Template Version Number: 01-2021

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

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

Reviewed by: Mark H. 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

GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF.MARK.HYRUM.1514447892
Date: 2023.03.08 09:58:33 -05'00'

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

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NOS/Name of IT System

Unique Project Identifier: NOAA6001

Introduction: System Description
Provide a brief description of the information system.

The National Ocean Service Enterprise Information System (NOSEIS); henceforth recognized as NOAA6001, is a general support system. NOAA6001 is a collection of integrated components architected for providing the NOS information technology-related services. NOAA6001 assets and resources provide NOS staff and program offices technology-based solutions for logical access control, office automation, network connectivity, data storage, and various cloud-based services.

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

NOAA6001 assets consisting of servers, client systems (desktops and laptops), digital storage and network devices are deployed at the Silver Spring Metro Campus (SSMC) in Silver Spring, MD, the NOAA Enterprise Data Center (EDC), in Ashburn, VA, and various program office locations that are located both CONUS and OCONUS.

Microsoft Azure is a FedRAMP approved cloud-based PaaS subscription servicing Assistant Administrator Management and Budget (AAMB) and National Centers for Coastal Ocean Science (NCCOS). Microsoft Azure cloud platforms enables the ability to quickly build, test, deploy, and manage applications and services across a vast network of datacenters, supporting NOS priorities.

The GovDelivery Communications Cloud system (GovDelivery) is a FedRAMP approved SaaS subscription that provides the elements of the NOS with a number of communication features to support the timely dissemination information to the general public.

Digital storage services provided by NOAA6001 for some NOS staff and program offices is delivered via network connectivity to the Cohesity DataProtect application. Cohesity is a software-defined solution for the storage and protection of NOS data. The application operates on a cluster of virtualized hosts managed by IMO system administrators. Cohesity provides short term storage, recovery in the event of a disruption or disaster and serves as the conduit for the long-term storage service provided by the Commercial Azure component of NOAA6001.

Adobe Connect is an (SaaS) application implemented as a video conferencing solution in support of NOS-related mission/business purposes. The information in video audio formats, is recorded by the application or the application can be used to upload content to public-facing social media forums

(i.e. YouTube, Twitter) 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.

Avaya Cloud Secure (Avaya) is a FedRAMP approved SaaS subscription that provides some elements in the NOS a Voice over Internet Protocol (VoIP), voice messaging, Instant Messaging, mobility support to various personnel devices, and Collaboration including basic and advanced audio and web conferencing.

The NOAA6001 kiosk components consist of two GFE laptops in possession of Communications and Education Division (CED) personnel and are managed by the NOAA6001 DIT. These laptops possess software utilized for packaging the content that is displayed by an interactive kiosk. There are 34 interactive kiosks set up at remote locations around the world that allows public consumption of CED outreach program information. The physical devices (kiosks) presenting the information do not belong to the NOAA6001 boundary but to the local institution that acquire the displayed information.

(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 NWave (NOAA0550)
- NOAA Cyber Security Center (NOAA0100)
- Office of Coastal Management (NOAA6101)
- Center for Operational Oceanographic Products and Services (NOAA6205)
- National Centers for Coastal Ocean Science (NOAA6301)
- National Geodetic Survey (NOAA6401)
- Office of Coast Survey (NOAA6501)
- Office of National Marine Sanctuaries (NOAA6602)
- Office of Response and Restoration (NOAA6701)
- NOAA Environmental Security Computing Center (NOAA0520)

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

NOAA6001 device assets are protected in organizational facilities that employ card readers and additional accesses 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 network communications for the NOS enterprise.

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 to all data, including 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).

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

The Network Infrastructure Team (NIT) is responsible for managing the NOAA6001 network infrastructure, ensuring network connectivity and operation. Nit responsibilities includes all aspects of network management such as configuration management, tuning, troubleshooting and installation and maintenance activities for network assets.

The Domain Infrastructure Team (DIT) is responsible for managing NOAA6001 assets and NOS enterprise-level services (e.g. storage and anti-virus), ensuring the that NOS employees are capable of completing assigned roles and responsibilities. DIT responsibilities include all aspects of system administration and management for servers, client systems, access management, printer management, database services, and endpoint security.

NOAA6001 provides the NOS short-term and long-term digital storage services. System engineers manage databases and one major application that deliver these functions. Digital storage consists of business data made up if BII and PII data labels. BII and PII produced by NOS staff and program offices can be derived from travel documents, passport information, badging, email names and addresses and phone numbers. Hard copies of BII and PII are required to be controlled by storing in cabinets that lock and arranged physical access protections.

The major and minor components that make up the NOAA6001 system are summarized below:

- Microsoft Azure Commercial Cloud is a FedRAMP approved IaaS and PaaS cloud service that enables the NOS (CED) to manage four websites that provides the public mission/business content. These websites could process and transmit PII in the form of names, email addresses, images, audio and video recordings, all related to NOS-related topics and interests. The content available on the websites is for public use and consumption. Azure also provides the NOS a its long-term data digital storage solution.

- GovDelivery Communications Cloud is a FedRAMP approved SaaS cloud subscription that provides CED with a number of features to support efficient communications of information to the general public. Access to manage data and its content is limited to only CED employees. The public only receives provided content from the CED. GovDelivery processes and transmits PII in the form of email addresses.

- Adobe Connect is an (SaaS) application managed by CED 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. PII/BII in the form of digital images, audio/video is transmitted by the application.

- CED manages NOS content for public consumption. A digital file is created and can be obtained by vetted partners of the NOS (i.e. museums, science foundations). There are 34 interactive kiosks set up at remote locations around the world that allows public consumption of CED outreach programs and information. 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 NOS BII/PII in the form of images, and audio/video formats that is produced for public consumption.

- Digital data storage services provided by NOAA6001 NOS program and staff offices is delivered via network connectivity to the Cohesity DataProtect application. Cohesity is a 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.

- Avaya Cloud Secure (Avaya) is a FedRAMP approved SaaS subscription that provides some NOS elements, basic Voice over Internet Protocol (VoIP), Voice Messaging, Instant Messaging, mobility support to various personnel devices, and Collaboration including basic and advanced audio and web conferencing.

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

- Microsoft Azure Commercial Cloud: NOS federal and contractor employees that possess privileged level access can retrieve information by leveraging logical access applied to the Azure environment. The public facing websites presented by the service are accessible by non-privileged users (i.e., public users) via navigation to the URL address. The BII/PII that can be viewed by the public are employee names, work addresses, email addresses, images, and digital audio and videos recordings of NOS employees.

- Google Sites: NOS federal and contractor employees that possess privileged access can retrieve information by leveraging logical access within the Google Sites environment. Google Sites functionality resides within the boundary of NOAA0900. This system is not a child system of NOAA6001 and is described as an accessible resource by NOS employees, utilizing services for uploading mission-related 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 possess BII/PII in the form of names, email addresses, and images. These websites are not publicly facing/accessible.

- GovDelivery Communications Cloud: NOS 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.

- 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 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).

- Kiosks: NOS federal and contractor employees that possess privileged access can manage information by leveraging logical access for creating the content for 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.

- GFE: NOS federal and contractor employees are assigned GFE client systems (laptops, desktops, mobile phones and tablets) for the purpose of conducting assigned roles and responsibilities in support of NOS mission and business functions. 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.

- Enterprise storage (Cohesity) and databases are data storage services, that support NOS staff and program offices. The Cohesity application and databases provide digital storage and short-term backup of data. Access to the data 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 the application is limited to personnel in the DIT. 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.

- Avaya Cloud Secure (Avaya) is a FedRAMP approved SaaS subscription that provides the NOS basic Voice over Internet Protocol (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.

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

- BII/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 (client systems) is encrypted at rest.

- 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.

- AAMB has a Local Registration Authority (LRA) function that provides an identification role in support of the NOS 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

Information is processed by based on NOS employee input/interaction with NOAA6001 components. Transmission is conducted by the system via its network infrastructure that is managed by the Network Infrastructure Team (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 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 TLS 1.2 for securing communications.
- Google Sites is not part of NOAA6001. Encryption for data transmission is the responsibility of Consolidated Cloud Applications (NOAA0900). Google Sites provides elements from the NOS to create and host websites for the consumption of NOS personnel only. These websites are deployed to the NOAA Intranet and are not publicly accessible. Logical controls (ICAM) are provided by NOAA0700. The data for the content of the websites is uploaded to the IaaS by NOS federal and contractor employees.
- 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 NOS 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 two GFE laptops and endpoints that display the content for public consumption. 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): 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.

(g) Any information sharing conducted by the system

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 kiosks could share 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

5 U.S.C. 301; 5 U.S.C. 332; 5 U.S.C. 1302; 5 U.S.C. 2951; 5 U.S.C. 3301; 5 U.S.C. 3372; 5 U.S.C. 4118; 5 U.S.C. 5379; 5 U.S.C. 7531; 5 U.S.C. 8347; 15 U.S.C. 1501; 15 U.S.C. 1512; 28 U.S.C. 533-535; 35 U.S.C. 2; 41 U.S.C. 433(d); 44 U.S.C. 3101; 44 U.S.C. 3554; E.O. 9397; E.O. 10450; E.O. 11478; E.O. 12065; E.O. 12564; E.O. 12656; E.O. 12107; E.O. 13164; 5 CFR Part 537; DAO 202-957; DAO 210-110; HSPD-12; FPC 65, July 26, 1999; Pub L. 92-261; Pub. L. 100-7; Pub. L. 106-229; Pub. L. 107-347

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

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non- Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

_____ 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.

__X___ 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.

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. Gender	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): The database utilized by PCAD contains data compiled from public names and business addresses of individuals whom are engaged and have interests with NOS-related missions and programs.					

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

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.

2.4 Is the information covered by the Paperwork Reduction Act?

X	• 0648-0784 External Needs Assessment for NOAA Education Products and Programs • 0648-0712 The Ocean Enterprise: A Study of US Business Activity in Ocean Measurement, Observation, and Forecasting.
	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):			

	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):			

	There is 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 NOS staff and program offices.

NOAA6001 provides to the NOS program and staff offices the services listed in the NOS CIO 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. The public facing websites presented by the service are accessible by non-privileged users (i.e. public users) via navigating to the applicable URL address. The PII that can be viewed by the public are employee names, work addresses, email addresses, images, and digital audio and videos recordings NOS employees.

- 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 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.

- 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).

- 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. PII/BII can be stored on local hard drives of these systems.

- 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. PII/BII is included as human resources data, sensitive government data, credit card information, passport information, contracting data, etc.

- Avaya Cloud Secure (Avaya) is a FedRAMP approved SaaS subscription that provides the NOS basic Voice over Internet Protocol (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.

Manual collection and storage of 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.

- 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 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.

- AAMB has a Local Registration Authority (LRA) that provides services in support of the NOS DOD public key infrastructure (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 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: 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.

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 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			X
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.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NOAA6001 is interconnected with the following systems in concurrence with CSAM: • NOAA NWave (NOAA0550) • NOAA Cyber Security Center (NOAA0100) • Office of Coastal Management (NOAA6101) • Center for Operational Oceanographic Products and Services (NOAA6205) • National Centers for Coastal Ocean Science (NOAA6301) • National Geodetic Survey (NOAA6401) • Office of Coast Survey (NOAA6501) • Office of National Marine Sanctuaries (NOAA6602) • Office of Response and Restoration (NOAA6701) • NOAA Environmental Security Computing Center (NOAA0520) NOAA6001 implements NIST Moderate level physical, technical and administrative controls for protecting interconnected system communication. NOAA6001 device assets are protected in organizational facilities that employ card readers and additional accesses 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 network communications for the NOS enterprise. 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 to all data, including 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).
	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: • 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. Screenshots of the website will be added to the end of this document for reference. • Microsoft Azure Commercial Cloud is utilized for hosting 4 public facing websites which all provide a link to the privacy act. https://oceantoday.noaa.gov/privacy.html • The GovDelivery SaaS provides a copy of the Privacy Act for the public upon signing up for the service. https://granicus.com/privacy-policy/ • The Privacy Act statement for OGC 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. • 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/commitment/ Specific social media privacy links: • Facebook: https://www.facebook.com/privacy/explanation/ • Vimeo: https://vimeo.com/features/video-privacy • Twitter: https://twitter.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. • The DD Form 2841 contains a privacy act statement for the audience to review.

	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 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 employees may decline in writing to provide PII to their supervisors, but this may affect the opportunity of employment. • 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. 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. • Policy and Constituent Affairs Division (PCAD) 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.
X	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 NOS 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.

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 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 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. • There are 34 interactive kiosks set up at remote locations around the world that allows public consumption of CED outreach programs and information. The NOAA6001 kiosk components consist of two GFE laptops in possession of CED personnel and are managed by the NOAA6001 DIT. These laptops possess software utilized for packaging the content that is displayed by an interactive kiosk. 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 NOS 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) is a data storage service, supporting the AAMB, CO-OPS, ONMS, and NCCOS program and staff 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. PII/BII is included as human resources data, sensitive government data, credit card information, passport information, contracting data, etc. 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. • Avaya Cloud Secure (Avaya) is a FedRAMP approved SaaS subscription that provides the NOS basic Voice over Internet Protocol (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. 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, 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. • 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 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 a Local Registration Authority (LRA) that provides services in support of the NOS DOD public key infrastructure (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 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. There isn't an opportunity for individuals to consent how their PII is used. • Office of General Council (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. • 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 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 PCAD for changing email addresses. • AAMB has a Local Registration Authority (LRA) that provides services in support of the NOS DOD public key infrastructure (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 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. 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 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 access or opportunity to review/update PII/BII pertaining 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. • There are 34 interactive kiosks set up at remote locations around the world that allows public consumption of CED outreach programs and information. The NOAA6001 kiosk components consist of two GFE laptops in possession of CED personnel and are managed by the NOAA6001 DIT.

		These laptops possess software utilized for packaging the content that is displayed by an interactive kiosk. 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 Voice over Internet Protocol (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: 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. 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.

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. • There are 34 interactive kiosks set up at remote locations around the world that allows public consumption of CED outreach programs and information. The NOAA6001 kiosk components consist of two GFE laptops in possession of CED personnel and are managed by the NOAA6001 DIT. These laptops possess software utilized for packaging the content that is displayed by an interactive kiosk. 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. • AAMB has a Local Registration Authority (LRA) that provides services in support of the NOS DOD public key infrastructure (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. • Policy and Constituent Affairs Division (PCAD) 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.

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): 10/14/2022 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
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 Accellion 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.

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).

- Kiosks: The laptops storing the information utilize drive encryption for encrypting data at rest. Drive encryption employs FIPS 140-2 compliant algorithms.

- GFE: Windows 10 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): Cohesity employs 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.

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."

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: 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
X	Yes, a SORN has been submitted to the Department for approval on (date).
	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	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
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

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: AAMB quantity of PII/BII collection, storage, and transmission is limited to mission/business purposes only.
X	Data Field Sensitivity	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: 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: 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: N/A

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.)

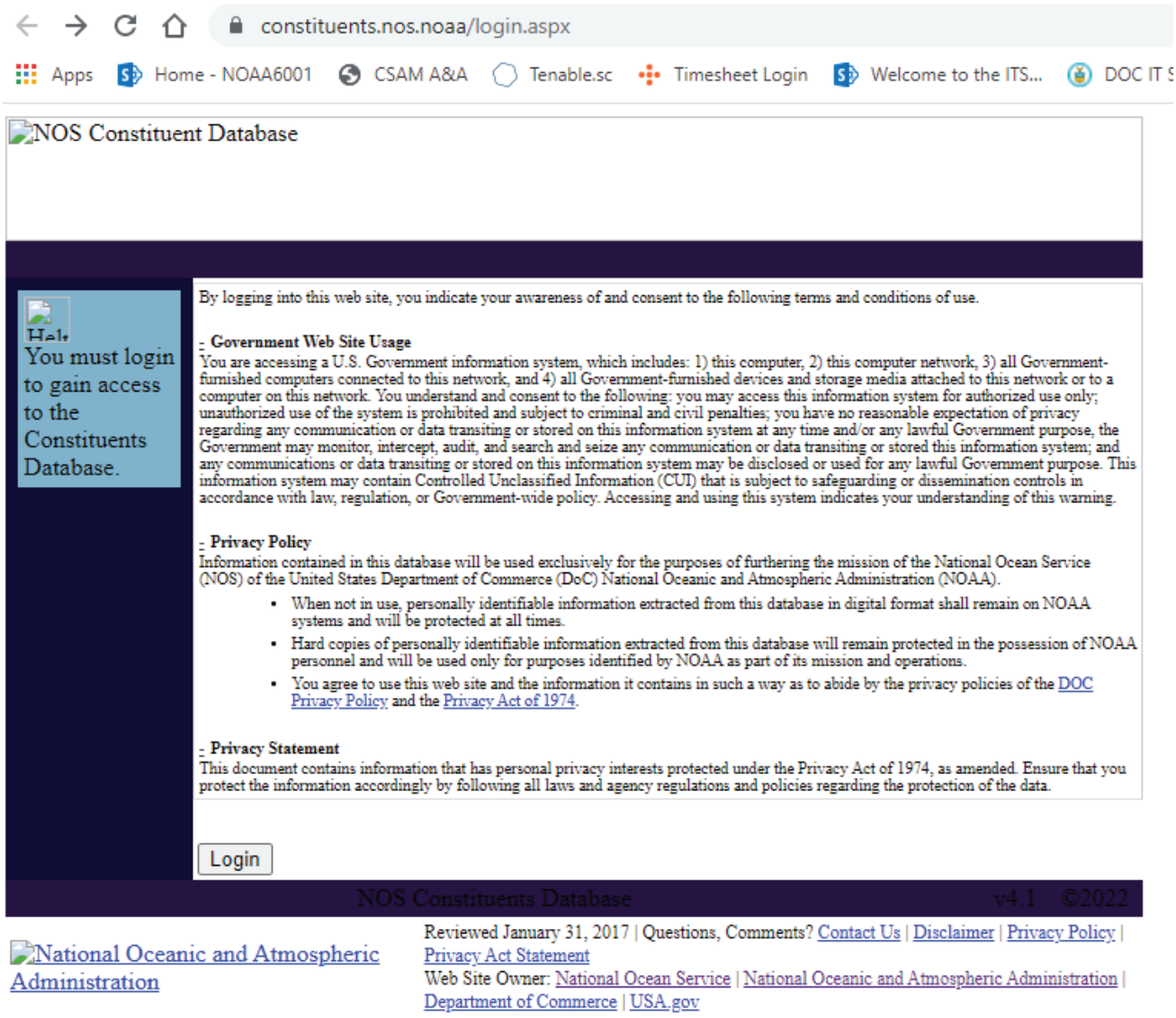
Minimal PII is collected. NOAA6001 collects only enough PII and BII for the necessary purposes of conducting business and completing missions. NOS federal and contractor employees submit/provide PII in order receive the information they request. The only PII attributes that are made available by the 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.


constituents.nos.noaa/login.aspx
Apps
Home - NOAA6001
CSAM A&A
Tenable.sc
Timesheet Login
Welcome to the ITS...
DOC IT S
NOS Constituent Database
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 ©2022
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