Version Number: 01-2021

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

Privacy Threshold Analysis for the NOS Enterprise Information System

NOAA6001

Version Number: 01-2021

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NOS/Enterprise Information System

Unique Project Identifier: NOAA6001

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system: *Provide a brief description of the information system.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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 Assistant Administrator/Management and Budget (AAMB) and elements of NOS solutions for office automation, network connectivity, data storage, and various cloud-based services.

Avaya Cloud Secure is a new enterprise-level SaaS VoIP solution employed by NOS and has been assigned to the NOAA6001 production environment.

Address the following elements:

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

NOAA6001 is a general support system.

b) System location

NOAA6001 devices consisting of servers, GFE, and network components are deployed at the Silver Spring Metro Campus (SSMC) in Silver Spring, MD, the NOAA Enterprise Data Center (EDC), in Ashburn, VA, and program office locations that are both CONUS and OCONUS.

Microsoft Azure is a FedRAMP approved cloud-based subscription employed by the NOS for its Infrastructure and Platform as a Service offerings (IaaS/PaaS). Microsoft Azure cloud platforms enables the NOS to quickly build, test, deploy, and manage applications and services across a vast network of datacenters.

The GovDelivery Communications Cloud system (GovDelivery) 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.

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 Domain Infrastructure Team (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.

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 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.

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 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.

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 (NOAA00100)
- 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 Moderate level technical controls for protecting communications with interconnect systems within the provided network (internal) connectivity. IPv4 is the protocol utilized as the internetworking method for connectivity. Access control enforcement is provided by established access control lists (ACL) that enforce authorized access for subjects and objects. These ACLs are designed to prevent unauthorized accesses to data, including PII/BII. NOAA6001 still relies on data loss prevention tools provided at the NOAA level.

NOAA6001 implements Moderate-level physical controls for protection physical network equipment. Locked doors, card readers, and physical access control lists are utilized as the protective mechanisms put into place.

d) The purpose that the system is designed to serve

The primary mission of NOAA6001 is to support the business units and mission objectives of the AAMB staff and program offices. It is also serving as an enterprise-level system for NOS program and staff offices a as a network storage, authentication, endpoint security and network connectivity solution.

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.

Social media services are leveraged by AAMB business units for extending their communications and outreach platforms. These services relay information for public consumption and could be in the form of PII. Social media services actively utilized include:

- https://www.facebook.com/usoceantodaygov/
- https://vimeo.com/noaaoceantoday
- https://twitter.com/NOAAOceanToday
- https://www.flickr.com/photos/usoceangov
- https://www.instagram.com/noaaocean/
- https://www.youtube.com/user/usoceangov

e) The way the system operates to achieve the purpose

The Network Infrastructure Team (NIT) manages NOAA6001 for providing the NOS program and staff offices network connectivity. The NIT as aspects of the NOS network (e.g. LAN and WAN) with configuration management, tuning, and troubleshooting activities.

The Domain Infrastructure Team (DIT) manages NOAA6001 to provide the NOS program and staff offices Active Directory service, anti-virus, Windows management that includes servers, desktops and mobile devices, printer management, Macintosh management, endpoint security (i.e., drive encryption), and web and database applications hosting management.

The storage solution within the NOAA6001 system, is the component that stores PII and BII for the NOS program and staff offices. These data types belonging to these program and staff offices can be derived from hiring processes, business/mission functions (e.g., traveling, passports, badging), email addresses, and phone numbers. When data is processed as soft copy, it is stored within the NOAA6001 system. Hard copies of PII and BII information types are required to be stored in locked cabinets and physical access must be controlled and limited to authorized personnel only.

NOAA6001 system components, including servers, applications, tools, processes and procedures that are configured to provide the following IT services/functions to NOS program and staff offices:

- 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.

- 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.

- 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. PII/BII in the form of digital images, audio/video is processed by the application.

- 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. 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 PII in the form of images, and audio/video formats that is produced for public consumption.

- 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.

- 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.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

NOAA6001 processes information (included PII and BII) in support of the various missions and business functions of the NOS program and staff officers. NOAA6001 operates an enterprise storage appliance for backup of shared storage appliance, but the data belongs to the respective NOS program and staff offices that utilize the storage solution provided by NOAA6001. The type of information collected, maintained, used, and disseminated by the system is mission and business related. For clarifying information that describes the purpose of each line office, navigate to https://oceanservice.noaa.gov/programs/welcome.html.

g) Identify individuals who have access to information on the system

NOS program and staff offices employees (federal and contractor) are granted access to the information system resources offered by NOAA6001. This access is enforced by technical and management controls implemented as part of the security control baseline (Moderate), applied on the system. The access control functionality applies to all NOAA6001 components and is applicable to all personnel permitted logical access to its components. The individual business unit information owners determine which employees are permitted access to and PII/BII processed for mission/business function(s).

There are four public facing systems (web servers) that do permit public access (read only). The type of information accessed is processed by NOAA6001 for public consumption.

h) 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 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. 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 being recorded by the application. The application records information from NOS all hands meetings and webinars and could present 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 controls applied by the server which host the software operating the kiosks. Access to the server and software is controlled and non-privileged individuals (e.g., public) can only view content that is being presented. The kiosks 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 the AAMB, Center for Operational Oceanographic Products and Services (CO-OPS), Office of National Marine Sanctuaries (ONMS), and National Centers for Coastal Ocean Science (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.

- 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 (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.

i) How information is transmitted to and from the system

Information is processed by the system 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 employs 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.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

X__ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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): Avaya Voice is a SaaS soft phone client that has been employed by NOS and is assigned to NOAA6001 as a NOS enterprise-level service. Verbal conversations are considered PII and any conversation could relay PII/BII information that could be sensitive. These conversations will not be saved or recorded.					

____ 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. *Continue to answer questions and complete certification.*

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

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

X__ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

X Yes. *(Check all that apply.)*

Activities			
Audio recordings	X	Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify): Video recordings (Adobe Connect) and voice conversations (Avaya).			

____ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

X Yes, the IT system collects, maintains, or disseminates BII.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

X Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- X DOC employees
- X Contractors working on behalf of DOC
- X Other Federal Government personnel
- X Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs),

including truncated form?

X Yes, the IT system collects, maintains, or disseminates SSNs, 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 transferred and be maintained by 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.
Provide the legal authority which permits the collection of SSNs, including truncated form. Executive Orders: 9397 – Numbering System for Federal Accounts Relating to Individual Persons, as amended by 13478, 9830, and 12107 10450 – Security Requirements for Government Employment 5 U.S.C. § 301 – authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records. 28 U.S.C. 534-535 – FBI / Acquisition, preservation, and exchange of identification records and information; Investigation of crimes involving government officers and employees, limitations

____ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

X Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact

level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

Points of Contact and Signatures

Information System Security Officer or System Owner

Name: Jason Byrd
Office: NOS
Phone: 240-533-0964
Email: Jason.Byrd@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: BYRD.JASON.MICHAEL.1142707752 Digitally signed by BYRD.JASON.MICHAEL.1142707752 Date: 2022.01.18 15:19:34 -05'00'

Date signed:

Information Technology Security Officer

Name: John D. Parker
Office: NOS
Phone: 240-533-0832
Email: John.D.Parker@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: PARKER.JOHN.DARYL.1365835914 Digitally signed by PARKER.JOHN.DARYL.1365835914 Date: 2022.01.19 10:25:54 -05'00'

Date signed:

Privacy Act Officer

Name: Adrienne Thomas
Office: NOAA OCIO
Phone: 240-577-2372
Email: Adrienne.Thomas@noaa.gov

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

Signature: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2022.01.20 12:09:24 -06'00'

Date signed:

Authorizing Official

Name: Paul M. Scholz
Office: NOS
Phone: 240-533-0969
Email: Paul.Scholz@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: SCHOLZ.PAUL.MITCHELL.1365867239 Digitally signed by SCHOLZ.PAUL.MITCHELL.1365867239 Date: 2022.01.19 12:52:07 -05'00'

Date signed:

Bureau Chief Privacy Officer

Name: Mark Graff
Office: NOAA OCIO
Phone: 301-628-5658
Email: Mark.Graff@noaa.gov

I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy.

Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2022.01.25 08:59:33 -05'00'

Date signed: