Version Number: 01-2019

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOS Enterprise Information System
NOAA6001

Reviewed by: MARK GRAFF, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 04/01/2021

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

U.S. Department of Commerce Privacy Impact Assessment
NOS Enterprise Information System

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

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

The National Ocean Service Enterprise Information System (NOSEIS); and henceforth recognized as NOAA6001, is an general support system made up of an integrated collection of components designed to provide general office automation, network infrastructure, and connectivity services in support of the mission and business functions of the National Ocean Service (NOS).

(b) System location

NOAA6001 system devices primarily reside at the Silver Spring Metro Campus (SSMC) 4, Silver Spring, MD, and multiple NOS field sites around the continental United States. Devices belonging to NOAA6001 are hosted at the NOS enterprise data center, located in Ashburn, VA, which serves as an Infrastructure as a Service (IaaS). Microsoft Azure Web Sites is a cloud service that has been acquired for hosting NOS sponsored websites. The GovDelivery application is a FedRAMP approved service that is a marketing-automation platform that enables the NOS to quickly and easily connect with its constituents (Constituents database). GovDelivery resides in the cloud and is included within the NOAA6001 system boundary of operation. NOAA6001 utilizes websites hosting services offered by the Software as a Service (SaaS), Google Sites. Adobe Connect is a cloud-based SaaS utilized for facilitating web conferencing and presentation services. There are approximately 42 kiosks located at remote locations worldwide that present data and offer public interaction. There is government furnished equipment (GFE) in the form of laptops and desktops that have been identified as a system component of NOAA6001.

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

This is a standalone system providing wide area networking for NOS FISMA systems and backup of shared storage appliance, but no data sharing.

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

NOAA6001 groups elements of the system into three areas, each of which serves a distinct and

specific function:

Network Infrastructure – NOAA6001 supports the NOS SSMC campus backbone and NOS WAN solutions.

Domain Infrastructure – NOAA6001 provides domain infrastructure services to the NOS that provides office automation, supports mission and business operations.

Cloud-Based Applications – NOS utilizes applications that serve the NOS for hosting sponsored government content. The cloud-based applications include web hosting services and software. These applications are described in full within section *e.*

Storage Services – NOAA6001 stores NOS data locally within its file shares for backup of shared storage appliance, but no data sharing. The storage function is only accessible to NOS employees. This function includes database devices and enterprise data storage.

NOAA6001 implements logically access controls for managing access to its system components. The system also utilizes network and information flow restrictions and functions when leveraging externally hosted services (i.e. cloud-based).

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

- Microsoft Azure Web Sites: NOS federal and contractor employees that possess privileged access can retrieve information by leveraging logical access controls provided by the service. The public facing websites presented by the service are accessible by non-privileged users via navigating to the URL accordingly. The PII that can be retrieved are names, addresses, email addresses, images, and digital audio and videos recordings of stakeholders talking about NOS-related topics. The applicable SORNs are noted below in Section 9.2.

- Google Sites: NOS federal and contractor employees that possess privileged access can retrieve information by leveraging logical access controls provided by the service. Non-privilege users are only NOAA federal and contractor employees who can view content and not change it. The data for the content is stored in the cloud with the SaaS. These websites contain PII in the form of names, email addresses, and images. These websites are not publicly accessible.

- GovDelivery: NOS federal and contractor employees that possess privileged access can retrieve information by leveraging logical access controls provided by the service. The data stored within the application is only accessible to NOS privileged users that must be connected to the NOS intranet for access. The application contains PII in the form of email addresses.

- Adobe Connect: NOS federal and contractor employees that possess privileged access can retrieve 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 contains and presents PII in the form of names, email addresses, images and digital audio and videos recordings of stakeholders talking about NOS-related topics. The application 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 controls provided by the software that presents the content on the kiosks. The software is not publicly accessible and non-privileged individuals (e.g. public) can only view content that is being presented. The kiosks present 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. The applicable SORNs are noted below in Section 9.2.

- GFE: NOS federal and contractor employees that possess privileged access can retrieve information by leveraging logical access controls provided by NOAA6001. Its purpose serves the NOS for local storage of PII and facilitates the management and interaction of several components of NOAA6001. GFE is utilized for uploading content to the kiosks, storing PII collected for the NOS Planet Stewards Education Project, uploading data to the Adobe Connect application, and access to all of the externally hosted websites (i.e., Microsoft Azure and Google Sites). GFE is not publicly accessible. PII in the form of names, email addresses, digital audio and videos recordings of NOS federal and contractor employees speaking to NOS-related topics is collected, stored, and/or processed by GFE. The applicable SORNs are noted below in Section 9.2.

- Network storage is a service provided by NOAA6001 and supports numerous elements of the NOS. Storage services include data from multiple NOS program offices for backup of shared storage appliance, but no data sharing. Only NOS federal and contractor employees that possess privileged access and have access to the Intranet can retrieve/view information. PII included is email addresses, names and digital audio and videos recordings of NOS federal and contractor employees speaking to NOS-related topics. PII/BII is included as human resources data, sensitive government data, credit card information, passport information, contracting data, etc.

Manual collection and storage of PII/BII by NOS 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 data is stored on GFE devices and not publicly accessible. The data stored at rest on the GFE is encrypted at rest.

- Policy and Constituent Affairs Division (PCAD) collects and stores both PII and BII for contact and communication purposes within the Constituents database. This data is stored within a database that resides within NOAA6001, thus receives all of the logical protections offered by NOAA6001. The PII data consists of names and email addresses. The PII is not publicly accessible.

- Communications and Education Digitization (CED) of NOAA Videotape Collection - NOAA's video production facility is an extensive collection of professional-level video footage and finished productions about NOAA and it's scientific, educational and outreach endeavors. The collection includes one-of-a-kind, camera-original footage that depicts nationwide and international field operations; master recordings of finished videos by or about NOAA; video documentation of scientific data; interviews with leaders and experts; and celebrations of NOAA milestones dating back to NOAA's beginnings and before. The collection also includes transfers from films that date as far back as the 1940s, documenting decades of historically significant subject matter about NOAA and its predecessor agencies. The PII data consists of images and digital video and audio recordings of NOS federal and contractor employees speaking to NOS-related topics.

- In NOS, the Local Registration Authority (LRA) is responsible for identity verification of NOS administrators that need to request public key infrastructure (PKI) certificates from DOD. This verification process uses form DD-2841 that requires the LRA to enter PII. This form is stored on the NOS network in 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 NOS federal or contractor employee provides the information in person directly to the LRA who returns the artifacts to the individual and does not store images of them on 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.

- General Counsel Ocean and Coasts (GCOC) attorneys collect PII/BII that is shared by NOS program offices for the purpose of legal review and support for FOIA, administrative appeals, litigation, agreements, or other legal reviews. Note: GCOC does not perform the collection of this information. This information is controlled at the NOS program office level and shared to GCOC when applicable.

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

Information is transmitted by the system based on NOS federal and contractor employees input into various applications and databases. Information is transmitted from the system via the network infrastructure for NOAA6001 using existing routing tables and logical connections.

- Microsoft Azure Web Sites enables the NOS to create websites to deploy content to its constituents. The data for the content of the websites is uploaded to the IaaS by NOS federal and contractor employees. These websites transmit information in the form of presenting content via a web page that are publicly accessible.

- Google Sites enables the NOS to create and host websites that deploy content to NOS personnel only. The data for the content of the websites is uploaded to the IaaS by NOS federal and contractor employees. These websites transmit information in the form of presenting content via an intranet web page that is only accessible by NOS personnel (non-privileged users).

- GovDelivery Communications cloud is a marketing-automation platform that enables the NOS to quickly and easily connect with its constituents. The information transmitted to the application is accomplished by personnel navigating to web site and manually inputting their information which is then recorded by the application. The application transmit mission data that is publicly accessible to these constituents using the email addresses that were provided.

- Adobe Connect is a SaaS communications application that provides the NOS with video conferencing services. The information is uploaded by NOS federal and contractor employees via accessing the application with privileged credentials. Information is presented to individuals who have access (non-privileged) to the application for participating in NOS webinars and all-hands meetings. The application is not publicly accessible, however, content can be shared publicly via social media platforms (i.e. YouTube).

- Kiosks are located at approximately 42 locations around the world. The kiosks present information and allow interaction with the public. The data for the content presented by the kiosks are stored locally on GFE that reside within NOAA6001. The kiosks present PII in the form of images and digital audio and videos recordings of NOS federal and contractor employees speaking to NOS-related topics.

- GFE is a NOAA6001 system component. Its purpose is to provide NOS federal and contractor employees local storage of PII and facilitate the management and interaction of with components of NOAA6001. GFE is utilized for uploading content to the kiosks, storing PII collected for the NOS Planet Stewards Education Project, uploading data to the Adobe Connect application, and access to all of the externally hosted websites (i.e. Microsoft Azure and Google Sites). GFE and its content is not publicly accessible. PII in the form of names, email addresses and digital audio and videos recordings of NOS federal and contractor employees speaking to NOS-related topics are collected, stored, and/or processed by GFE.

- Network storage is a service provided by NOAA6001 and supports numerous elements of the NOS. Storage services include data from multiple NOS program offices for the backing up of shared storage appliance, but no data sharing. PII included is email addresses, names, audio and video. PII/BII is included as human resources data in the form of resumes both digital and hard copy the NOAA6001 might keep in their storage

files or on their desks, sensitive government data, credit card information, passport information, contracting data, etc.

Manual collection and storage of PII/BII by NOS 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 data is stored on GFE devices and not publicly accessible. The data stored at rest on the GFE is encrypted at rest.

- Policy and Constituent Affairs Division (PCAD) collects and stores both PII and BII for contact and communication purposes within the Constituents database. This data is stored within a database that resides within NOAA6001, thus receives all of the logical protections offered by NOAA6001. The PII data consists of names and email addresses. The PII is not publicly accessible.

- The LRA uses forms DD-2841 that manually collects PII for DOD issued certificates. This information is transmitted to DOD sources via email.

- General Counsel Ocean and Coasts (GCOC) attorneys (federal and contractor employees) collect PII/BII that is shared by NOS program offices for the purpose of legal review and support for FOIA, administrative appeals, litigation, agreements, or other legal reviews. Note: GCOC does not perform the collection of this information. This information is controlled at the NOS program office level and shared to GCOC when applicable.

(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 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; and
- Still images.

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

- Audio;
- Video; and
- Still images.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting,

maintaining, using, and disseminating the information

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

From NOAA-11: 5 U.S.C. 301, Departmental Regulations and 15 U.S.C. 1512, Powers and duties of Department.

From DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.

From DEPT-18: Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

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

From GSA/GOVT-7: 5 U.S.C. 301; Federal Information Security Management Act of 2002 (44 U.S.C. 3554); E-Government Act of 2002 (Pub. L. 107–347, Sec. 203); Government Paperwork Elimination Act (Pub. L. 105–277, 44 U.S.C. 3504 note); Homeland Security Presidential Directive 12 (HSPD–12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

From OPM/GOVT-1: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons

DEPT-3, Conflict of Interest Records, Appointed Officials

DEPT-4, Congressional Files

DEPT-5, Freedom of Information Act and Privacy Act Request Records

DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons

DEPT-12, OIG Investigative Records

DEPT-14, Litigation, Claims, and Administrative Proceeding Records

DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs

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

NOAA6001 is categorized as a Moderate system.

Section 1: Status of the Information System

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

_____ This is a new information system.

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	
c. Significant System Management Changes		f. Commercial Sources	x	i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): Photographs and Voice Recording/Signature collections including the Adobe Connect and Kiosks added.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015).

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

Section 2: Information in the System

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

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): Common Access Card (CAC) personal identifiers. Only a dollar amount is captured for Planet Steward. And for reimbursement purposes, any credit card data on receipts must be redacted and not stored in the system. Financial accounts are collected in support of the Planet Stewards program. All credit card and financial accounts and transactions are applicable to government accounts.

*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: NOS program offices collected SSNs in support of official duties that administrative-related (e.g. performance reviews, hiring activities, security clearances). SSNs are manually collected and could temporarily maintained within the network storage capability of NOAA6001. GCOC may use social security numbers as part of the OSY/security clearance process for interns, staff hiring, and other personal forms. These forms are stored in hard copy format in a controlled file locked cabinet within GCOC office spaces.

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. Physical Characteristics	
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		j. Proprietary or Business Information	x
c. Work Address	x	g. Work History	x		
d. Work Telephone Number	x	h. Employment Performance Ratings or other Performance Information	x		
k. Other work-related data (specify): GCOC PII may contain salary and employment performance information. These forms are stored in hard copy format in a controlled file locked cabinet within GCOC office spaces. There is a potential for GCOC to receive confidential business information.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs	x	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures	x	f. Vascular Scan		i. Dental Profile	
j. 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		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		Private Sector	x	Commercial Data Brokers	
Third Party Website or Application			x		
Other (specify): The Constituents Database is compiled from public media providing names and business addresses of people with whom NOS routinely engages who have a known interest in the NOS mission and program, from public-facing websites.					

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

The data owners review PII and BII at least annually via manual audits. If the data is outdated, it is the responsibility of the data owner to correct any inaccuracies. NOAA6001 does implement privacy-related security controls for ensuring the accuracy of the information processed, stored, and/or transmitted.

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. 0648-0784 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):			

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 of stakeholders talking about NOS-related topics.			

	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): GCOC performs (litigation and civil enforcement activities) administrative matters including procurement, grant award activities, administration of FOIAs, records requirements, agreements and financial assistance awards, and support of agency legal requirements.			

Section 5: Use of the Information

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

In addition to the general purpose office automation support (i.e., file/printer sharing, application hosting, collaboration, etc.), NOAA6001 provides help desk services, web application/services and data storage to the line offices of the NOS.

NOAA6001 file shares store PII and BII on an ad-hoc basis. This data is part of the application and hiring of NOS federal and contractor employees, including electronic copies of resumes, the processing of human resource data about employees, and hiring ranking are stored temporarily during the hiring phase. 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 is also included. The travel information collected is kept in both hard and soft forms. The hard copies are kept in a locked file cabinet and the soft copies are kept on the shared drive in a folder accessible only to travel admins. The travel documents contain only the traveler's name, home address, and a truncated vendor number associated to the traveler's name. There could be SSN and DOB stored within NOAA6001 file shares that resulted from manual collection by various NOS program offices.

NOAA6001 collects PII/BII in support of different business functions to include human resource support to NOAA, travel data, acquisition data and general office support-related activities.

Major NOAA6001 applications, services, and programs that collect, store, and/or process PII/BII:

- Microsoft Azure Web Sites enables the NOS to create websites to deploy content to its constituents. The data for the content of the websites is uploaded to the IaaS by privileged users (federal employee and contractor). These websites contain PII in the form of names, email addresses, images, audio and video of federal employees and contractors talking about NOS-related topics. The websites are publicly accessible. The PII could be used by individuals accessing the websites for informational purposes (i.e., education, news, information sharing).

- Google Sites enables the NOS to create and host websites that deploy content to NOS personnel only (federal employee and contractor). The data for the content is stored in the cloud with the SaaS. These websites contain PII in the form of names, email addresses, and images of federal employees and contractors. These websites are not publicly accessible. The PII used by individuals accessing these websites are for mission/business related purposes.

- GovDelivery Communications cloud is a marketing-automation platform that enables the NOS to quickly and easily connect with its constituents. The data stored within the application is only accessible to NOS privileged users (federal employee and contractor) that must be connected to the NOS intranet for access. Users can sign up for the services offered by GovDelivery by submitting an email address. The application contains PII in the form of email addresses belonging to members of the public. The PII used by this application is for the purpose of communicating with constituents via email addresses.

- Adobe Connect is a SaaS communications application that provides the NOS with video conferencing services. The data for the content presented by the application is stored in the cloud. The application contains PII in the form of names, email addresses, images, audio and video belonging to federal employees and contractors talking about NOS-related topics. The application is not publicly accessible, however, the content is shared publicly via social media and other publicly accessible platforms (i.e., YouTube). The PII is used for information sharing purposes related to NOS related activities.

- Kiosks are located at approximately 42 locations around the world. The kiosks present information and allow interaction with the public. The data for the content presented by the kiosks are stored locally on GFE that reside within NOAA6001. The kiosks present PII in the form of images and audio and video of federal employees and contractors talking about NOS-related topics. CED requires Notice and Consent forms signed by all employees and contractors who participate in the productions.

- GFE is a NOAA6001 system component. Its purpose serves the NOS for local storage of PII and facilitates the management and interaction of several components of NOAA6001. GFE is utilized for uploading content to the kiosks, storing PII collected for the NOS

Planet Stewards Education Project, uploading data to the Adobe Connect application, and access to all of the externally hosted websites (i.e. Microsoft Azure and Google Sites). GFE is not publicly accessible. PII in the form of names, email addresses and digital audio and video belonging to members of the public talking about NOS-related topics are collected, stored, and/or processed by GFE.

- Network storage is a service provided by NOAA6001 and supports numerous elements of the NOS. Storage services include data from multiple NOS organizations for backup of shared storage appliance, but no data sharing. 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 that belongs to NOS federal and contractor employees. The PII/BII is utilized for mission/business purposes.

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

- PII is collected to support the NOS Planet Stewards Education Project. The PII collected as part of this effort consists of members of the public individual and business names, mailing addresses, phone numbers, email addresses, fax numbers, and business tax IDs. All PII data is stored on GFE devices and not publicly accessible. The data stored at rest on the GFE is encrypted at rest. The PII is used for program office purposes in support to the Planet Stewards Education Project.

- Policy and Constituent Affairs Division (PCAD) collects and stores both PII and BII for contact and communication purposes within the Constituents database. This data is stored within a database that resides within NOAA6001, thus receives all of the logical protections offered by NOAA6001. The PII data consists of names and email addresses of members of the public and external government agency personnel. The PII is not publicly accessible. The PII is utilized by the program office for maintaining communication with its constituents.

- In NOS, the Local Registration Authority (LRA) is responsible for identity verification of NOS administrators that need to request public key infrastructure (PKI) certificates from DOD. This verification process uses form DD-2841 that requires the LRA to enter PII. This form is stored on the NOS network in 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 employee provides the information in person directly to the LRA who returns the artifacts to the user and does not store images of them 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 user to whom he grants access.

- General Counsel Ocean and Coasts (GCOC) attorneys collect PII/BII that is shared by NOS program offices for the purpose of legal review and support for FOIA, administrative appeals, litigation, agreements, or other legal reviews. Note: GCOC does not perform the collection of this information. This information is controlled at the NOS program office level and shared to GCOC 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.)

Data breach or spillage of PII/BII is the primary threat to privacy. Mitigation for these threats to NOAA6001 PII/BII data, logical and physical controls are implemented. In addition, the following is 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): GCOC may share with DOC bureaus and Federal agencies.			

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

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

	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:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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

Class of Users			
General Public	X	Government Employees	X
Contractors	X		
	Other (specify): For general public, users have access to the PII presented by the kiosk component of NOAA6001.		

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 by the following applications: • Microsoft Azure Web Sites all possess a link to a page that contains the applicable Privacy Policy and rights under the privacy act. https://oceantoday.noaa.gov/privacy.html • Google Sites all possess a link to a page that contains the applicable Privacy Policy and rights under the privacy act. https://oceanservice.noaa.gov/privacy.html • GovDelivery possesses a link to the applicable Privacy Policy. https://www.noaa.gov/protecting-your-privacy • The Privacy Act statement and/or privacy policy can be found at: The Privacy Act statement for the Constituents Database can be found at: https://constituents.nos.noaa/login.aspx. NOTE: This is an internal system and not accessible outside of NOS. Screen shots of the privacy policy will be provided to the privacy officers.

	• Adobe Connect: Individuals are provided a notice prior to the beginning of recording the all-hands meetings or webinars talking about NOS-related topics.	
X	Yes, notice is provided by other means.	Specify how: Manual collection and storage of PII/BII by multiple NOS organizations: PII is collected to support the NOS Planet Stewards Education Project. A copy and notification of privacy is conducted at the moment of collection. LRA: The DD-2841 form has a disclosure for the principle purpose(s) for collecting PII.
X	No, notice is not provided.	Specify why not: GCOC does not directly collect PII/BII. GCOC attorneys collect PII/BII that is shared by NOS program 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 office level and shared to GCOC when applicable.

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 their 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. • Adobe Connect is a SaaS communications application that provides the NOS with video conferencing services. Users can decline to be videotaped by not participating in the recording activities talking about NOS-related topics. Manual collection and storage of PII/BII by NOS 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. • Policy and Constituent Affairs Division (PCAD) collects and stores both PII and BII for contact and communication purposes within the Constituents database. They 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: GCOC does not directly collect PII/BII. GCOC attorneys collect PII/BII that is shared by NOS program 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 office level and shared to GCOC when applicable.

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.	• 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 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 not have an opportunity to consent to particular uses of their PII/BII Major NOAA6001 applications, services, and programs that collect, store, and/or process PII/BII: • Microsoft Azure Web Sites enables the NOS to create websites to deploy content to its constituents. The data for the content of the websites is uploaded to the IaaS by privileged users. These websites contain PII in the form of names, email addresses, images and digital audio and videos recordings of stakeholders talking about NOS-

		related topics. The websites are publicly accessible. The application does not collect PII directly therefore the opportunity to consent how PII is used does not present itself. • Google Sites enables the NOS to create and host websites that deploy content to NOS personnel only. The data for the content is stored in the cloud with the SaaS. These websites contain PII in the form of names, email addresses, and images. These websites are not publicly accessible. The application does not collect PII directly therefore the opportunity to consent how PII is used does not present itself. • Adobe Connect is a SaaS communications application that provides the NOS with video conferencing services. Users can decline to be videotaped by not participating in the recording activities talking about NOS-related topics. The application does not collect PII directly, therefore the opportunity to consent how PII is used does not present itself. • Kiosks are located at approximately 42 locations around the world. The kiosks present information and allow interaction with the public. The kiosk components do not directly collect PII, therefore there isn't an opportunity presented to decline. The application does not collect PII directly therefore the opportunity to consent how PII is used does not present itself • GFE is a NOAA6001 system component. Its purpose serves the NOS for local storage of PII and facilitates the management and interaction of several components of NOAA6001. GFE does not directly collect PII, therefore there isn't an opportunity presented to decline. The application does not collect PII directly therefore the opportunity to consent how PII is used does not present itself • Network storage is a service provided by NOAA6001 and supports multiple NOS organizations. The network storage function does not directly collect PII, therefore there isn't an opportunity presented to decline. The application does not collect PII directly therefore the opportunity to consent how PII is used does not present itself Manual collection and storage of PII/BII by NOS 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. There isn't an opportunity for individuals to consent how their PII is used. • Policy and Constituent Affairs Division (PCAD) collects and stores both PII and BII for contact and communication purposes within the Constituents database. They do not 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 send an email can click the unsubscribe button to request that they be removed from the database. There isn't an opportunity for individuals to consent how their PII is used. • In NOS, the Local Registration Authority (LRA) is responsible for identity verification of NOS administrators that need to request public key infrastructure (PKI) certificates from DOD. This verification process uses form DD-2841 that requires the LRA to enter PII. This form is stored on the NOS network in 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 employee provides the information in person directly to the LRA who returns the artifacts to the user and does not store images of them 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 user to whom he grants access. There isn't an opportunity for individuals to consent how their PII is used. • GCOC: Much of the PII/BII information GCOC receives is collected by NOS Program Offices and shared with us for purposes of legal review/support for FOIA, administrative appeals, litigation, agreements, or other legal reviews. The collection of this information would be controlled by the NOS Programs and not by GCOC.

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 employees have an opportunity to review/update PII/BII pertaining to them by coordinating efforts with a supervisor data custodian. Major NOAA6001 applications, services, and programs that collect, store, and/or process PII/BII: • Google Sites enables the NOS to create and host websites that deploy content to NOS personnel only. The data for the content is stored in the cloud with the SaaS. These websites contain PII in the form of names, email addresses, and images. These websites are not publicly accessible. Individuals can review/update PII by communicating a desire to change to the data owner/data custodian. • 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. Changes can be made to individuals email by accessing the application. Manual collection and storage of PII/BII by NOS 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 has been collected can be reviewed/updated by contacting the program office for Planet Steward. • Policy and Constituent Affairs Division (PCAD) collects and stores both PII and BII for contact and communication purposes within the Constituents database. They do not have an opportunity to decline to provide PII/BII, but those users who no longer want to receive information from NOS can send an email requesting that they be removed from the database or if PII needs to be reviewed/updated. In NOS, the Local Registration Authority (LRA) is

		responsible for identity verification of NOS administrators that need to request public key infrastructure (PKI) certificates from DOD. This verification process uses form DD-2841 that requires the LRA to enter PII. This form is stored on the NOS network in 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 employee provides the information in person directly to the LRA who returns the artifacts to the user and does not store images of them 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 user to whom he grants access. Individuals will need to submit a new form DD-2841 in order to update/change PII via the verification process described above.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: • Microsoft Azure Web Sites enables the NOS to create websites to deploy content to its constituents. The websites do not support the functionality for individuals to review/update PII. These websites contain PII in the form of names, email addresses, images and digital audio and video recordings of stakeholders talking about NOS-related topics. • Adobe Connect is a SaaS communications application that provides the NOS with video conferencing services. Users can decline to be videotaped by not participating in the recording activities talking about NOS-related topics. The application does not support the functionality that enables individuals to review/update PII. • Kiosks are located at approximately 42 locations around the world. The kiosks present information and allow interaction with the public. The kiosk components do not directly collect PII, therefore there isn't an opportunity presented for individuals to decline or conduct a review/update of PII. • Network storage is a service provided by NOAA6001 and supports multiple NOS organizations. The network storage function does not directly collect PII, therefore there isn't an opportunity presented for individuals to decline or review/update PII.

		• GFE is a NOAA6001 system component. Its purpose serves the NOS for local storage of PII and facilitates the management and interaction of several components of NOAA6001. GFE does not directly collect PII, therefore there isn't an opportunity presented for individuals to decline or review/update PII. • GCOC does not directly collect PII/BII. GCOC attorneys collect PII/BII that is shared by NOS program 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 office level and shared to GCOC when applicable.

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: NOAA6001 file shares (network storage) store PII and BII on an ad-hoc basis. The file shares are protected with technical and management controls. Administrative controls for monitoring tracking and recording PII is the responsibility of the data owner and program office. • Microsoft Azure Web Sites implement technical controls to restrict access to PII/BII. The IaaS has implemented a High security control baseline. Administrative controls for monitoring tracking and recording PII is the responsibility of the data owner and program office. • Google Sites enables the NOS to create and host websites that deploy content to NOS personnel only. The IaaS has implemented a High security control baseline. Administrative controls for monitoring tracking and recording PII is the responsibility of the data owner and program office. • GovDelivery Communications cloud is a marketing-automation platform that enables the NOS to quickly and easily connect with its constituents. The data stored within the application is only accessible to NOS privileged users that must be connected to the NOS intranet for access. This SaaS has implemented a High security control baseline. Administrative controls for monitoring tracking and recording PII is the responsibility of the data owner and program office. • Adobe Connect is a SaaS communications application that provides the NOS with video conferencing services. The data for the content presented by the application is stored in the cloud and the program office relies on its security function for protecting any PII. • Kiosks are located at approximately 42 locations around the world. The kiosks present information and allow interaction with the public. The data for the content presented by the kiosks are stored locally on GFE that reside within NOAA6001.

	• GFE is a NOAA6001 system component that possesses end point protection and access controls as a means of protecting any PII stored on the hard drive of the device. Manual collection and storage of PII/BII by NOS 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 data is stored on GFE devices and not publicly accessible. The data stored at rest on the GFE is encrypted at rest. • Policy and Constituent Affairs Division (PCAD) collects and stores both PII and BII for contact and communication purposes. This data is stored within a database that resides within NOAA6001, thus receives all of the logical protections offered by NOAA6001. The PII data consists of names and email addresses. The PII is not publicly accessible. • In NOS, the Local Registration Authority (LRA) is responsible for identity verification of NOS administrators that need to request public key infrastructure (PKI) certificates from DOD. This verification process uses form DD-2841 that requires the LRA to enter PII. This form is stored on the NOS network in 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 employee provides the information in person directly to the LRA who returns the artifacts to the user and does not store images of them 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 user to whom he grants access.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): September 30, 2020 ☐ 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).*

All information is stored within the accredited boundaries of NOAA6001is in network data shares controlled by established permission based on the organizational, project, or employee

access rights. Any access to specific restricted files or folders is requested through an access change request, which is reviewed and documented by the NOAA6001 Information System Security Officer for authorization and mission 'need-to-know' requirement prior to implementation.

NOAA6001 implements least privilege through file share permissions to ensure privacy and open only to those demonstrating a "need to know."

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

NOAA6001 IT staff implements the security controls listed in NIST Special Publication 800- 53 R4 required for a moderate system. In compliance with NIST Special Publication 800-53 rev 4, NOAA6001 has a full security program, with performance measures and goals, in order to complete continuous monitoring activities, which include annual security control reviews, quarterly vulnerability scanning, monthly review of security access control list, weekly review of audit logs, handling of access change requests and change control board activities. The risk assessment includes the possible threats and vulnerability to the confidentiality, integrity, and availability of mission and sensitive PII data along with the countermeasures.

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

NOAA6001 implements Microsoft Active Directory for enforcing access control protections for PII/BII stored on its file shares. Least privileged is employed, assuring only individuals with a need to know have logical access to PII/BII. PII/BII that is at rest is protected with FIPS 140-2 compliant encryption. Auditing is employed to address non-repudiation and after-the-fact investigations.

- CED utilizes government furnished equipment (GFE) in the form of laptops for its contractors that support the Planet Steward program. These devices possess endpoint protection mechanisms for encrypting PII/BII at rest. In addition, logical access controls are employed to ensure only authorized users can access the laptops and data stored within.

- Adobe Connect digital audio and video recordings of stakeholders talking about NOS-related topics are encrypted at rest within the files shares of NOAA6001.

- GovDelivery is a FedRAMP approved system that implements FIPS 140-2 compliant encryption mechanisms to protect the confidentiality and integrity names and email addresses stored within the system (data at rest).

- Microsoft Azure Web Sites use TLS for encrypting communication. The data for the content of the websites is uploaded to the IaaS by privileged users only. There is no data to protect at rest. The websites are publicly accessible.

- CED uses Google Sites to create and host websites that deploy content to NOAA6001 personnel only. The data for the content is stored in the Google Sites with the SaaS. These websites contain PII/BII in the form of names, email addresses, and images. These websites are not publicly accessible. Access to the sites is password protected with the google login credentials.

- GovDelivery Communications cloud encrypts the database where the PII resides.

- Adobe Connect is a SaaS communications application that provides the NOS with video conferencing services. The data for the content presented by the application is stored in the cloud. The application contains PII in the form of names, email addresses, images and digital audio and video recordings of stakeholders talking about NOS-related topics. The application is not publicly accessible, however, the content is shared publicly via social media and other publicly accessible platforms (i.e., YouTube).

- Kiosks are located at approximately 42 locations around the world. The data for the content presented by the kiosks are stored locally on GFE that reside within NOAA6001.

- Network storage is a service provided by NOAA6001 and supports multiple NOS organizations. Technical and management controls implemented for NOAA6001 are utilized to protect the confidentiality and integrity of files stored within the system.

- In NOS, the Local Registration Authority (LRA) is responsible for identity verification of NOS administrators that need to request public key infrastructure (PKI) certificates from DOD. This verification process uses form DD-2841 that requires the LRA to enter PII. This form is stored on the NOS network in 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 employee provides the information in person directly to the LRA who returns the artifacts to the user and does not store images of them 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 user to whom he grants access.

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. *(list all that apply)*: OPM/GOVT-1, General Personnel Records DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons DEPT-3, Conflict of Interest Records, Appointed Officials DEPT-4, Congressional Files DEPT-5, Freedom of Information Act and Privacy Act Request Records DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons DEPT-12, OIG Investigative Records DEPT-13, Investigative and Security Records DEPT-14, Litigation, Claims, and Administrative Proceeding Records DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs DEPT-25, Access Control and Identity Management System NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission GSA/GOVT-7 - Federal Personal Identity Verification Identity Management System (PIV IDMS)
X	Yes, a SORN has been submitted to the Department for approval on (date). Submitted 9/25/2019 for the CED Digitization of NOAA Videotape Collection and images on the websites, which is pending.
	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 Records 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 levels. *(Check all that apply.)*

X	Identification	Provide explanation: NOS federal and contractor employees and civilian individuals can be identified. NOAA6001 collects, maintains, and transmits 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: 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 business purposes only and not available to the public. 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 by NOAA6001.
X	Context of Use	Provide explanation: PII/BII that is collected and/or maintained by NOS program offices is used for official mission/business purposes only. PII that is displayed by the remote KIOSKS and Adobe Connect components for public consumption, is in support of NOS missions.
X	Obligation to Protect Confidentiality	Provide explanation: 5 USC 552(b)(4) and the FAR, in accordance with 41 CFR 13.
X	Access to and Location of PII	Provide explanation: Only authorized personnel; which includes NOS federal and contractor employs have access the PII/BII via role-based access control. NOAA6001 implements security controls which employ the principle of least privilege; secure network; transmission, and encrypted data storage. The PII displayed by the remote KIOSK devices allow PII in the form of audio and video recordings and still images of NOS federal and contractor employees to be viewed by the public. The Adobe Connect application enables NOS program offices to share PII with the public making it available via social media platforms (i.e. YouTube).
	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. NOS program offices collect 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.