U.S. Department of Commerce

NOAA

Privacy Threshold Analysis for the

NOS Enterprise Information System

NOAA6001

U.S. Department of Commerce Privacy Threshold Analysis
NOS Enterprise Information System
(NOAA6001)

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

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 and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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).

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, 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. NOAA6001 components and devices 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 an IaaS 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 incorporated 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 purpose that the system is designed to serve

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.

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, the processing of human resource data about NOS federal and contractor 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. 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.

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 NOS federal and contractor employees that possess privileged access. 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.

- 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.

- 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 federal and contractor employees that possess privileged access 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.

- 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 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 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 stakeholders talking about NOS-related topics.

- 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 videos recordings of stakeholders 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 video 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.

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.

- 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 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: NCOC does not perform the collection of this information. This information is controlled at the NOS program office level and shared to GCOC when applicable.

e) The way the system operates to achieve the purpose

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 *d.*

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 federal and contractor 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).

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

NOAA6001 processes information (included PII and BII) in support of the various missions and business functions of the NOS. NOAA6001 operates an enterprise storage appliance for backup of shared storage appliance, but the data belongs to the respective NOS program offices. 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/.

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

NOS federal and contractor employees are the individuals that possess privileged access to information within NOAA6001. This access is enforced by technical and management controls implemented as part of the security control baseline implemented on the system. This type of access includes access to all components of the system (i.e., privileged access to externally hosted websites, GFE, Adobe Connect, and locally hosted services and functions).

The publicly accessible content is read only. Publicly accessible content does include PII (e.g. names, email addresses, images, and digital audio and videos recordings of stakeholders talking about NOS-related topics) presented by the NOS public facing websites and kiosks and is accessible by the public (read only access).

h) 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.

- Google Sites: NOS federal and contractor employees that possess privileged access can retrieve information by leveraging logical access controls provided by the service. Non-privileged 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.

- 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 and digital audio and videos recordings of stakeholders 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 program offices for backup of shared storage appliance, but no data sharing. Only NOS federal and contractor employees that possess privileged access that have access to the Intranet can retrieve/view information. 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.

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.

- 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: NCOC does not perform the collection of this information. This information is controlled at the NOS program office level and shared to GCOC when applicable.

i) 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 a web page that are 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 level) to the application for participating in NOS webinars and all-hands meetings. The application is not publicly accessible, however, the 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 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.
- 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 (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: NCOC does not perform the collection of this information. This information is controlled at the NOS program office level and shared to GCOC when applicable.

Questionnaire:

1. 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	X	i. Alteration in Character of Data	
j. 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. *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 (version 01-2015).

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 (version 01-2017 or later). *Skip questions and complete certification.*

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			

___ 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
- ____ National Institute of Standards and Technology Associates
- 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.

Provide an explanation for the business need requiring the collection of SSNs, 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.
Provide the legal authority, which permits the collection of SSNs, including truncated form. The legal authority for collecting SSNs can be found in the following SORN: COMMERCE-18, Employee Personnel Files Not Covered By Notices of Other Agencies

____ 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 approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

I certify the criteria implied by one or more of the questions above **apply** to the NOS Enterprise Information System and as a consequence of this applicability, I will perform and document a PIA for this IT system.

Name of Information System Security Officer (ISSO): Jason Byrd

Signature of ISSO: BYRD.JASON.MICHAEL.1142707752 Digitally signed by BYRD.JASON.MICHAEL.1142707752 Date: 2021.02.16 10:16:45 -05'00' Date: _____

Name of Information Technology Security Officer (ITSO): John D. Parker

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2021.02.16 11:48:22 -05'00' Date: _____

Name of Privacy Act Officer (PAO): Adrienne Thomas

Signature of PAO: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2021.02.17 09:15:28 -06'00' Date: _____

Name of Authorizing Official (AO): Paul M. Scholz

Signature of AO: SCHOLZ.PAUL.M.1365867239 Digitally signed by SCHOLZ.PAUL.M.1365867239 Date: 2021.02.17 06:39:16 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2021.03.08 12:11:12 -05'00' Date: _____