Template Version Number: 01-2021

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

Privacy Threshold Analysis for the
NOAA6101

Office for Coastal Management (OCM) General Support System

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NOS/Office for Coastal Management General Support System

Unique Project Identifier: NOAA6101

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 mission of the National Oceanic and Atmospheric Administration (NOAA) NOAA6101, Office for Coastal Management (OCM) is to catalyze and influence a broad base of leaders, citizens, and coastal practitioners to ensure healthy coastal ecosystems, resilient coastal communities, and vibrant and sustainable coastal economies. The coast and its residents are at the epicenter of the impacts of changes in weather, climate, demographics, and economies. OCM manages coastal resources and uses through strengthening governance and investments in the development and implementation of comprehensive policies, rules, and plans. OCM administers the Coastal Zone Management Act, the Coral Reef Conservation Act, the Deep Seabed Hard Mineral Resources Act of 1980, and the Ocean Thermal Energy Conversion Act of 1980.

New additions since the last PIA:

- None

New removals since the last PIA:

- None

Address the following elements:

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

NOAA6101 is a general support system used to ensure that the Office for Coastal Management's (OCM's) operational, programmatic and internal administrative needs are met. The system is an integrated collection of subsystems designed to provide general office automation, infrastructure, and

connectivity services to the National Oceanic and Atmospheric Administration's (NOAA) Office for Coastal Management (OCM).

b) *System location*

Federal Law Enforcement Training Center (FLETC), North Charleston, SC
NOAA Inouye Regional Center (IRC), Honolulu, HI
Stennis Space Center, MS
Ronald V. Dellums Federal Building, Oakland, CA
Silver Spring Metro Center (SSMC), Silver Spring, MD
Microsoft Azure (Central US)
Microsoft Azure (East US)

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

NOAA6101 has interconnections with the following FISMA systems:

NOAA0100 – NOAA Cyber Security Center (H) NOAA OCIO (NCSC/ESS/NCIRT) (Managed by NOAA6101) PII is shared (NCIRT tickets, vulnerability data).

NOAA0550 – NOAA Enterprise Network NOAA N-Wave (NOAA Enterprise Network) (Managed by NOAA6101) PII is shared (sensitive information transmitted through the network).

NOAA0700 – NOAA High Availability Enterprise Services (HAES) (EDS/ICAM/NSD) (Managed by NOAA6101) PII is shared (employee addresses and contact information).

NOAA0900 – NOAA Consolidated Cloud Applications (H) Cloud SaaS Applications (ENS/G-Suite/MaaS360/ESRI etc.) (Managed by NOAA6101) PII is shared (NOAA has allowed employees to send and store PII using g-suite products).

NOAA6001 – NOS Enterprise Information System and cloud services (Azure) (Managed by NOAA6001)

Adobe Connect – audio/video recordings are hosted in Adobe Connect Managed Services. PII is shared (audio and video). (Adobe Connect Managed Services # 1331L521A13ES0041)

d) *The purpose that the system is designed to serve*

Internally, NOAA6101 provides services including help desk support, file sharing, data storage, Intranet applications, Internet connectivity, and print services for NOAA6101's users. Externally, NOAA6101 provides services which include web and GIS applications to its partners and the public

that enables NOAA6101 to achieve its mission, which is to support the environmental, social, and economic well-being of the coast by linking people, information, and technology. NOAA6101 also assists the nation's coastal resource management community by providing access to information, technology, and training, and by producing new tools and approaches that often can be applied nationwide.

The OCM Strategic Plan addresses three strategic outcomes for the coastal management community: healthy coastal ecosystems, resilient coastal communities, and vibrant and sustainable coastal economies.

e) The way the system operates to achieve the purpose

NOAA6101 groups elements of the system into three areas, each of which serves a distinct and specific function:

• Network Devices - OCM Wide Area Network (WAN) and OCM Local Area Network (LAN).

• OCM Domain Servers - The domain infrastructure LAN components (File, Print, Application) services.

• Web Application Servers - OCM application and database hosting services

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

Personally Identifiable Information (PII) is manually entered into the system by the administrator or through a bulk upload from a spreadsheet(s).

Social Security Numbers (SSNs) are collected for new NOAA/NOS/OCM employees, and when renewing Common Access Card or Personal Identification Verification (CAC/PIV) cards for staff members. These are transmitted to the NOAA Security Office via a secure file sharing platform that facilitates access to enterprise content sources (i.e., Kiteworks). OCM does not maintain SSNs on the IT system or as hard copy files. Passport numbers are handled in the same way as SSNs. Taxpayer or employer ID information is collected infrequently (see section 5.1 in the OCM Privacy Impact Assessment for more details), but is stored only temporarily on the system.

Point of Contact (POC) information is entered into various applications/web sites as detailed below. This POC information generally consists of name, email, phone number, organization name, and is collected for the following reasons (not exhaustive, and not applicable to each application/site - see Section 5 for specific details):

- preparing collaborative partner project plans
- requesting delivery of data or information

- posting of subject matter expert contact information
- requesting training
- managing task order information
- joining webinars

PII is collected to communicate with OCM customers and stakeholders on topics where they have an explicitly expressed professional interest, or have made a specific request for data or information.

Other PII is collected for OCM staff employment and personnel records (federal/contractor) and OCM visitor access information (federal/contractor/member of the public/foreign national).

Just like DOC, NOAA and NOS internal/public-facing websites, OCM internal/public-facing websites also have photographs of OCM staff involved in research and/or educational programs/activities, voluntarily submitted with implied consent to serve a purpose, reviewed, verified and managed through OCM website content managers prior to publishing them on the websites.

Business Identifiable Information (BII) is collected and maintained for purposes such as contractual agreements and grants.

Details are found below.

NOAA's Office for Coastal Management Business Operations Division collects data containing personally identifiable and business identifiable information (BII) for internal government operations / administrative processes. The processes include:

Employee / Contractor information needed for personnel, performance evaluation, merit rewards, training, travel, accident reporting, etc. This type of PII information is reviewed and updated annually by staff.

Employee / Contractor / Visitors / Foreign National information required by DOC and/or OPM for security purposes and/or background checks. Passport numbers are collected for foreign visitors, sent as appropriate for security checks, and removed from the system. All information is required per DOC PII Policy and Foreign National Processing guidance, as well as the Federal Law Enforcement Training Center (FLETC) Foreign National Visitor Process.

Employee / Contractor emergency contact information for use in call trees and Continuity of Operations Plan (COOP), which includes names, phone numbers, and addresses

Applicant information submitted in response to requests for proposals (RFPs) and/or in response to a solicitation. External grant applications/proposals are not typically collected *by* OCM. Per the NOAA Grants Management Office policy, proposals almost always run through the Grants.gov submission process and end up in the Grants Online system. In rare cases, applicants without access to the Internet [e.g., US Territories] are permitted to submit paper applications. When this happens, OCM scans the proposals and loads them into Grants Online. Any subsequent sharing of grant proposals via email (e.g., for review) must be done via a secure file transfer process (e.g., Grants Online, Accellion/Kiteworks if emailing internally or externally to NOAA, a secure Google Drive or a network location for internal NOAA reviewers, or a password protected website for internal and external NOAA reviewers). Once reviews are complete and awards are made, proposals are removed from the OCM system and the Grants Online system is the official repository.

Typical personal or business identifiable information collected for grant applications includes:

proposer's name
email
phone #
organization name
organization DUNS # or Unique Entity Identifier
employer identification number or taxpayer identification number

For acquisitions, the business identifiable information collected typically includes:

proposer's name
email
phone #
organization name
organization DUNS # or Unique Entity Identifier
Cost proposal information is also collected, and would be considered BII, as it is often proprietary.
Management and technical approaches found in vendor proposals is often considered BII.

Other PII that is being collected and/or made available via Internet / Web sites or applications include the following.

(Any personal information on any of the following sites is voluntary and can be removed by

request at any time.)

Coastal and Marine Management Program (CAMMP): Application that allows for collaborative project planning with partners (State Coastal Zone Management (CZM) and National Estuarine Research Reserves (NERRS)). Data collected includes names, title, email, and budget. This is an internal (authenticated) site and information is not shared publicly.

Coastal Zone Management Act Program Changes is an application where proposed State CZM Program changes are posted for public comment. Information collected includes name, affiliation, email address, city, state, zip code, comments. An email address is collected to verify a user exists and a two-step authentication process is in place to make sure the user receives an email before comments are posted.

Coral Database: Application that collects internal NOAA staff proposals to the NOAA Corals matrix program. This is an internal (authenticated) site and information is not shared publicly.

Data Access Viewer (DAV): Application that receives requests for data from the public. Email addresses are stored to provide a method of contacting the requester when the data is ready for pickup via the OCM web site.

Digital Coast: Publishes contact information of trainers and/or subject matter experts for some trainings listed on the Digital Coast Training page. Information includes name, email, and location. Permission is acquired (via a form) from each trainer before listing their information on the site.

Digital Coast Academy Campus: Digital Coast Academy Campus is the name for a Moodle based Learning Management System (LMS) where online users participate in blended (self-paced and in person) trainings. Required data collected from students includes: name and email address; voluntary information collected with user consent includes, work address, phone number, institution/department, and profile picture.

Estuaries Education: Website that publicly lists some OCM and partner organization POCs (name, organization, email, phone number). POC information is entirely voluntary and can be removed at any time upon request.

Green Infrastructure Database is a catalog of literature resources documenting the effectiveness of using green infrastructure to reduce impacts from coastal hazards.

Information published includes study authors as typical with standard citations.

NERRs and State Coastal Zone Management (CZM) Performance Measures Databases are authenticated applications for NERRs and CZM partners to document grant performance measures in a standardized way, and to work collaboratively with OCM staff. Information collected includes name, organization, email, and phone number. This is an internal site and information is not shared publicly.

National Estuarine Research Reserves (NERRS): Website that publicly lists some partner organization POCs (name, organization, email, phone number), along with OCM POCs. POC information is entirely voluntary and can be removed at any time upon request.

OCM Intranet (Inet): Contains current information on staff, including phone numbers, names, email addresses, and emergency contacts. The system is used to maintain up to date records on staff contact information. This is an internal site and information is not shared publicly.

OCM Staff Info: Contact information for OCM staff. Information published includes name, email and phone number.

Pacific Risk Management ‘Ohana (PRiMO): Web site that publicly lists some partner organization POCs (name, organization, email, phone number, photos), along with OCM POCs. POC information is entirely voluntary and can be removed at any time upon request.

Task Order Management Information System (TOMIS): Application that collects and maintains POC information (name, email, phone, company name) for use in administering various contractor tasks and deliverables. This is an internal site and information is not shared publicly.

Training Manager System: Web site that collects information on training courses, hosts, and participants of OCM training programs. Information that is collected is not shared publicly. Fields collected include (name, organization, address, city, state, zip, email, phone). This is an internal site and information is not shared publicly.

Virtual Conferencing and Webinars: Adobe Connect and Google Meet are being used for virtual meetings and webinars. Adobe Connect recorded webinars are stored on Adobe’s site. Please reference question 2 in the questionnaire section of this document for NOAA guidance on recording Google Meet sessions. Attendee information is anonymized when saved for republishing.

Still images and video on web sites, online newsletters, video streaming, to fulfill OCM's mission to provide coastal information to interested stakeholders and the general-public. Images and video with identified individuals are searchable when included on web pages with descriptive text of the person in the image or video. People identified in images and videos are required to submit a POC Consent Form prior to the images or videos being published.

Uncrewed Systems (UxS): As outlined in the System of Records Notice (SORN) Commerce/DEPT-29 (Unmanned Aircraft Systems, February 2018), the use of UxS for OCM purposes has the potential for inadvertent collection of PII, such as images of individuals along the coastlines that are within the area of study by the UxS vehicle. However, no retrieval of information using any unique identifier within UxS collected datasets will be conducted, and any PII inadvertently collected will be deleted within 30 days. NOAA6101 does not contain any application capable of facial recognition within any captured images. OCM is working with vendors to use UxS (drones) for gathering Light Detection and Ranging (lidar) or aerial photos in order to assist with the accuracy of the mapping of beach, marsh, wetlands, and water study areas. It is anticipated that the UxS collected imagery will be at a resolution to meet organizational needs, but it would not have the ability (resolution or clarity) to uniquely identify any individuals. If the drone goes down during flight, the retrieval of the unit would be at the discretion of the operator, based on safety and technical factors. Inadvertently obtained PII captured during the flight could potentially be retrieved by others from the damaged drone, if technically possible. OCM will comply with all policies and procedures posted on the NOAA Office of Marine and Aviation Operations site as it relates to Uncrewed Systems and as posted to the NOAA Uncrewed Systems Research to Operations site. Relevant policy documents include but are not limited to:

- *NOAA Unmanned Aircraft System Handbook, v1.0, June 2017*
- *NOAA Aircraft Operations Center UAS Policy 220-1-5 (Version 7)*
- *NOAA Uncrewed Systems Research Transition Office Privacy Policy (NOAA OCIO)*

g) *Identify individuals who have access to information on the system*
OCM has dedicated staff assigned by duties such as HR specialists, travel preparers, budget analysts, etc.… whose access to files is managed through role-based access controls for internal NOAA only information. The users of the NOAA6101 systems that collect non-sensitive PII and BII are authorized government employees and contractor affiliates within the program office and approved partners. These systems are not accessible to the public. Public access of information is provided by web application interfaces. Just like DOC, NOAA and NOS internal/public-facing websites, OCM internal/public-facing websites also have photographs of OCM staff involved in research and/or educational programs/activities, voluntarily submitted with implied consent to serve a purpose,

reviewed, verified and managed through OCM website content managers prior to publishing them on the websites

h) *How information in the system is retrieved by the user*

All NOAA6101 users must be furnished with GFE and valid accounts before access is granted. The information is retrieved through applications. Remote access is provided via NOAA's N-WAVE VPN solution. Internal web sites and internal information is only accessible by NOAA6101 employees. General public will only have access to the public web sites. Public data is hosted on publicly accessible web sites which are all hosted with SSL/TLS certificates for enhanced security.

i) *How information is transmitted to and from the system*

All sensitive information identified in section f is transmitted through secure e-mail (Kiteworks), facsimile, or data is manually entered into online web applications such as Travel Manager, CBS, etc. Google mail and G-Suite is used by NOAA6101 for email and data sharing as NOAA preferred provider. Internal data security is provided by defense in depth with layered security for internal data (Physical access, Firewalls, Active Directory, Access Controls, etc.). Public data is hosted on publicly accessible web sites which are all hosted with SSL/TLS certificates for enhanced security. NOAA6101's Communications Office manages its social media sites. PII is manually entered into the system by the administrator or through a bulk upload from a spreadsheet(s).

Social Security Numbers (SSNs) are collected for new NOAA/NOS/OCM employees, and when renewing Common Access Card or Personal Identification Verification (CAC/PIV) cards for staff members. These are transmitted to the NOAA Security Office via a secure file sharing platform that facilitates access to enterprise content sources *(i.e.,* Kiteworks*).* OCM does not maintain SSNs on the IT system or as hard copy files. Passport numbers are handled in the same way as SSNs. Taxpayer or employer ID information is collected infrequently (see section 5.1 in the OCM Privacy Impact Assessment for more details), but is stored only temporarily on the system.

POC information is entered into various applications/web sites as detailed in Section 5 below. This POC information generally consists of name, email, phone number, organization name, and is collected for the following reasons (not exhaustive, and not applicable to each application/site - see Section 5 for specific details):

- preparing collaborative partner project plans
- requesting delivery of data or information
- posting of subject matter expert contact information
- requesting training
- managing task order information
- joining webinars

Adobe Connect recorded webinars are stored on Adobe's site. Attendee information is anonymized when saved for republishing. Adobe Connect is using TLS/SSL.

Please reference question 2 in the questionnaire section of this document for NOAA guidance on recording Google Meet sessions. Google Meet is using TLS/SSL.

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. The use of UxS for data collection has not yet

occurred within OCM. Any planned UxS usage would be via OCM's Coastal Geospatial Services Contract (CGSC) and a new task order would require the submission of an IT Compliance in Acquisitions Checklist

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	X
Video surveillance	X	Electronic purchase transactions	

Other (specify):

Audio/video recordings: Virtual Conferencing and Webinars - Adobe Connect is being used for virtual meetings and webinars. Attendee information and recorded webinars are stored on Adobe site, and when appropriate (i.e. trainings and webinars) published for later viewing. Google Meet recordings have been recently approved within NOAA, in compliance with the NOAA Privacy Office defined Standard Operating Process.

Video Surveillance: Video monitoring occurs in the Charleston, SC office at the front door. The video is streamed to an individual's desk for monitoring, but the data is not recorded, saved, or stored. OCM is only responsible for the video monitoring at the OCM Charleston location, although other NOAA Line Offices are likely responsible for video surveillance at other NOAA locations hosting OCM staff.

Building Entry Readers: Information is captured for physical access to OCM buildings.

The utilization of UxS (drones) to gather aerial photos to assist with the accuracy of mapping of beach, marsh, wetlands, and water study areas. The use of drones is not for surveillance. Although the UxS has the potential to collect PII via patterned single images taken during the drone flight, it is not the purpose of the device and any inadvertently captured PII will be immediately deleted, when identified during the data processing stage.

____ 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.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form. Social Security Numbers (SSNs) are collected for new NOAA/NOS/OCM employees, and when renewing Common Access Card or Personal Identification Verification (CAC/PIV) cards for staff members. These are transmitted to the NOAA Security Office via a secure file sharing platform that facilitates access to enterprise content sources (i.e., Kiteworks). OCM does not maintain SSNs on the IT system or as hard copy files. Passport numbers are handled in the same way as SSNs. Taxpayer or employer ID information is collected infrequently (see section 5.1 in the OCM Privacy Impact Assessment for more details), but is stored only temporarily on the system.

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.

____ 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 the NOAA6101 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 the NOAAXXXX 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: Zack Gamble Office: Office for Coastal Management Phone: 240-622-5799 Email: Zack.Gamble@noaa.gov Signature: GAMBLE.ZACK.WEBSTER.1365896166 Digitally signed by GAMBLE.ZACK.WEBSTER.1365896166 Date: 2023.05.05 18:10:26 -04'00' Date signed:	**Information Technology Security Officer** Name: John D. Parker Office: National Ocean Service Phone: 240-533-0832 Email: John.D.Parker@noaa.gov Signature: PARKER.JOHN.DARYL.1365835914 Digitally signed by PARKER.JOHN.DARYL.1365835914 Date: 2023.05.10 15:16:11 -04'00' 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: 2023.05.22 09:14:23 -04'00' Date signed:	**Authorizing Official** Name: Jeff Payne Office: Office for Coastal Management Phone: 843-212-6520 Email: Jeff.Payne@noaa.gov Signature: PAYNE.JEFFREY.LYNN.1365833881 Digitally signed by PAYNE.JEFFREY.LYNN.1365833881 Date: 2023.05.06 18:37:31 -04'00' 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: 2023.05.22 12:54:33 -04'00' Date signed:	