio, any screen shared (i.e., slides) images and chat logs, including names that appear in chat of stakeholders talking about NOS-related topics. Written consent will be collected from the owner of any slides that are being recorded.

Manual collection and storage of PII/BII by AAMB employees:

- The BII/PII is collected to support the Planet Stewards Education Project. The PII collected as part of this effort consists of individual and business names, mailing addresses, phone numbers, email addresses, fax numbers, and business tax IDs. All PII/BII data is stored on GFE devices and not publicly accessible. The data stored locally on GFE (client systems) is encrypted at rest.
- The Budget Formulation Division (BFD), formerly known as the Policy and Constituent Affairs Division (PCAD), collects and stores both PII and BII for contact and communication purposes and this data is stored within a database that is a component of NOAA6001. Logical access is granted to authorized personnel based on a role-based schema. The BII/PII data consists of names and email addresses. The database system that stores and manages the BII/PII for this office is not publicly facing or accessible.
- The AAMB has a Local Registration Authority (LRA) function that provides an identification role in support of the NOS Department of Defense (DOD) public key infrastructure (PKI) verification process. The verification process uses form DD-2841 that requires the LRA to process PII. This form is stored in the NOAA6001 system within a password protected zip file. The PII collected consists of the unique identification number from a federal government-issued identification credential with a picture, for example Military ID card or Passport card; the unique identification number from a non-federal government-issued identification card (for example, Driver License card). The form also contains common access card (CAC) card electronic data interchange personal identifier (EDIP), full name, work email, work phone number. Only the numbers are collected from the artifacts and stored in the system. The LRA has posted a privacy act statement at the LRA station. The LRA provides a hard copy of the privacy act statement to each individual granted access.
- Office of General Council (OGC): These attorneys collect PII/BII that is shared by NOS program and staff offices for the business purpose of legal review and support for FOIA, administrative appeals, litigation, agreements, or other legal reviews. Note: OGC does not conduct the collection of this information. This information is controlled at the NOS program and staff office levels and shared to GCOC when applicable.

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

Access to information that is transmitted to and from NOAA6001 is controlled by access controls that are based on permissions assigned to authorized personnel within NOAA6001 boundary. Transmission is conducted by the system via its network infrastructure that is managed by the NIT. The NIT is responsible for managing the procedures, methods, and tools required to effectively operate, administrate, and maintain the NOAA6001 network.

- Microsoft Azure Commercial Cloud: The cloud service employs Federal Information Processing Standard (FIPS) 140-2 validated encryption to data transmission for any provided services. NOAA6001 employs FIPS 140-2 encryption for communications between it and the cloud service. The service implements Transport Layer Security (TLS) version 1.2 for securing communications.
- Google websites that host NOS content do not reside within NOAA6001. Encryption for data transmission is the responsibility of Consolidated Cloud Applications (NOAA0900). Google websites provide AAMB a capability to create and host content for the consumption of NOS personnel (Intranet) only. These websites are deployed to the NOAA Intranet and are not publicly accessible. The Identity, Credential, and Access Management (ICAM) logical controls are provided by NOAA0700.
- GovDelivery Communications Cloud: The SaaS application utilizes TLS 1.2 or higher encryption for connections to the system service offerings.
- Adobe Connect: The application is accessed via utilizing GFE. The data (PII/BII) transmission is protected with TLS 1.2, the protocol employed by NOAA6001. Adobe Connect is a SaaS communications application that provides the AAMB with video streaming of NOS conferences and meetings. Note: Individuals can decline to be videotaped by not participating in the recording activities talking about NOS-related topics. The disclaimer presented prior to the recording session is added to this document.
- Kiosks: The kiosk components consist of information sharing conducted by CED. The displaying endpoints (kiosks) at the remote locations are not in the boundary of NOAA6001. The laptops are utilizing TLS 1.2 for encrypting communications.
- GFE: Laptops and desktops are configured to utilize TLS 1.2 for encrypting network communications.
- Network storage (Cohesity): NOAA6001 provides enterprise storage services to NOS organizations. The storage services are hosted and managed by the DIT. The DIT administrators access the storage services using GFE utilizing TLS 1.2 for encryption network communication. Specialized network storage (nVIDIA's Quantum) appliances are dedicated to the CatDV application and access is limited to authorized DIT, CED and CED approved individuals and require GFE utilizing TLS 1.2 for encryption network communication.
- Avaya Cloud Secure (Avaya): The application is configured to implement TLS 1.2 for securing voice communication confidentiality.

- The IOOS Ocean Enterprise Study spreadsheets are shared using email that implements TLS 1.2 encryption. Final reports are posted to IOOS web site using Hyper Text Protocol Secure (HTTPS) and TLS encryption.
- The Cisco Webex Meetings: The application is accessed via utilizing GFE. The data (PII/BII) transmission is protected with TLS 1.2 or later for encryption network communications. Cisco Webex Meetings is a SaaS communications application that provides the IOOS with video streaming of IOOS Advisory Committee Public Meeting. Note: Individuals can decline by not participating in the recording activities talking about NOS-related topics. The disclaimer presented prior to the recording session is added to this document.

(g) Any information sharing

Any information that are shared with NOAA, DOC, and other federal agencies on a case-by-case basis when a business need is required/necessary. Information exchanges with the private sector and data for public consumption receive further analysis by information owners prior to its release.

None of the applications with the exception of the kiosk component and the manual upload of information to social media, share BII/PII outside of NOAA except that NOS employee information may be shared with Commerce and other federal agencies in the event of a data breach or spill.

The information shared for the kiosks could display the following PII attributes of NOS federal and contractor employees that are made accessible to the public include:

- Audio
- Video
- Digital images

The manual uploading of the following PII attributes of NOS federal and contractor employees to social media platforms using Adobe Connect that are publicly accessible include:

- Audio
- Video
- Digital images

Avaya Cloud Secure could relay/share the following PII/BII attributes of NOS federal and contractor employees that are holding conversations when utilizing the system:

- Audio

Social media could relay/share the following PII/BII attributes of NOS federal and contractor employees:

- Audio
- Video
- Digital images

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

Please reference the table at the end of this document linking the data records, SORNs, and authorities.

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

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.

X 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	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): The Webex Meetings maybe used to record IOOS Advisory Committee Public Meeting video conferences, transcription, direct messaging to individual attendees and autosave of the chat log. IOOS personnel do not make the recordings or the transcripts public, the recordings and transcripts are used to accurately capture the comments and the discussion conveyed during the public meetings. No third party PII/BII is being collected outside the authority of COMMERCE/DEPT-23.					

_____ 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.

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*	X	f. Driver's License	X	j. Financial Account	X
b. Taxpayer ID	X	g. Passport	X	k. Financial Transaction	X
c. Employer ID		h. Alien Registration	X	l. Vehicle Identifier	
d. Employee ID		i. Credit Card	X	m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: Program offices could collect SSNs in support of official duties that are administrative-related (e.g., performance reviews, hiring activities, security clearances). SSNs are collected manually and hard copies of					

this data type could digitally transfer and be temporarily maintained by NOAA employees from AAMB, CO-OPS, ONMS and NCCOS program offices, within network storage provided by the Cohesity solution. Hard copies that are not digitally processed for storage within NOAA6001 are stored in locked and controlled file cabinets residing in AAMB working spaces.

The Planet Stewards collects individual and business names, mailing addresses, phone numbers, email addresses, fax numbers, and business tax IDs.

The IOOS Ocean Enterprise Study collects numerous BII information (e.g., name, address, phone number, latitude, longitude, Dun & Bradstreet (D-U-N-S) number, Standard Industrial Classification (SIC) number, North American Industry Classification System (NAICS) number, Ocean Enterprise revenue, etc.) and non-sensitive PII (name, address, phone number).

The OGC might use social security numbers as part of the OSY/security clearance process for interns, staff hiring, and other mission/business related purposes. These forms are stored in hard copy format in a controlled space within a locked file cabinet within OGC office space.

General Personal Data (GPD)

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

Work-Related Data (WRD)

a. Occupation	X	e. Work Email Address	X	i. Business Associates	X
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	X
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):					

Distinguishing Features/Biometrics (DFB)

a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	X
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording	X	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):					

System Administration/Audit Data (SAAD)

a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	X

g. Other system administration/audit data (specify):

Other Information (specify)

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	X
Telephone	X	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			X		
Other (specify): A database utilized by BFD contains data compiled from names and business addresses of non-organizational individuals whom are engaged with and have NOS-related mission and business interests. IOOS Ocean Enterprise Study consists of a contractor to engage in developing/maintaining two spreadsheets. The first spreadsheet contains details of 2020 Ocean Enterprise survey respondents and the information they provided in the survey instrument they completed. The second spreadsheet comprises details of businesses determined to be active in the provision of Ocean Enterprise products and services together with details concerning their business activity collated from their websites and from other public and proprietary sources.					

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

CUI, PII and BII data types are not subject to automatic collection (transfer) by NOAA6001 system components. These data types are input or transmitted via manual interaction by AAMB employees.

The data owners conduct audits and review PII and BII at least annually. This ensures data accuracy, viability, and to determine if outdated. NOAA6001 does implement the privacy control family as part of its Moderate baseline categorization.

IOOS Ocean Enterprise Study manual updates the two spreadsheets prior to the IOOS Ocean Enterprise survey being issued.

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. 0648-0712 The Ocean Enterprise: A Study of US Business Activity in Ocean Measurement, Observation, and Forecasting. 0607-1018, FOIA
	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	X	Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify): Video recordings (Adobe Connect & Cisco Webex Meetings) and voice conversations (Avaya).			
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	

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)	X	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).

The primary mission of NOAA6001 is to support the business units and mission objectives of the AAMB staff and program offices.

NOAA6001 provides to the NOS program and staff offices the services listed in the NOS ACIO IT Services catalog. These IT services include network engineering and administration, domain infrastructure management, help desk operations, Windows configuration management that includes laptops, servers, database and web application hosting, implementing security management (endpoints), Apple Macintosh management, storage management, and enterprise cloud subscription management.

- Microsoft Azure Commercial Cloud: NOS federal and contractor employees that possess privileged level access can retrieve information by leveraging logical access controls applied within the Azure environment.
- Google Sites: NOS federal and contractor employees that possess privileged access can retrieve information by leveraging logical access controls within the Google Sites environment. Google Sites functionality resides within the boundary of NOAA0900, Consolidated Cloud Applications. This component is not a child system of NOAA6001 and is described as an accessible resource by NOS employees utilizing for uploading mission-related CUI/BII/PII data types to Intranet websites. Non-privileged users are only NOAA federal and contractor employees who do possess the ability to change content hosted by Google Sites. These internal facing websites contain PII in the form of names, email addresses, and images. These websites are not publicly facing or accessible.
- GovDelivery Communications Cloud: NOS federal and contractor CED employees that possess privileged access can retrieve information by leveraging logical access controls via Max.gov, applied by the SaaS. The data stored within the application is only accessible to privileged users that must be connected to the NOAA6001 network for

access. The application contains PII in the form of email addresses. Access to the GovDelivery is limited to only authorized NOS federal and contractor personnel.

- Adobe Connect: NOS federal and contractor employees that possess privileged access can access information by leveraging logical access controls provided by the service. NOS federal and contractor employees that possess non-privileged with read only access and view information by participating in the meetings/webinars presented by the application. The application receives uploaded information from CED and presents PII in the form of names, email addresses, images and digital audio and video recordings of stakeholders talking about NOS-related topics. The application back end is not publicly accessible; however, the content is shared publicly via social media and other publicly accessible platforms (i.e., YouTube). Access to the Adobe Connect storage is limited to only authorized NOS federal and contractor personnel. NOAA6001 transferred NOAA6001 public access information to NOAA6301 managed web sites, which facilitates uploading NOAA6001 public information to the NOAA6301 hosted web sites and to the above identified commercial social media sites.
- Kiosks: CED federal and contractor employees that possess privileged access can manage information by leveraging logical access controls implemented by NOAA6001. Access to the GFE laptop and locally installed software is controlled by NOAA6001. The public can only view content that is being presented at the 34 interactive kiosks globally located. The kiosks could display PII in the form of images and digital audio and videos recordings of NOS federal and contractor employees that are speaking to NOS-related topics.
- GFE: NOS federal and contractor employees are assigned GFE devices (laptops, desktops, mobile phones and tablets) for the purpose of conducting assigned roles and responsibilities in support of mission and business functions. The computer image for GFE is managed by the DIT. The GFE component enables NOS employees the ability to access NOAA6001 resources based on role-based access controls. CUI/PII/BII can be stored on local hard drives of these systems. Access to the GFE is limited to only authorized NOS federal and contractor personnel.
- Network storage (Cohesity) is a data storage service, supporting some NOS staff and offices. The Cohesity application provides storage and short-term backup of data. Access to the data stored in Cohesity is enforced utilizing a role-based access schema. Only program and staff office employees that possess an authorization, are capable of retrieving or viewing data. This action can be conducted using GFE. Privileged access to the application is limited to the DIT. PII included is email addresses, names and digital audio and videos recordings of stakeholders talking about NOS-related topics. CUI/PII/BII is included as human resources data, sensitive government data, credit card information, passport information, contracting data, etc. Access to the network storage is limited to only authorized NOS federal and contractor personnel.

- Avaya Cloud Secure (Avaya) is a FedRAMP approved SaaS subscription that provides the NOS basic VoIP, Voice Messaging, Instant Messaging, mobility support to various personnel devices, and Collaboration including basic and advanced audio and web conferencing. PII/BII can be relayed via audio and video conversations communicated by NOS employees.
- CatDV is an internal digital asset management and workflow platform that provides asset management, cataloging, video workflow automation, and collaboration to NOAA's video production teams. CatDV is our internal video catalog and stores all video production assets, including thumbnails, audio, project files and their associated metadata. CatDV also stores information pertaining to rights management associated with clips such as copyright or source of stock footage. This enables optimization of media analysis and custom search engines of very large databases. CatDV only stores data associated with video production assets (title, description, location, summary, etc.). This also provides full audit capability, analytics, and asset control rules for digital media data. Access to the CatDV is limited to only authorized NOAA federal and contractor personnel.
- The IOOS Ocean Enterprise Study uses the maintained spreadsheets as the source of participates for their Ocean Enterprise survey. The survey results are collected using SurveyMonkey to the contractor. The contractor generates the Ocean Enterprise Study from the survey results and provides the report to IOOS. The Ocean Enterprise Study report is posted to the IOOS public web site (<https://ioos.noaa.gov/project/ocean-enterprise-study/>).
- The Cisco Webex Meetings recordings/videos are only available to IOOS federal and contractor employees who possess privileged access. The application back end is not publicly accessible and the content of the recordings are not shared outside of IOOS federal and contractor employees who possess privileged access. The application records information from IOOS Advisory Committee Public Meetings and could present BII/PII in the form of audio, any screen shared (i.e., slides) images and chat logs, including names that appear in chat of stakeholders talking about NOS-related topics. Written consent will be collected from the owner of any slides that are being recorded.

Manual collection and storage of CUI/PII/BII by NOS program and staff offices:

- PII is collected to support the NOS Planet Stewards Education Project. The PII collected as part of this effort consists of individual and business names, mailing addresses, phone numbers, email addresses, fax numbers, and business tax IDs. All PII/BII data is stored on GFE devices and not publicly accessible. The data stored locally on GFE (laptops) is encrypted at rest. The NOS Planet Stewards Education Project is a CED sponsored and is outsourced to a contractor using GFE to perform the identified PII collection. CED has provided the contractor with specific instructions on the handling and destruction of collected PII in the performance of this contract. Collected PII is only shared between CED and contractor performing the work.
- The BFD collects and stores both PII and BII for contact and communication purposes and this data is stored within a database that is a component of NOAA6001. Logical access controls enforce role-based access on permitted authorized personnel access to the information contained. The PII data consists of names and email addresses. The database system that stores the PII for this office is not publicly facing or accessible. The BFD

database access is limited to only authorized NOS federal and contractor personnel and stored on GFE.

- The AAMB has an LRA that provides services in support of the NOS DOD PKI operation. The verification process uses form DD-2841 that requires the LRA to process PII. This form is stored in the NOAA6001 system within a password protected zip file. The PII collected consists of the unique identification number from a federal government-issued identification credential with a picture, for example Military ID card or Passport card; the unique identification number from a non-federal government-issued identification card (for example, Driver License card). The form also contains CAC card EDIP, full name, work email, work phone number. Only the numbers are collected from the artifacts and stored in the system. The LRA has posted a privacy act statement at the LRA station. The LRA provides a hard copy of the privacy act statement to each individual granted access. The LRA collected and processed PII is limited to only authorized NOAA and DOD federal and contractor personnel and stored on GFE. DOD processes the collected PII and returns a PKI certificate used for creating Secure Sockets Layer (SSL)/ TLS Version 2.1 access to GFE from GFE.
- Office of General Council: These attorneys collect PII/BII that is shared by NOS program and staff offices for the business purpose of legal review and support for FOIA, administrative appeals, litigation, agreements, or other legal reviews. Note: OGC does not conduct the collection of this information. This information is controlled at the NOS program and staff office levels and shared to OGC when applicable. OGC only receives copies of PII/BII from NOS program and staff offices that is only shared with authorized NOS federal and contractor personnel and stored on GFE.

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.)

Insider threat, data, or spillage of PII/BII are the primary threats to privacy. Mitigation for these threats to NOAA6001 PII/BII data, logical and physical controls are implemented. In addition, the protection mechanisms are applied:

- NOAA has established privacy-related resources (i.e., Privacy Officer).
- Data owners are provided privacy training and follow all applicable privacy data directives.
- Authorized users that possess access to CUI/PII/BII are required to complete applicable privacy trainings.

All users are required to sign rules of behavior related to IT access at the completion of mandatory security awareness training.

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

	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?

X	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.
	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.

	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: NOAA6001 is interconnected with the following systems in concurrence with CSAM: • NOAA N-Wave (NOAA0550) • NCSC (NOAA0100) • OCM General Support System (NOAA6101) • CO-OPS PORTS and NWLON (NOAA6205) • NCCOS Research Support System (NOAA6301) • NGS General Support System (NOAA6401) • OCS Nautical Charting System (NOAA6501) • ONMS (NOAA6602) • OR&R Local Area Network (NOAA6701) • NOAA EDC (NOAA0520)
--	---

	NOAA Consolidated Cloud Applications (NOAA0900) NOAA6001 implements NIST Moderate level physical, technical and administrative controls for protecting interconnected system communication and data. NOAA6001 information system assets are protected in organizational facilities that employ card readers and additional accesses restrictions based on a need-to-know and/or business requirement (physical access control list). TLS is the cryptographic protocol utilized for providing communications security to NOAA6001. Logical access control is facilitated by established access control lists (ACL), enforcing authorized access for subjects and objects. These ACLs are architected to prevent unauthorized accesses for all data types, including CUI/PII/BII. In addition, NOAA6001 leverages data loss prevention tools provided at the NOAA level to assist mitigating potential spillage of sensitive PII/BII through NOAA provided email (GMAIL). These information types are shared with NOAA, DOC and other federal agencies on a case-by-case basis when a business need is required/necessary, the private sector and public consumption.
	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	X	Government Employees	X
Contractors	X		
Other (specify): For general public, users have access (view only) of the PII (NOAA employees) presented by the kiosk components located at remote locations around the world. Note: The kiosks are not part of the NOAA6001 boundary of operation. NOAA6001 takes no responsibility if these devices collect PII on behalf of the institutions where they reside.			

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: The CatDV application privacy policy: https://oceanservice.noaa.gov/privacy.html

- <https://sites.google.com/noaa.gov/nos-for-employees-intranet/about-nos/all-hands-meetings/upcoming-event-registration>. Note: This website is not accessible by non-NOS employees. See screenshot appended to PIA.
- The GovDelivery SaaS provides a copy of the Privacy Act for the public upon signing up for the service. <https://granicus.com/privacy-policy/>
- BFD collection leverages the NOS Constituents' Portal and can be retrieved at: <https://constituents.nos.noaa/login.aspx>. NOTE: This is an internal facing system and not accessible to non-organizational personnel. See screenshot appended to PIA.
- BFD collection leverages the development version of the NOS Constituents' Portal and Privacy Act statement is available at: <https://devconstituents.nos.noaa/login.aspx>. NOTE: This is an internal facing system and not accessible to non-organizational personnel. See screenshot appended to PIA.
- BFD collection leverages the NOS Memorandum of Agreement (MOA) Tracking System and can be retrieved at: <https://moa.nos.noaa/Login>. NOTE: This is an internal facing system and not accessible to non-organizational personnel. See screenshot appended to PIA.
- BFD collection leverages the development version of the NOS MOA Tracking System and can be retrieved at: <https://devmoa.nos.noaa/Login>. NOTE: This is an internal facing system and not accessible to non-organizational personnel. See screenshot appended to PIA.
- The link to Adobe Connect privacy guidance can be retrieved at: <https://www.adobe.com/privacy.html>
- The link to Avaya privacy guidance can be retrieved at: <https://www.avaya.com/en/privacy/policy/>
- Microsoft Azure Commercial Cloud privacy guidance available at: <https://www.microsoft.com/en-us/trustcenter/privacy/>
- NOAA & NOS operated Google Sites and Google Workspace Privacy Policy is available at:
 - <https://www.noaa.gov/protecting-your-privacy>
 - Google Privacy Policy is available at: <https://policies.google.com/privacy>
- Planet Stewards Education Project Privacy Act statement is provided as a hardcopy or as an attachment to electronic email message and is not posted to a web site. See screenshot appended to PIA.
- The Cisco Webex Meetings cloud service privacy guidance can be retrieved at:
 - IOOS Consent Form: <https://docs.google.com/forms/d/e/1FAIpQLSeuikCitamW1IVMLQe2xsA0W6YGBc2KmKQlI8hqwTjTrbo4UQ/viewform>
 - IOOS PAS: <https://cdn.ioos.noaa.gov/media/2025/04/Privacy-Act-Statement-for-WebEx-Recordings.pdf>
 - Cisco Webex Privacy: https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=Privacy%20Data%20Sheet|Privacy%20Data%20Map&prodse rv=Cisco%20Webex%20Meetings&search_keyword=privacy#/1554085468927155

Specific social media privacy links:

- Facebook: <https://www.facebook.com/privacy/explanation/>
- Vimeo: <https://vimeo.com/features/video-privacy>

	• X: https://x.com/en/privacy • Flickr: https://www.flickr.com/help/privacy • Instagram: https://help.instagram.com/519522125107875 • YouTube: https://policies.google.com/privacy?hl=en	
X	Yes, notice is provided by other means.	Specify how: There is manual collection and physical storage of PII and BII by NOS program and staff offices. • The PII collected in support of the Planet Steward program provides a copy and notification of the NOAA privacy policy. Planet Stewards Education Project privacy requirements remain a part of the NOAA Acquisition and Grants awarded contract available upon request to the Contracting Officer. • The DD Form 2841 contains a privacy act statement for the audience to review. LRA individual has posted a privacy act statement at the LRA station. The LRA provides a hard copy of the privacy act statement to each individual granted access.
	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: • NOAA6001 file shares store CUI, PII and BII on an ad-hoc basis. This data is part of the application and hiring of AAMB employees, including electronic copies of resumes and the processing of human resource data about employees, including hiring ranking are stored temporarily during the hiring phase, including, standard human resource information such as travel authorization and vouchers, passports and international travel forms, information for transmitting the security badge request email which includes only an email address and possibly a phone number, and performance appraisal ranking. Employees can decline in writing to provide PII to their supervisors. • GovDelivery Communications cloud provides an unsubscribe function in every email it sends to users. Users can opt out at any time and any stage in the process. Users can sign up for the services offered by GovDelivery by submitting an email address. • CatDV allows at the time of collection for individuals to decline PII/BII. Manual collection and physical storage of PII by AAMB program and staff offices: • PII is collected to support the NOS Planet Stewards Education Project. All the PII is collected on a voluntary basis and individuals can decline by not participating in the program. • BFD collects and stores both PII and BII for contact and communication purposes within the Constituents database. Individuals have an opportunity to decline to provide PII/BII during the annual user audit. Users who no longer want to receive information from NOS can click the unsubscribe button to request that they be removed from the database. • LRA: The DD-2841 form has a disclosure that states clearly that failure to provide information (PII included) may result in denial of issuance of a token containing PKI private keys.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: • OGC does not directly collect PII/BII. OGC attorneys collect PII/BII that is shared by NOS program and staff offices for the purpose of legal review and support for FOIA, administrative appeals, litigation, agreements, or other legal reviews. This information is controlled at the NOS program and staff office level and shared to OGC when applicable. • Adobe Connect is a SaaS communications application that provides the NOS with video streaming of

		conferences and meetings. Users can decline to be videotaped by not participating in the recording activities talking about NOS-related topics. However, the application does not collect PII directly therefore there is no opportunity for declining. The Cisco Webex Meetings is a cloud-based and video conferencing solution employed as a meeting collaboration conferencing solution in support of NOS-related mission/business purposes. The IOOS office uses the Cisco Webex Meetings services to collect PII/BII from individuals. PII/BII is collected in the form of audio, any screen shared (i.e., slides) images and chat logs including names that appear in chat. The information captured during the meeting is for internal (bureau) use only and is accessed through the Webex portal. The captured information is used to support the IOOS Advisory Committee Public Meetings. Users can decline by not participating in the recording activities talking about NOS-related topics.
--	--	---

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: GovDelivery Communications cloud provides an unsubscribe function in every email it sends to users. Users can opt out at any time and any stage in the process. Users can sign up for the services offered by GovDelivery by submitting an email address.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: NOAA6001 file shares store PII and BII on an ad-hoc basis. This data is part of the application and hiring of employees, including electronic copies of resumes and the processing of human resource data about employees, including hiring ranking are stored temporarily during the hiring phase, including, standard human resource information such as travel authorization and vouchers, passports and international travel forms, information for transmitting the security badge request email which includes only an email address and possibly a phone number, and performance appraisal ranking. Federal and contractor employees do not have an opportunity to consent to particular uses of their PII/BII. Microsoft Azure Commercial Cloud is an IaaS platform that enables the NOS to create websites for deploying mission/business content. These websites could process PII in the form of names, email addresses, images, audio and video recordings, all related to NOS-related topics

		and interests. The content and websites are designed for public use and consumption. Azure also serves the NOS as its long-term data storage solution. Individuals do not have an opportunity to consent to particular uses of their PII/BII presented by the website. • Adobe Connect is an (SaaS) application employed as a video conferencing solution in support of NOS-related mission/business purposes. The information is uploaded to the application and then the content is transmitted in video format for both internal (bureau) and external (public) consumption. Adobe Connect does directly collect PII/BII from individuals. PII/BII in the form of digital images, audio/video is processed by the application. Individuals do not have an opportunity to consent to particular uses of their PII/BII processed by the application. All presentations conducted using the Adobe Connect application possess a Privacy notice that disclaims that the meeting is being recorded. Names appearing in the chat box will be recorded. • The interactive kiosks are set up at remote locations around the world that allows public consumption of CED outreach programs and information. The NOAA6001 kiosk component consists of CED personnel sharing NOS information with its partners around the globe. The physical devices (kiosks) presenting the information do not belong to the NOAA6001 boundary but to the local institution that acquire the displayed information. These systems display PII in the form of images, and audio/video formats that is produced for public consumption. Individuals do not have an opportunity to consent to particular uses of their PII/BII processed by the system component. • The GFE component is utilized by AAMB federal and contractor employees via assigned GFE devices (laptops, desktops, mobile phones and tablets) for the purpose of conducting assigned roles and responsibilities in support of mission and business functions. The computer image for GFE is managed by the DIT. The GFE component enables NOS employees the ability to access NOAA6001 resources based on role-based access controls. PII/BII can be stored on local hard drives of these systems. This component does not collect PII/BII directly or in an automated technique, therefore the opportunity to consent how PII is used does not present itself to the individual. • Network storage (Cohesity) and Quantum are digital data storage services, supporting the AAMB, CO-OPS, ONMS, and NCCOS program and staff offices. The
--	--	---

		Cohesity and Quantum applications provide storage and short-term backup of data. Access to the data stored in both Cohesity and Quantum are enforced utilizing a role-based access schema. Only program and staff office employees that possess an authorization, are capable of retrieving or viewing data. This action can be conducted using GFE. Privileged access to the application is limited to the DIT. PII included is email addresses, names and digital audio and videos recordings of stakeholders talking about NOS-related topics. PII/BII is included as human resources data, sensitive government data, credit card information, passport information, contracting data, audio/video, etc. These components do not collect PII/BII directly or utilizing an automated technique, therefore the opportunity to consent how PII is used does not present itself to the individual. • Avaya Cloud Secure (Avaya) is a FedRAMP approved SaaS subscription that provides the NOS basic VoIP, voice messaging, instant messaging, mobility support to various personnel devices, and collaboration including basic and advanced audio and web conferencing. PII/BII can be relayed via audio and video conversations communicated by NOS employees. This component does not collect PII/BII directly or in an automated technique, therefore the opportunity to consent how PII is used does not present itself to the individual. AT&T does offer an optional service for voice mail transcription, and we do work with our customers to provide a disclaimer on their personal greetings. At this time, NOS is not subscribing to that service, therefore, this issue does not need to be addressed. The capability offered as part of the standard service is the normal retrieval of audio voice mail messages which should not require a disclaimer. • The Cisco Webex Meetings is a cloud-based and video conferencing solution employed as a meeting collaboration conferencing solution in support of NOS-related mission/business purposes. The IOOS office uses the Cisco Webex Meetings services to collect PII/BII from individuals. PII/BII is collected in the form of audio, any screen shared (i.e., slides) images and chat logs including names that appear in chat. The information captured during the meeting is for internal (bureau) use only and is accessed through the Webex portal. Privacy Act Statement states the particular uses of their PII/BII. Individuals can decline to participate in the meeting. All presentations conducted using the Cisco Webex Meetings service requires the individual to
--	--	--

		(Google Form) register for the meeting that possess a consent question and a link to the Privacy Act Statement. Manual collection and physical storage of PII/BII by AAMB program offices: • PII is collected to support the NOS Planet Stewards Education Project. The PII collected as part of this effort consists of individual and business names, mailing addresses, phone numbers, email addresses, fax numbers, latitude, longitude, D-U-N-S number, SIC number, NAICS number, Ocean Enterprise revenue and business tax IDs. All PII/BII data is stored on GFE devices and not publicly accessible. The data stored locally on GFE (laptops) is encrypted at rest. The program does not present an opportunity to consent how PII is used. • BFD collects and stores both PII and BII for contact and communication purposes and this data is stored within a database that is a component of NOAA6001. Logical access controls enforce role-based access on permitted authorized personnel access to the information contained. The PII data consists of names and email addresses. The database system that stores the PII for this office is not publicly facing or accessible. There isn't an opportunity for individuals to consent how PII is used. • AAMB has an LRA that provides services in support of the NOS DOD PK) operation. The verification process uses form DD-2841 that requires the LRA to process PII. This form is stored in the NOAA6001 system within a password protected zip file. The PII collected consists of the unique identification number from a federal government-issued identification credential with a picture, for example Military ID card or Passport card; the unique identification number from a non-federal government-issued identification card (for example, Driver License card). The form also contains CAC card EDIP identifier, full name, work email, work phone number. Only the numbers are collected from the artifacts and stored in the system. The LRA has posted a privacy act statement at the LRA station. The LRA provides a hard copy of the privacy act statement to each individual granted access. There isn't an opportunity for individuals to consent how their PII is used. • OGC attorneys collect PII/BII that is shared by NOS program and staff offices for the business purpose of legal review and support for FOIA, administrative appeals, litigation, agreements, or other legal reviews.
--	--	---

		Note: OGC does not conduct the collection of this information. This information is controlled at the NOS program and staff office levels and shared to OGC when applicable.
--	--	---

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: NOAA6001 file shares store PII and BII on an ad-hoc basis. This data is part of the application and hiring of NOS employees, including electronic copies of resumes and the processing of human resource data about employees, including hiring ranking are stored temporarily during the hiring phase, including, standard human resource information such as travel authorization and vouchers, passports and international travel forms, information for transmitting the security badge request email which includes only an email address and possibly a phone number, and performance appraisal ranking. Federal and contractor employees do have an opportunity to review/update PII/BII pertaining to them by coordinating efforts with a supervisor or the information owner. Major NOAA6001 components that collect, store, and/or process PII/BII: - GovDelivery Communications Cloud is a FedRAMP approved SaaS subscription that provides the NOS with a number of features to support the efficient communication of timely information to the general public. Access is limited to only NOS employees and the managing the data and content is not publicly accessible. The public only receives provided content from the NOS. GovDelivery processes PII in the form of email addresses. Individuals have an opportunity to change/update their email address. Manual collection and physical storage of PII/BII AAMB staff and program offices: - PII is collected to support the NOS Planet Stewards Education Project. All the PII is collected on a voluntary basis and individuals can decline by not participating in the program. PII that is collected can be reviewed/updated by coordinating through CED and the supervisor for the Planet Steward Education Project. - BFD collects and stores both PII and BII for contact and communication purposes and this data is stored within a database that is a component of NOAA6001. Logical access controls enforce role-based access on permitted authorized personnel access to the information contained. The PII data consists of names and email addresses. Individuals can coordinate with BFD for changing email addresses. - AAMB has an LRA that provides services in support of
---	---	---

		the NOS DOD PKI operation. The verification process uses form DD-2841 that requires the LRA to process PII. This form is stored in the NOAA6001 system within a password protected zip file. The PII collected consists of the unique identification number from a federal government-issued identification credential with a picture, for example Military ID card or Passport card; the unique identification number from a non-federal government-issued identification card (for example, Driver License card). The form also contains CAC card EDIP identifier, full name, work email, work phone number. Only the numbers are collected from the artifacts and stored in the system. The LRA has posted a privacy act statement at the LRA station. The LRA provides a hard copy of the privacy act statement to each individual granted access. Individuals will need to submit a new form, DD-2841, to update/change PII.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Microsoft Azure Commercial Cloud is an IaaS platform that enables the NOS to operate back-end infrastructure supporting mission/business content. Azure also serves the NOS as its long-term data storage solution. Individuals do not have access or opportunity to review/update PII/BII pertaining to them because this component does not collect PII/BII directly. Adobe Connect is an (SaaS) application employed as a video conferencing solution in support of NOS-related mission/business purposes. Adobe Connect does not directly collect PII/BII from individuals. The information is uploaded to the application and then the content is transmitted in video format for both internal (bureau) and external (public) consumption. PII/BII in the form of digital images, audio/video is processed by the application. Individuals do not have an opportunity to review/update PII/BII pertaining to them because the application does not collect PII/BII directly. The interactive kiosks are set up at remote locations around the world that allows public consumption of CED outreach programs and information. The NOAA6001 kiosk component consists of CED personnel sharing NOS information with its partners around the globe. The physical devices (kiosks) presenting the information do not belong to the NOAA6001 boundary but to the local institution that acquire the displayed information. These systems display PII in the form of images, and audio/video formats that is produced for public consumption. Individuals do not have an opportunity to review/update PII/BII pertaining to them because the component does not collect PII/BII directly. Data storage services provided by NOAA6001 for some NOS program and staff offices is delivered via network connectivity to the Cohesity DataProtect application. Cohesity is a software-defined solution for protecting and storing NOS data. The enclave operates on a cluster of virtualized hosts managed by the DIT. Cohesity provides short term storage, recovery vitality in the event of a disruption and serves as the conduit for the

		long-term storage service provided by the Commercial Azure component of NOAA6001. Individuals do not have an opportunity to review/update PII/BII pertaining to them because the component does not collect PII/BII directly. Avaya Cloud Secure (Avaya) is a FedRAMP approved SaaS subscription that provides the NOS basic VoIP, Voice Messaging, Instant Messaging, mobility support to various personnel devices, and Collaboration including basic and advanced audio and web conferencing. Individuals do not have an opportunity to review/update PII/BII pertaining to them because the component does not offer the functionality to do so. GFE: AAMB federal and contractor employees are assigned GFE devices (laptops, desktops, mobile phones and tablets) for the purpose of conducting assigned roles and responsibilities in support of mission and business functions. The computer image for GFE is managed by the DIT. The GFE component enables NOS employees the ability to access NOAA6001 resources based on role-based access controls. PII/BII can be stored on local hard drives of these systems. Individuals do not have an opportunity to review/update PII/BII pertaining to them because the component does not collect PII/BII directly. OGC personnel do not manually collect PII/BII directly from individuals. PII/BII is shared with OGC when applicable to its roles and responsibilities. Individuals do not have an opportunity to review/update PII/BII pertaining to them because the program and staff office does not collect PII/BII directly. CatDV is an internal digital asset management and workflow platform that provides asset management, cataloging, video workflow automation, and collaboration to NOAA's video production teams. Individuals do not have an opportunity to review/update PII/BII pertaining to them with the CatDV system because the component does not collect PII/BII directly. The Cisco Webex Meetings is a cloud-based and video conferencing solution employed as a meeting collaboration conferencing solution in support of NOS-related mission/business purposes. The IOOS office uses the Cisco Webex Meetings services to collect PII/BII from individuals. PII/BII is collected in the form of audio, any screen shared (i.e., slides) images and chat logs including names that appear in chat. The information captured during the meeting is for internal (bureau) use only and is accessed through the Webex portal. Individuals do not have an opportunity to review/update PII/BII pertaining to them because the Cisco Webex requires a license for accessing the stored recordings.
--	--	---

Section 8: Administrative and Technological Controls

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

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: - Microsoft Azure Commercial Cloud: This component implements security controls at a high baseline in accordance with FedRAMP policies. Administrative controls for content hosted in this component is the responsibility of the data owner and/or program office. - GovDelivery Communications Cloud: NOS federal and contractor CED employees that possess privileged access can retrieve information by leveraging logical access controls via Max.gov, applied by the SaaS. The data stored within the application is only accessible to privileged users that must be connected to the NOAA6001 network for access. The application contains PII in the form of email addresses. This SaaS implements security controls at a Moderate baseline. Administrative controls for monitoring and tracking PII is the responsibility of the data owner and/or program office. - Adobe Connect is a SaaS application that provides CED with video conferencing services. The audio and video presented by the application is stored in the cloud and CED relies on its security function for protecting PII. - The interactive kiosks are set up at remote locations around the world that allows public consumption of CED outreach programs and information. The NOAA6001 kiosk component consists of CED personnel sharing NOS information with its partners around the globe. The physical devices (kiosks) presenting the information do not belong to the NOAA6001 boundary but to the local institution that acquire the displayed information. These systems display PII in the form of images, and audio/video formats that is produced for public consumption. The data for the content presented by Kiosk stored locally on a GFE laptop and Moderate baseline security controls are implemented for technical, management and physical protections. - GFE components possess endpoint protection mechanisms (i.e., McAfee) and Moderate security control baseline for technical, management, and physical protections. - CatDV resides on NOAA6001 GFE and is covered under NOAA6001 moderate security controls and only accessible by the system administrator and approved CED employees. - NOS Network Storage (Cohesity) resides on NOAA6001 GFE and is covered under NOAA6001 moderate security controls and only accessible by authorized NOS federal and contractor personnel. - Avaya Cloud Secure (Avaya) is a FedRAMP approved SaaS subscription that has a shared responsibility between Avaya and NOAA6001 GFE. Avaya and NOAA6001 are covered under moderate security controls and only accessible by authorized Avaya personnel and NOAA6001 NOS federal and contractor personnel. - AAMB has an LRA that provides services in support of the NOS DOD PKI operation. The verification process uses form DD-2841 that requires the LRA to process PII. This form is stored in the NOAA6001 system within a password protected zip file. The LRA has posted a privacy act statement at the LRA station. The LRA provides a hard copy of the privacy act statement to each individual granted access. Individuals will need to submit a new form, DD-2841, to update/change PII. Administrative and physical controls protect hard copies of these forms. - PII collected in support of the Planet Steward Education Project is stored on GFE that receives the endpoint protection mechanism McAfee and the Moderate baseline security controls for technical, management, and physical protections.

	- BFD collects and stores PII/BII. The data is stored on a database residing within NOAA6001. This database device receives Moderate security control baseline implemented by NOAA6001. - Office of General Council collected PII/BII covers business purpose of legal review and support for FOIA, administrative appeals, litigation, agreements, or other legal reviews. OGC collected PII/BII resides on NOAA6001 GFE and is covered under NOAA6001 Moderate security control baseline for technical, management, and physical protections. - The Cisco Webex Meetings is a cloud-based and video conferencing solution that provides IOOS with meeting collaboration conferencing services. The audio presented by the application is stored in the cloud and IOOS relies on its security function for protecting PII.
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>2/24/2025</u> ☐ 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). NIST SP 800-53 Revision 4 has been replaced with NIST SP 800-53 Revision 5 that develop a new security control family devoted to Privacy.
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.
	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).*

Policies set for by DOC stipulate that all PII/BII data electronically transmitted must follow federal government and NOAA standard procedures of secure packaging such as utilization of DOC Kiteworks for encryption in transit.

NIST Special Publication 800-53r4 is the reference utilized for implementing the Moderate level security controls for NOAA6001. The Moderate baseline of security controls are administrative, technical and physical implementations throughout the operating boundary of NOAA6001. These controls implement the security program, are continuously monitored, and are subjected to annual assessments. The privacy controls listed in this publication are included as part of the security control baseline for NOAA6001. These controls for NOAA6001 are subjected to an annual assessment per DOC and NOAA IT security policies. Other continuous monitoring activities for validating security controls includes vulnerability scanning, audit analysis

All data stored (data at rest) within Cohesity file shares (network storage) are encrypted with FIPS 140-2 compliant encryption algorithms. Access to files and folders is granted by the information owner and controlled logically by NOAA6001 Moderate security controls.

The principle of least privilege applies throughout AAMB and NOAA6001. All business units within AAMB only grant access to information on a need-to-know basis. NOAA6001 utilizes

Active Directory (AD) directory service to manage permissions and access to network (system) resources. The main service is Active Directory Domain Services (AD DS), which stores directory information and handles the interaction of the user with the domain. AD DS controls access permissions and group policies for NOAA6001.

Major system components protect transmitted information by employing the following:

- Microsoft Azure Commercial Cloud: The cloud service employs FIPS 140-2 validated encryption to data transmission for any provided services. NOAA6001 employs FIPS 140-2 encryption for communications between it and the cloud service. The service employs TLS 1.2 for securing communications.
- GovDelivery Communications Cloud: The SaaS application utilizes TLS 1.2 or higher encryption for connections to the system service offerings.
- Adobe Connect: The application is accessed via utilizing GFE. The data (PII/BII) transmission is protected with TLS 1.2, the protocol employed by NOAA6001.
- Kiosks: The kiosk component consist of two GFE laptops. The endpoints displaying the content provided by CED are not in the boundary of NOAA6001. The laptops are utilizing TLS 1.2 for encrypting communications.
- GFE: Laptops and desktops are configured to utilize TLS 1.2 for encrypting network communications.
- Network storage (Cohesity): The application is hosted and managed by the DIT. The administrators access the application using GFE utilizing TLS 1.2 for encryption network communication.
- Avaya Cloud Secure (Avaya): The application is configured to implement TLS 1.2 for security voice communication.
- The Cisco Webex Meetings: The application is accessed via utilizing GFE. The data (PII/BII) transmission is protected with TLS 1.2 or later 2 for encryption network communications.

Major system components protect information at rest by employing the following:

- Microsoft Azure Commercial Cloud: Data storage in the service is encrypted and decrypted transparently using 256-bit AES encryption (FIPS 140-2 compliant).
- GovDelivery Communications Cloud: All data is automatically encrypted using a FIPS-compliant algorithm at the disk level.
- Adobe Connect: All data in the database is encrypted using AES-256 (FIPS 140-2 compliant).
- GFE: Windows 10, Windows 11 and Macintosh laptops utilize drive encryption for encrypting data at rest. Drive encryption employs the FIPS 140-2 compliant algorithm AES-256.
- Network storage (Cohesity) and CatDV employ a FIPS 140-2 compliant encryption algorithm for encrypting data at rest.
- Avaya Cloud Secure (Avaya): This component deploys storage device where data resides. The device employs a FIPS 140-2 compliant algorithm for protecting data at rest.

- The Cisco Webex Meetings packets are encrypted using either AES 256 or AES 128 based ciphers. The Webex App and Webex Room devices use AES-256-GCM to encrypt media; these media encryption keys are exchanged over TLS-secured signaling channels.

Section 9: Privacy Act

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

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

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

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

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

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(List all that apply):</i> GSA/GOV-7, HSPD-12 USAccess OPM/GOVT-1, General Personnel Records OPM/GOVT-10, Employee Medical File System Records COMMERCE/DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons COMMERCE/DEPT-3, Conflict of Interest Records, Appointed Officials COMMERCE/DEPT-4, Congressional Files COMMERCE/DEPT-5, Freedom of Information Act and Privacy Request Records COMMERCE/DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons COMMERCE/DEPT-12, OIG Investigative Records COMMERCE/DEPT-13, Investigative and Security Records COMMERCE/DEPT-14, Litigation, Claims, and Administrative Proceeding Records COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies COMMERCE/DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs COMMERCE/DEPT-25, Access Control and Identity Management System
---	--

	COMMERCE/DEPT-31, Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission *COMMERCE/DEPT-30, Public Affairs Archives
	Yes, a SORN has been submitted to the Department for approval on ____.
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

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

X	There is an approved record control schedule. Provide the name of the record control schedule: Records Schedules - Chapter 1600 – National Ocean Service (NOS) Functional Files. Records Schedules - Chapter 2200 - Records of the Chief Information Officer (CIO) Records Schedules - Chapter 2300 - General Information Technology Management Record Records Schedules - Chapter 2400 – Information Systems Security Records
X	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: NOAA is in the process of creating a records retention schedule for Webex recordings. Until a records schedule is approved by NARA, Webex recordings will be treated as permanent records.
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.)*

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: AAMB federal and contractor employees and non-organizational individuals can be identified. NOAA6001 system components and AAMB federal and contract employees collect, maintain, and transmit names, email addresses, still and video images, and audio recordings which all can be used as methods for identification.
X	Quantity of PII	Provide explanation: Provide explanation: AAMB quantity of PII/BII collection, storage, and transmission is limited to mission/business purposes only.
X	Data Field Sensitivity	Provide explanation: Provide explanation: SSNs are stored for AAMB business purposes only and not accessible by non-organizational individuals. Collected and maintained email addresses and associated names, audio recordings, still images and video images are all non-sensitive data fields maintained and/or stored within elements of NOAA6001.
X	Context of Use	Provide explanation: Provide explanation: PII/BII collected, maintained, processed and transmitted by AAMB business units and NOAA6001 is for business/mission purposes only. Privacy notices are provided manually by applications, components, forms, or by personnel where applicable. All uses of privacy adhere to government, department, and bureau regulations.
X	Obligation to Protect Confidentiality	Provide explanation: Provide explanation: AAMB is obligated to protect PII/BII in accordance with 5 USC 552(b)(4) and the FAR, in accordance with 41 CFR 13.
X	Access to and Location of PII	Provide explanation: Refer to section 8 of this document for a full description of administrative, technical and physical controls put into place for protecting PII/BII data sets within the NOAA6001 information system and AAMB office spaces.
	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.)

Minimal PII is collected. NOAA6001 collects only enough PII and BII for the necessary purposes of conducting business and completing missions. AAMB federal and contractor employees submit/provide PII in order receive the information they request. The only PII attributes that are made available by the kiosks for public consumption are accesses to non-sensitive types (i.e., video and still images and audio recordings).

- 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.

	Type of Information Collected (Introduction h.)	Applicable SORNs (Section 9.2)	Programmatic Authorities (Introduction h.)
1.	Badging & CAC Issuance	COMMERCE/DEPT-18	Electronic Signatures in Global and National Commerce Act, Public Law 106-229
			5 U.S.C. 301
		GSA/GOVT-7	5 U.S.C. 301
			Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
			Federal Information Security Management Act of 2002 (44 U.S.C. 3554)
			E-Government Act of 2002 (Pub. L. 107-347, Sec. 203)

2.	Personnel Actions Including Training	OPM/GOVT-1	5 U.S.C. 1302, 2951, 3301, 3372, 4118, 5379, 8347
			Executive Orders 9397, as amended by 13478, 9830, and 12107
		COMMERCE/DEPT-1	31 U.S.C. 66a
			44 U.S.C. 3101, 3309
			Title 5 U.S.C.
		COMMERCE/DEPT-18	44 U.S.C. 3101
			Executive Orders 12107, 13164,
			41 U.S.C. 433(d)
			5 U.S.C. 5379
			5 CFR Part 537
			Executive Order 12564
			Public Law 100-71
			Executive Order 11246
			26 U.S.C. 3402
3.	Conflict of Interest Records, Appointed Officials	COMMERCE/DEPT-3	5 U.S.C. 301
			18 U.S.C. 208
			28 U.S.C. 533-535
			44 U.S.C. 3101
			Executive Order 10450 and 11222
4.	FOIA & Privacy Act Requests	COMMERCE/DEPT-5	5 U.S.C. 552, Freedom of Information Act
			5 U.S.C. 552a, Privacy Act of 1974 as amended
			5 U.S.C. 301
			44 U.S.C. 3101
5.	Travel Records	COMMERCE/DEPT-9	Budget and Accounting Act of 1921
			Accounting and Auditing Act of 1950
			Federal Claim Collection Act of 1966
6.	OIG Investigative Records	COMMERCE/DEPT-12	The Inspector General Act of 1978, 5 U.S.C. App. 3, as amended

7.	The Inspector General Act of 1978, 5 U.S.C. App. 3, as amended	COMMERCE/DEPT-13	5 U.S.C 301
			5 U.S.C. 7531-332
			28 U.S.C. 533-535
			Equal Employment Act of 1972
8.	Litigation	COMMERCE/DEPT-14	5 U.S.C. 301
			28 U.S.C. 533-535 and 1346(b)
			44 U.S.C. 3101
9.	Info Collected Electronically in Connection w/ DOC Activities, Events & Programs	COMMERCE/DEPT-23	15 U.S.C. § 272
			15 U.S.C. § 1151
			15 U.S.C. § 1512
			15 U.S.C. § 1516
			E.O. 11625
10.	Log Data	COMMERCE/DEPT-25	5 USC 301
			Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
11.	Public Health Emergency Info & Reasonable Accommodation	COMMERCE/DEPT-31	Rehabilitation Act, 29 U.S.C. 701 et. seq
			Americans with Disabilities Act of 1990, as amended, 102(d), 42 U.S.C. 12112(d)
			29 CFR parts 1602, 1630, 1904, 1910, and 1960
			29 USC chapter 15 (e.g., 29 U.S.C. 668)
			Executive Order 12196
			5 U.S.C. 7902
		OPM/GOVT-1	5 U.S.C. 1302, 3301
12.	Contact Information for the Public	NOAA-11	5 U.S.C. 301, Departmental Regulations
			15 U.S.C. 1512, Powers and duties of Department

13	Public Affairs Records	COMMERCE/DEPT-30	5 U.S.C. 301, Departmental Regulations
			44 U.S.C. 2912, Preservation of Electronic Messages and Other Records

Privacy Information (Section 7.1)

NOS For Employee's All Hands portal

<https://sites.google.com/noaa.gov/nos-for-employees-intranet/about-nos/all-hands-meetings/upcoming-event-registration?authuser=0#h.fzorhtkajb18>

Privacy Information

Your privacy matters to us. By joining this meeting your likeness (name in text) may be subject to being filmed or photographed and your image stored on a government website in perpetuity. This information will not be shared outside of NOS, unless extraordinary circumstances require us to share it with NOAA or the Department of Commerce, our parent organizations.

Authority: The collection of this information is authorized under 5 U.S.C. 301(Departmental regulations), 5 USC 552a (Records maintained on individuals); 15 U.S.C. 1512 (Powers and duties of Department), 44 U.S.C. 2904 (General responsibilities for records management), and Commerce/Dept-23 (Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs).

← → ↻ sites.google.com/noaa.gov/nos-for-employees-intranet/about-nos/all-hands-meetings/upcoming-event-registration?authuser=0#h.fzorhtkajb18 ☆

NOS For Employees Home About NOS Employee Resources IT EEO & Diversity NOS Policies and Procedures NOS Too

Enter as a **Guest** and type in your name when joining.

Add this event to your Google calendar by [clicking on this link](#).

All Hands Meeting Archives

Please note that this Webcast will be archived and made accessible in the near future.

To view past slide shows and videos, go to the [All Hands meetings archives page](#).

Privacy Information

Your privacy matters to us. By joining this meeting your likeness (name in text) may be subject to being filmed or photographed and your image stored on a government website in perpetuity. This information will not be shared outside of NOS, unless extraordinary circumstances require us to share it with NOAA or the Department of Commerce, our parent organizations.

Authority: The collection of this information is authorized under 5 U.S.C. 301(Departmental regulations), 5 USC 552a (Records maintained on individuals); 15 U.S.C. 1512 (Powers and duties of Department), 44 U.S.C. 2904 (General responsibilities for records management), and Commerce/Dept-23 (Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs).

AdobeConnect:

Important! Always check with your local system/network administrator before installing any software on your computer.

AdobeConnect integrates captions, video and anything displayed during the event.

Contact Information:

For technical questions regarding accessing this event contact Mike Shelby at 443-745-0400 or Mike.Shelby@noaa.gov.

Browser Requirements:

You must use either **Internet Explorer** or **Edge** on Windows computers and **Safari** on the Macintosh. Test your ability to use AdobeConnect [here](#). Contact your help desk if you have any trouble completing this test.

BFD collections leverages the production and development Constituents' portals (screenshots below show the production and develop web portals)

BFD Constituents' portal (Production)

<https://constituents.nos.noaa/login.aspx>

By logging into this web site, you indicate your awareness of and consent to the following terms and conditions of use.

- Government Web Site Usage

You are accessing a U.S. Government information system, which includes: 1) this computer, 2) this computer network, 3) all Government-furnished computers connected to this network, and 4) all Government-furnished devices and storage media attached to this network or to a computer on this network. You understand and consent to the following: you may access this information system for authorized use only; unauthorized use of the system is prohibited and subject to criminal and civil penalties; you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system at any time and/or any lawful Government purpose, the Government may monitor, intercept, audit, and search and seize any communication or data transiting or stored on this information system; and any communications or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose. This information system may contain Controlled Unclassified Information (CUI) that is subject to safeguarding or dissemination controls in accordance with law, regulation, or Government-wide policy. Accessing and using this system indicates your understanding of this warning.

- Privacy Policy

Information contained in this database will be used exclusively for the purposes of furthering the mission of the National Ocean Service (NOS) of the United States Department of Commerce (DOC) National Oceanic and Atmospheric Administration (NOAA).

- When not in use, personally identifiable information extracted from this database in digital format shall remain on NOAA systems and will be protected at all times.
- Hard copies of personally identifiable information extracted from this database will remain protected in the possession of NOAA personnel and will be used only for purposes identified by NOAA as part of its mission and operations.
- You agree to use this web site and the information it contains in such a way as to abide by the privacy policies of the [DOC Privacy Policy](#) and the [Privacy Act of 1974](#).

- Privacy Statement

This document contains information that has personal privacy interests protected under the Privacy Act of 1974, as amended. Ensure that you protect the information accordingly by following all laws and agency regulations and policies regarding the protection of the data.

- Accessibility Statement

- [NOS Accessibility Statement](#)

NOS Constituents - Login

← → 📄 🔍 🔄 \$ 📧 🖨️ 🛡️ https://constituents.nos.noaa/login.aspx

NOS Constituent Database

Help
You must login to gain access to the Constituents Database.

By logging into this web site, you indicate your awareness of and consent to the following terms and conditions of use.

- Government Web Site Usage
You are accessing a U.S. Government information system, which includes: 1) this computer, 2) this computer network, 3) all Government-furnished computers connected to this network, and 4) all Government-furnished devices and storage media attached to this network or to a computer on this network. You understand and consent to the following: you may access this information system for authorized use only; unauthorized use of the system is prohibited and subject to criminal and civil penalties; you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system at any time and/or any lawful Government purpose, the Government may monitor, intercept, audit, and search and seize any communication or data transiting or stored this information system; and any communications or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose. This information system may contain Controlled Unclassified Information (CUI) that is subject to safeguarding or dissemination controls in accordance with law, regulation, or Government-wide policy. Accessing and using this system indicates your understanding of this warning.

- Privacy Policy
Information contained in this database will be used exclusively for the purposes of furthering the mission of the National Ocean Service (NOS) of the United States Department of Commerce (DoC) National Oceanic and Atmospheric Administration (NOAA).

- When not in use, personally identifiable information extracted from this database in digital format shall remain on NOAA systems and will be protected at all times.
- Hard copies of personally identifiable information extracted from this database will remain protected in the possession of NOAA personnel and will be used only for purposes identified by NOAA as part of its mission and operations.
- You agree to use this web site and the information it contains in such a way as to abide by the privacy policies of the [DOC Privacy Policy](#) and the [Privacy Act of 1974](#).

- Privacy Statement
This document contains information that has personal privacy interests protected under the Privacy Act of 1974, as amended. Ensure that you protect the information accordingly by following all laws and agency regulations and policies regarding the protection of the data.

Login

NOS Constituents Database v4.1 ©2024

[National Oceanic and Atmospheric Administration](#)

Reviewed January 31, 2017 | Questions, Comments? [Contact Us](#) | [Disclaimer](#) | [Privacy Policy](#) | [Privacy Act Statement](#)
Web Site Owner: [National Ocean Service](#) | [National Oceanic and Atmospheric Administration](#) | [Department of Commerce](#) | [USA.gov](#)

BFD Constituents' portal (Development)

<https://devconstituents.nos.noaa/login.aspx>

NOS Constituents - Login

← → 📄 🔍 🔄 \$ 📧 🖨️ 🛡️ https://devconstituents.nos.noaa/login.aspx

NOS Constituent Database

Help
You must login to gain access to the Constituents Database.

By logging into this web site, you indicate your awareness of and consent to the following terms and conditions of use.

- Government Web Site Usage
You are accessing a U.S. Government information system, which includes: 1) this computer, 2) this computer network, 3) all Government-furnished computers connected to this network, and 4) all Government-furnished devices and storage media attached to this network or to a computer on this network. You understand and consent to the following: you may access this information system for authorized use only; unauthorized use of the system is prohibited and subject to criminal and civil penalties; you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system at any time and/or any lawful Government purpose, the Government may monitor, intercept, audit, and search and seize any communication or data transiting or stored this information system; and any communications or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose. This information system may contain Controlled Unclassified Information (CUI) that is subject to safeguarding or dissemination controls in accordance with law, regulation, or Government-wide policy. Accessing and using this system indicates your understanding of this warning.

- Privacy Policy
Information contained in this database will be used exclusively for the purposes of furthering the mission of the National Ocean Service (NOS) of the United States Department of Commerce (DoC) National Oceanic and Atmospheric Administration (NOAA).

- When not in use, personally identifiable information extracted from this database in digital format shall remain on NOAA systems and will be protected at all times.
- Hard copies of personally identifiable information extracted from this database will remain protected in the possession of NOAA personnel and will be used only for purposes identified by NOAA as part of its mission and operations.
- You agree to use this web site and the information it contains in such a way as to abide by the privacy policies of the [DOC Privacy Policy](#) and the [Privacy Act of 1974](#).

- Privacy Statement
This document contains information that has personal privacy interests protected under the Privacy Act of 1974, as amended. Ensure that you protect the information accordingly by following all laws and agency regulations and policies regarding the protection of the data.

- Accessibility Statement

- [NOS Accessibility Statement](#)

Login

NOS Constituents Database v4.1 ©2024

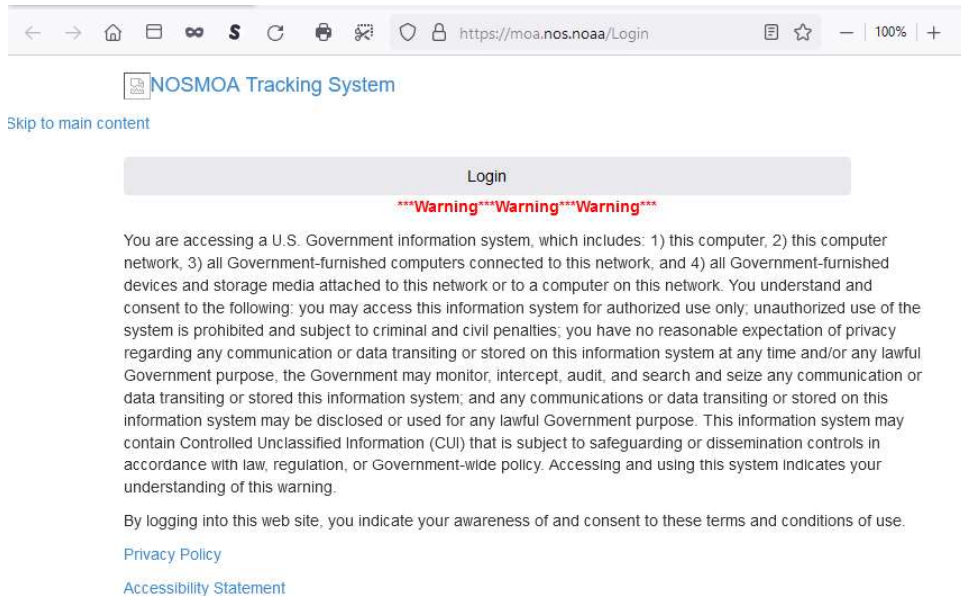
[National Oceanic and Atmospheric Administration](#)

Reviewed January 31, 2017 | Questions, Comments? [Contact Us](#) | [Disclaimer](#) | [Privacy Policy](#) | [Privacy Act Statement](#)
Web Site Owner: [National Ocean Service](#) | [National Oceanic and Atmospheric Administration](#) | [Department of Commerce](#) | [USA.gov](#)

BFD collections leverages the production and development NOS MOA Tracking System (screenshots below show the production and develop web portals)

[BFD MOA Tracking System](#) (Production)

<https://moa.nos.noaa/Login>



WarningWarning***Warning***

You are accessing a U.S. Government information system, which includes: 1) this computer, 2) this computer network, 3) all Government-furnished computers connected to this network, and 4) all Government-furnished devices and storage media attached to this network or to a computer on this network. You understand and consent to the following: you may access this information system for authorized use only; unauthorized use of the system is prohibited and subject to criminal and civil penalties; you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system at any time and/or any lawful Government purpose, the Government may monitor, intercept, audit, and search and seize any communication or data transiting or stored this information system; and any communications or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose. This information system may contain Controlled Unclassified Information (CUI) that is subject to safeguarding or dissemination controls in accordance with law, regulation, or Government-wide policy. Accessing and using this system indicates your understanding of this warning.

By logging into this web site, you indicate your awareness of and consent to these terms and conditions of use.

[Privacy Policy](#)

[Accessibility Statement](#)

[BFD MOA Tracking System](#) (Development)

<https://devmoa.nos.noaa/Login>

NOSMOA - x +

← → ☰ ∞ ↺ S 🔍 🖨️ 🔒 https://devmoa.nos.noaa/Login

 NOSMOA Tracking System

[Skip to main content.](#)

Login

*****Warning***Warning***Warning*****

You are accessing a U.S. Government information system, which includes: 1) this computer, 2) this computer network, 3) all Government-furnished computers connected to this network, and 4) all Government-furnished devices and storage media attached to this network or to a computer on this network. You understand and consent to the following: you may access this information system for authorized use only; unauthorized use of the system is prohibited and subject to criminal and civil penalties; you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system at any time and/or any lawful Government purpose, the Government may monitor, intercept, audit, and search and seize any communication or data transiting or stored on this information system; and any communications or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose. This information system may contain Controlled Unclassified Information (CUI) that is subject to safeguarding or dissemination controls in accordance with law, regulation, or Government-wide policy. Accessing and using this system indicates your understanding of this warning.

By logging into this web site, you indicate your awareness of and consent to these terms and conditions of use.

[Privacy Policy](#)

[Accessibility Statement](#)

Planet Stewards Education Project

Hard copy provided with the funding disbursement form



FUNDING DISBURSEMENT FORM

DISBURSEMENT PURPOSE (Stewardship Project ☐ Travel Reimbursement ☐ Workshop ☐ Other ☐

RECIPIENT INFORMATION

CONTACT FIRST & LAST NAME:

PHONE NUMBER WHERE YOU CAN BE REACHED:

E-MAIL ADDRESS:

DISBURSEMENT INFORMATION

Check appropriate boxes where applicable, then provide information. Complete the bank account and routing number fields if you prefer direct deposit:

FUNDING AMOUNT:

CHECK PAYABLE TO (INSTITUTION ☐ INDIVIDUAL ☐):

MAILING ADDRESS:

BANK ROUTING NUMBER:

BANK ACCOUNT NUMBER:

TAX ID (INSTITUTION ☐ INDIVIDUAL ☐):

Submit completed form (and all receipts – if applicable) to Scott Smith at scott.a.smith@noaa.gov and Megan Harmon at megan.harmon@issmgt.com. **We recommend you make a copy of this and all documents prior to submitting.**

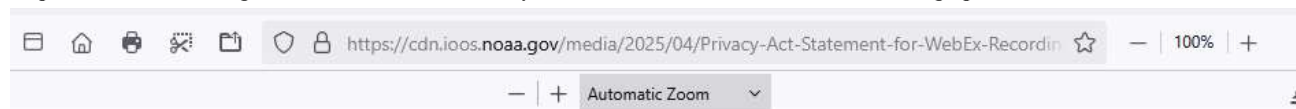
If you are unable to submit via email, mail your forms to Megan Harmon at the address below.

Mailing Address: Megan Harmon
Integrated Systems Solutions, Inc.
8609 Westwood Center Drive, Suite 110
Tysons Corner, VA 22182

Email Bruce.Moravchik@noaa.gov and Mike.Shelby@noaa.gov when you have submitted your form(s), and the amount you have submitted for, but **DO NOT** submit your forms to them.

IOOS PAS for Recording Meetings and Training Sessions

<https://cdn.ioos.noaa.gov/media/2025/04/Privacy-Act-Statement-for-WebEx-Recordings.pdf>



Privacy Act Statement (Record Meetings and Training Sessions)

Authority: The collection of this information is authorized under 5 U.S.C. 301 (*Departmental regulations*), 5 USC 552a (*Records maintained on individuals*); 15 U.S.C. 1512 (*Powers and duties of Department*), and 44 U.S.C. 2904 (General responsibilities for records management).

Purpose: Individual's permission is required for use of photographs, video, and audio in any format, used for communications, outreach, interviews, and dissemination of mission products intended to promote an awareness and appreciation of the environment and NOAA's science, service and stewardship roles.

Routine Uses: The information is used for the purpose set forth above and may be: forwarded to another NOAA or non-NOAA user social media account; shared among NOAA staff for work-related purposes. Photographs, videos, audio recordings may be shared externally and displayed on NOAA websites and social media platforms, and as part of physical displays/exhibits. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among Department staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice [DEPT-18](#), Employees Personnel Files Not Covered by Notices of Other Agencies and [DEPT-23](#), Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs.

Disclosure: Voluntary; by joining and participating in the meeting consent is being given to the recording.