Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
NOAA6001
National Ocean Service Enterprise Information System (NOSEIS)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NOS/NOEIS

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 NOS staff and program offices technology-based solutions for logical access control, office automation, network connectivity, data storage, and various cloud-based services.

Address the following elements:

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

NOAA6001 is classified as a general support system.

b) System location

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

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

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

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

Adobe Connect is an (SaaS) application implemented as a video conferencing solution in support of NOS-related mission/business purposes. The information in video audio formats, is recorded by the application or the application can be used to upload content to public-facing social media forums (i.e. YouTube, Twitter) in video format for both internal (bureau) and external (public) consumption. PII/BII in the form of digital images, audio/video is processed by the application.

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

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

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

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

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

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

NOAA6001 device assets are protected in organizational facilities that employ card readers and additional accesses based on a need-to-know and/or business requirement (physical access control list).

TLS is the cryptographic protocol utilized for providing communications security to network communications for the NOS enterprise.

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

d) The purpose that the system is designed to serve

The primary mission of NOAA6001 is to support the business units and mission objectives of the NOS staff and program offices. NOAA6001 accomplishes this by serving as an enterprise information system to the NOS by providing service solutions for digital storage management, logical access management, cloud-based services, server and client systems management and network connectivity management. These activities are based on the services identified on the NOS CIO IT Services portal (internal).

Social media services are leveraged by NOS staff and program business units for the purpose of extending a communications and outreach platform. These are employed services that relay information to the public for sharing and consuming information. Some of this information could be in the form of non-sensitive BII and PII. These resources do not operate or reside within the boundary of NOAA6001. Social media resources currently active 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) is responsible for managing the NOAA6001 network infrastructure, ensuring network connectivity and operation. NIT responsibilities includes all aspects of network management such as configuration management, tuning, troubleshooting and installation and maintenance activities for network assets.

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

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

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

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

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

- Adobe Connect is an (SaaS) application managed by CED as a video conferencing solution in support of NOS-related mission/business purposes. The information is uploaded to the application and then the content is transmitted in video format for both internal (bureau) and external (public) consumption. PII/BII in the form of digital images, audio/video is transmitted by the application.

- CED manages NOS content for public consumption. A digital file is created and can be obtained by vetted partners of the NOS (i.e. museums, science foundations). There are 34 interactive kiosks set up at remote locations around the world that allows public consumption of CED outreach programs and information. The physical devices (kiosks) presenting the information do not belong to the NOAA6001 boundary but to the local institution that acquire the displayed information. These systems display NOS BII/PII in the form of images, and audio/video formats that is produced for public consumption.

- Digital data storage services provided by NOAA6001 NOS program and staff offices is delivered via network connectivity to the Cohesity DataProtect application. Cohesity is a software-defined solution for protecting and digitally storing NOS data. The enclave operates on a cluster of virtualized hosts managed by the DIT. Cohesity provides short term storage, recovery vitality in the event of a disruption and serves as the conduit for the long-term storage

service provided by the Commercial Azure component of NOAA6001.

- Avaya Cloud Secure (Avaya) is a FedRAMP approved SaaS subscription that provides NOS elements, 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 (including both PII and BII) to support the various missions and business functions of the NOS. NOAA6001 operates and maintains an enterprise-level digital storage solution for backing up data. The type of information collected, maintained, processed, and transmitted by NOAA6001 is mission and business related. For clarifying information that describes the purpose of NOS staff and program offices, navigate to https://oceanservice.noaa.gov/programs/welcome.html.

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

NOS staff and program office federal and contractor employees are granted access to the information system resources offered by NOAA6001. This access is enforced by Moderate-level technical, administrative and physical controls, that are applied to 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 data owners determine how employees are permitted access to and PII/BII processed for mission/business function(s) based on a need to know and least privilege models.

There are four public facing systems (web-sites) that permit public read-only access. This type of information accessed is 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 applied to the Azure environment. The public facing websites presented by the service are accessible by non-privileged users (i.e., public users) via navigation to the URL address. The BII/PII that can be viewed by the public are employee names, work addresses, email addresses, images, and digital audio and videos recordings of NOS employees.

- Google Sites: NOS federal and contractor employees that possess privileged access can retrieve information by leveraging logical access within the Google Sites environment. Google Sites functionality resides within the boundary of NOAA0900. This system is not a

child system of NOAA6001 and is described as an accessible resource by NOS employees, utilizing services for uploading mission-related BII/PII data types to Intranet websites. Non-privileged users are only NOAA federal and contractor employees who do possess the ability to change content hosted by Google Sites. These internal facing websites possess BII/PII in the form of names, email addresses, and images. These websites are not publicly facing/accessible.

- GovDelivery Communications Cloud: NOS federal and contractor CED employees that possess privileged access can retrieve information by leveraging logical access enforced by Max.gov, for accessing the SaaS. The data stored within the application is only accessible to privileged users that must be connected to the NOAA6001 network for access. The application contains BII/PII in the form of email addresses.

- Adobe Connect: NOS Federal and contractor employees that possess privileged access can access information by leveraging logical access controls provided by the service. NOS federal and contractor employees that possess non-privileged with read only access and view information by participating in the meetings/webinars being recorded by the application. The application records information from NOS all hands meetings and webinars and could present BII/PII in the form of names, email addresses, images and digital audio and video recordings of stakeholders talking about NOS-related topics. The application back end is not publicly accessible; however, the content is shared publicly via social media and other publicly accessible platforms (i.e., YouTube).

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

- GFE: NOS federal and contractor employees are assigned GFE client systems (laptops, desktops, mobile phones and tablets) for the purpose of conducting assigned roles and responsibilities in support of NOS mission and business functions. The GFE component enables NOS employees the ability to access NOAA6001 resources based on role-based access controls. PII/BII can be stored on local hard drives of these systems.

- Enterprise storage (Cohesity) and databases are data storage services, that support some NOS staff and program offices. The Cohesity application and databases provide digital storage and short-term backup of data. Access to the data is enforced utilizing a role-based access schema. Only staff and program office employees that possess authorization, are capable of accessing data. This action can be performed using a GFE. Privileged access to the application is limited to personnel in the DIT. BII/PII could be in the form of email addresses, names and digital audio and videos recordings of stakeholders talking about NOS-related topics, human resources data, credit card information, passport information, contracting data, etc.

- Avaya Cloud Secure (Avaya) is a FedRAMP approved SaaS subscription that provides the

NOS basic Voice over Internet Protocol (VoIP), Voice Messaging, Instant Messaging, mobility support to various personnel devices, and Collaboration including basic and advanced audio and web conferencing. PII/BII can be relayed via audio and video conversations communicated by NOS employees.

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

- BII/PII is collected to support the NOS Planet Stewards Education Project. The PII collected as part of this effort consists of individual and business names, mailing addresses, phone numbers, email addresses, fax numbers, and business tax IDs. All PII/BII data is stored on GFE devices and not publicly accessible. The data stored locally on GFE (client systems) is encrypted at rest.

- Policy and Constituent Affairs Division (PCAD) collects and stores both PII and BII for contact and communication purposes and this data is stored within a database that is a component of NOAA6001. Logical access is granted to authorized personnel based on a role-based schema. The BII/PII data consists of names and email addresses. The database system that stores and manages the BII/PII for this office is not publicly facing or accessible.

- AAMB has a Local Registration Authority (LRA) function that provides an identification role in support of the NOS DOD public key infrastructure (PKI) verification process. The verification process uses form DD-2841 that requires the LRA to process PII. This form is stored in the NOAA6001 system within a password protected zip file. The PII collected consists of the unique identification number from a federal government-issued identification credential with a picture, for example Military ID card or Passport card; the unique identification number from a non-federal government-issued identification card (for example, Driver License card). The form also contains common access card (CAC) card electronic data interchange personal identifier (EDIP), full name, work email, work phone number. Only the numbers are collected from the artifacts and stored in the system. The LRA has posted a privacy act statement at the LRA station. The LRA provides a hard copy of the privacy act statement to each individual granted access.

- Office of General Council (OGC): These attorneys collect PII/BII that is shared by NOS program and staff offices for the business purpose of legal review and support for FOIA, administrative appeals, litigation, agreements, or other legal reviews. Note: OGC does not conduct the collection of this information. This information is controlled at the NOS program and staff office levels and shared to GCOC when applicable.

i) How information is transmitted to and from the system

Information is processed by based on NOS employee input/interaction with NOAA6001 components. Transmission is conducted by the system via its network infrastructure that is managed by the Network Infrastructure Team (NIT). The NIT is responsible for managing the procedures, methods, and tools required to effectively operate, administrate, and maintain the

NOAA6001 network.

- Microsoft Azure Commercial Cloud: The cloud service employs FIPS 140-2 validated encryption to data transmission for any provided services. NOAA6001 employs FIPS 140-2 encryption for communications between it and the cloud service. The service implements TLS 1.2 for securing communications.
- Google Sites is not part of NOAA6001. Encryption for data transmission is the responsibility of Consolidated Cloud Applications (NOAA0900). Google Sites provides elements from the NOS to create and host websites for the consumption of NOS personnel only. These websites are deployed to the NOAA Intranet and are not publicly accessible. Logical controls (ICAM) are provided by NOAA0700. The data for the content of the websites is uploaded to the IaaS by NOS federal and contractor employees.
- GovDelivery Communications Cloud: The SaaS application utilizes TLS 1.2 or higher encryption for connections to the system service offerings.
- Adobe Connect: The application is accessed via utilizing GFE. The data (PII/BII) transmission is protected with TLS 1.2, the protocol employed by NOAA6001. Adobe Connect is a SaaS communications application that provides the NOS with video streaming of NOS conferences and meetings. Note: Individuals can decline to be videotaped by not participating in the recording activities talking about NOS-related topics. The disclaimer presented prior to the recording session is added to this document.
- Kiosks: The kiosk components consist of two GFE laptops and endpoints that display the content for public consumption. The displaying endpoints (kiosks) at the remote locations are not in the boundary of NOAA6001. The laptops are utilizing TLS 1.2 for encrypting communications.
- GFE: Laptops and desktops are configured to utilize TLS 1.2 for encrypting network communications.
- Network storage (Cohesity): The application is hosted and managed by the DIT. The administrators access the application using GFE utilizing TLS 1.2 for encryption network communication.
- Avaya Cloud Secure (Avaya): The application is configured to implement TLS 1.2 for security voice communication.

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.*

____ 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):					

____ 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.*

X___ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment. *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): Audio and video recordings (Adobe Connect) and voice conversations and recordings (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 office employees could collect SSNs in support of official duties that are administrative-related (e.g., performance reviews, hiring activities, security clearances). SSNs are collected manually and hard copies of this data type could digitally transfer and be 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 collect 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. 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.

CERTIFICATION

__X__ The criteria implied by one or more of the questions above **apply** to NOAA6001 and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_____ The criteria implied by the questions above **do not apply** to NOAA6001 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Jason Byrd Office: NOAA/NOS/AAMB/IMO Phone: 240-533-0964 Email: Jason.Byrd@noaa.gov Signature: BYRD.JASON.MICHAEL.1142707752 Digitally signed by BYRD.JASON.MICHAEL.1142707752 Date: 2023.01.24 08:46:22 -05'00' Date signed:	**Information Technology Security Officer** Name: John D. Parker Office: NOAA/NOS/AAMB/IMO Phone: 240-533-0964 Email: John.d.Parker@noaa.gov Signature: PARKER.JOHN.DARYL.1365835914 Digitally signed by PARKER.JOHN.DARYL.1365835914 Date: 2023.01.24 13:46:39 -05'00' Date signed:
Privacy Act Officer Name: Robin Burress Office: NOAA OCIO Phone: 828-271-4695 Email: robin.burress@noaa.gov Signature: BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2023.02.13 10:44:30 -05'00' Date signed:	**Authorizing Official** Name: Cherish Johnson Office: NOAA/NOS/AAMB Phone: 202-936-5744 Email: Cherish.Johnson@noaa.gov Signature: JOHNSON.CHERISH.KEANN.1380835840 Digitally signed by JOHNSON.CHERISH.KEANN.1380835840 Date: 2023.02.10 18:08:18 -05'00' Date signed:
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2023.03.07 09:38:46 -05'00' Date signed:	

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PTA.