Version Number: 01-2021

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

Privacy Threshold Analysis for the
NOAA6301
National Centers for Coastal Ocean Science (NCCOS)
Research Support System

Version Number: 01-2021

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NOS/National Centers for Coastal Ocean Science (NCCOS)

Research Support System

Unique Project Identifier: NOAA6301

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: National Centers for Coastal Ocean Science (NCCOS) mission is to deliver ecosystem science solutions for stewardship of the Nation's ocean and coastal resources to sustain thriving coastal communities and economies. NCCOS helps NOAA meet its coastal stewardship and management responsibilities, and provides coastal managers with the scientific information necessary to decide how best to protect environmental resources and public health, preserve valued habitats, and improve the way communities interact with coastal ecosystems.

NCCOS supports NOAA's environmental and economic missions by providing valuable scientific information to its constituents. NCCOS's fundamental principles are:

- To deliver high–quality science in a timely and consistent manner using productive and strong partnerships.
- To develop and maintain relevant research, long-term data collection and analyses, and forecasting capabilities in support of its customers, stakeholders, and partners.
- To build capacity in the private, local, state, and tribal sectors by transferring technology and providing technical assistance and knowledge to its customers and partners.
- To conduct the anticipatory science necessary to manage potential impacts of multiple stressors on coastal ecosystems.

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).

Address the following elements:

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

NOAA6301 is a General Support System. NOAA6301 defined as NCCOS Research Support System (N-RSS) is a General Support System for the National Centers for Coastal Ocean Science (NCCOS) Program Office, and provides the infrastructure, hardware and software necessary to enable the mission of NCCOS, the organization.

b) System location

NOAA6301 has system components in four NCCOS research facilities (Silver Spring, MD; Charleston, SC; Beaufort, NC; Oxford, MD) and Microsoft Azure Cloud.

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

NOAA6301 has interconnections with the following FISMA systems:

- NOAA0100 – NOAA OCIO (NCSC/ESS/NCIRT)
- NOAA0550 – NOAA N-Wave (NOAA Enterprise Network)
- NOAA0700 – NOAA High Availability Enterprise Services (HAES) (EDS/ICAM/NSD)
- NOAA0900 – NOAA Cloud SaaS Applications (ENS/G-Suite/MaaS360/ESRI etc.)
- NOAA6001 – NOS Enterprise Information System

Note: No PII/BII is shared with any of the FISMA systems listed above. NOAA0100, NOAA0550, NOAA0700 and NOAA0900 do not issue interconnection agreements. SLAs with NOAA0550 for NCCOS Silver Spring MD location only is managed through NOAA6001, where as for other NCCOS locations (Oxford MD, Beaufort NC and Charleston SC) it is managed by NOAA6301.

d) The purpose that the system is designed to serve

NOAA6301 provides the network infrastructure, hardware and software necessary to enable the mission of NCCOS, the organization. The NOAA6301 system:

- Provides support to the *Stressor Impacts & Mitigation (SIM)* program that focuses on ecological forecasting, stressor detection, and an understanding of stressor impacts on coastal resources. NCCOS conducts its research in two SIM sub-priorities:
    - Harmful Algal Blooms
    - Biological Effects of Contaminants and Nutrients
- Provides support to the *Marine Spatial Ecology (MSE)* program that integrates a broad spectrum of physical, biological, and social sciences, to inform coastal and marine decision making, and provides unique capabilities to ensure that special places are valued, protected, and preserved, and to assist in growing the economies that are dependent on our nation's maritime resources. NCCOS has identified four MSE sub-priorities:
    - Ecological and Biogeographic Assessments
    - Habitat Mapping
    - Regional Ecosystem Science
    - Coastal Aquaculture Siting and Sustainability
- Provides support to the *Coastal Change* program, that seeks to understand the ecosystem services to improve a community's resistance to the impacts of weather and changing climate conditions, and provide timely and actionable scientific assessments, information, and tools that coastal communities use to make risk management decisions. NCCOS has identified four Coastal Change portfolio sub-priorities:
    - Vulnerability and Risk Assessment
    - Natural and Nature-Based Features
    - Climate Impacts on Ecosystems
    - Restoration
- Provides support to the *Social Science* programs that focuses on the study of connections between people and the environment and prioritizes investigations into these connections within three

interconnected sub-priorities of research:
    - Ecosystem Services Valuation
    - Assessing Human Use
    - Assessing Vulnerability and Resilience
- Provides an operational environment supporting the overall NCCOS mission and division staff located in the Silver Spring Metro Center (SSMC) Campus, MD; Beaufort, NC; Charleston, SC; and Oxford, MD;
- Provides resources supporting the following services – IT acquisition (non-enterprise), facilities coordination (non-SSMC), desktop management, server administration, high performance computing (HPC), data management, print services, application management (static/dynamic websites and specialty applications for GIS/statistical analysis), database administration, field data acquisition, backup and restoration, service desk, mobile device management, and other media support services;
- Provides LAN and WAN services fully managed by NOAA N-Wave (NOAA0550) for all NCCOS locations. Particularly for Silver Spring MD these services are managed by NOAA0550 through NOAA6001 (NOS).

In addition to the general purposes office automation support (file/printer sharing, application hosting, collaboration, etc.) provided by NOAA6301, the system provides help desk services and supports a number of web sites and internal minor applications.

e) The way the system operates to achieve the purpose

NOAA6301 is a logical interconnection of system components (Network Devices, Servers, Workstations, Printers, Storage, Applications, Databases and Miscellaneous Devices) residing in four NCCOS research facilities (Silver Spring, MD; Charleston, SC; Beaufort, NC; and Oxford, MD) and in Microsoft Azure Cloud (East US2 and Central US region). Each research facility contributes to the overall mission of the NCCOS Program Office along with unique partnerships and cooperatives established to support and further strategic science goals. The physical and logical connections are managed through NOAA0550 (NOAA N-Wave) and NOAA6001 (NOS Enterprise Information System). All NOAA6301 research facilities are behind NOAA Trusted Internet Connections Access Provider (NOAA N-Wave). Virtual Routing & Forwarding (VRFs) allow for both the internet connections and private network connections, which is managed through NOAA6001 by NOAA0550. All NOAA6301 *on-prem* IT components exist behind firewalls or on firewalled networks. NOAA6301 IT components in Microsoft Azure Cloud are configured utilizing Azure identity management and networking offerings but are currently not TIC compliant (work in progress with NOAA N-Wave). NOS domain services are implemented entirely within the security boundary provided by NOAA6001. NOAA6301 follows the Firewall Policy as defined by NOAA6001. VPN services are provided by the NOAA0550 through the management of NOAA6001. Private IP address space is supported by network address translation. This level consists of devices which can initiate connections to outside networks. No public access to the private network is permitted. Direct inbound access from the Internet is not allowed. The public network is designed to support services that must be accessible to NOAA collaborators and partners outside the Trusted Private Network. All NOAA6301 applications and databases are hosted in Microsoft Azure Cloud utilizing Platform-as-a-Service (PaaS) deployment model.

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

Scientific Information **–** NCCOS collects, maintains and disseminates scientific information as a part of its mission activities to deliver ecosystem science solutions for stewardship of the Nation's ocean and coastal resources to sustain thriving coastal communities and economies. The information helps to decide

how best to protect environmental resources and public health, preserve valued habitats, and improve the way communities interact with coastal ecosystems. Imagery and spatial data is collected from the utilization of NOAA-approved Uncrewed Aerial System (UAS) for conducting coastal ecology research in remote areas with uneven topography and/or for measuring the performance of Natural and Nature Based Features such as salt marshes, nearshore subtidal habitats, emergent vegetation, elevation and nearshore vegetative communities). The data collected is reviewed as a part of post-flight procedures and any unintentional/accidental collection of PII is deleted immediately. NCCOS adheres to the privacy requirements established by *NOAA UAS Privacy Policy* at all times. No PII will be collected utilizing NOAA-approved UAS without prior notice covering the purpose of the collection and the use of identifiable information will be provided.

PII – Limited PII is collected, stored and maintained for internal COOP, Human Resources, Facility Management and Workforce Planning purposes (federal employee/contractor). Names, telephone numbers and email addresses voluntarily submitted by staff, partners, volunteers, and government and non-government collaborators is collected to facilitate internal and external communications and to facilitate business and collaborative functions. This is not a central collection, but rather separated by function or individual project or person. Information about individuals is gathered during the application and hiring process (electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase), including standard HR information – travel authorization and vouchers, passports and international travel forms (completed by the employee through the travel portal), information for security badging process (contact information only and employee completes the badge application on paper forms which are taken to the *NOAA Office of Security*), and performance appraisal ranking. Information from video surveillance and building card readers is temporarily acquired as a part of facilities safety and security process/procedures is stored within NCCOS Facility Access Control Systems (ACS), accessible only to authorized Facility Managers, to support incident response and review process and is deleted immediately (if not related to any security incidents) after review. Just like DOC, NOAA and NOS internal/public-facing websites, NCCOS internal/public-facing websites also have photographs of NCCOS staff involved in research and/or educational programs/activities, voluntarily submitted with implied consent to serve a purpose, reviewed, verified and managed through NCCOS website content managers prior to publishing them on the websites. NCCOS staff can anytime request the removal/update of a photograph through NCCOS website content managers.

BII – NCCOS collects limited BII during the pre/post acquisition activities associated with the acquisition and management of contracts. The storage is in the form of PDF forms or MS Word documents. Information extracted from *NOAA Grants Online* (NOAA1101) system to support the *NCCOS Grants Management Program* is stored temporarily to facilitate the review process lifecycle. Although it is not the intent to extract sensitive PII from the *NOAA Grants Online* system, it is possible that the information could contain the *Employer Identification Number (EIN)*. The EIN is a non-mandatory field, which may be populated on the grants information made available by federal forms not managed by NCCOS. NOAA6301 does not collect this identifying information directly.

Note: There is *no* major application or database used to collect or store BII or PII. NCCOS does not have a separate HR division since NCCOS utilizes the *NOAA Office of Human Capital Services*. No PII or BII information, except photographs on public-facing NCCOS websites voluntarily submitted by the NCCOS staff with implied consent, is accessible to the public.

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

Access to all information (including limited PII/BII) is stored on restricted access file storage available only

to the specific employee(s) following principle of least privilege, separation of duties and on a need to know basis, by permissions settings and/or passwords. Any data stored on a laptop, is encrypted utilizing McAfee full device encryption. NOAA/NCCOS public-facing websites accessible to the general public provide information meant for public to use.

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

Access to all information (including limited PII/BII) is stored on restricted access file storage available only to the specific employee(s) following principle of least privilege, separation of duties and on a need to know basis, by permissions settings and/or passwords. Any data stored on a laptop, is encrypted utilizing full device encryption. NOAA/NCCOS public-facing websites accessible to the general public provide information meant for public to use.

i) How information is transmitted to and from the system

Scientific information is collected from scientific equipment, other government/non-government entities and partners and from the field. All information is scanned prior to being stored on restricted file storage and transmitted only using NOS/NOAA/DOC managed enterprise solutions (e.g., NOAA Google Suite, DOC Kiteworks, NOS File Storage, NOAA-managed FTP, NCCOS/NOAA Websites etc.).
As a part of the HR, Acquisition and Badging process sensitive information containing PII/BII is transmitted (only if needed) securely only to the concerned via DOC-managed secure file collaboration tool (*Kiteworks*).

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): N/A					

____ 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

tothose 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		Building entry readers	X
Video surveillance	X	Electronic purchase transactions	
Other (specify): N/A			

NOAA6301 Comments: Unintentional/accidental collection of PII may occur during the utilization of NOAA-approved Uncrewed Aerial Systems (UAS) for NCCOS's coastal ecology research activity to collect imagery and spatial data in remote areas with uneven topography and/or for measuring the performance of Natural and Nature Based Features (NNBF). As a part of post-flight procedures, data collected is reviewed and PII if identified any is deleted immediately. NCCOS adheres to the privacy requirements established by *NOAA UAS Privacy Policy* at all times. No PII will be collected utilizing NOAA-approved UAS without prior notice covering the purpose of the collection and the use of identifiable information will be provided. Information from video surveillance and building card readers is temporarily acquired as a part of facilities safety and security process/procedures is stored within NCCOS Facility Access Control Systems (ACS), accessible only to authorized Facility Managers, to support incident response and review process and is deleted immediately (if not related to any security incidents) after review. Just like DOC, NOAA and NOS internal/public-facing websites, NCCOS internal/public-facing websites also have photographs of NCCOS staff involved in research and/or educational programs/activities, voluntarily submitted with implied consent to serve a purpose, reviewed, verified and managed through NCCOS website content managers prior to publishing them on the websites. NCCOS staff can anytime request the removal/update of a photograph through NCCOS website content managers.

____ 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?

____ 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.
Provide the legal authority which permits the collection of SSNs, including truncated form.

X 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 National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301) 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 National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301) 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: Rohit Munjal (ISSO) Office: NOAA/NOS/NCCOS Phone: 240-533-0289 Email: Rohit.Munjal@noaa.gov Signature: MUNJAL.ROHIT.1500946381 Digitally signed by MUNJAL.ROHIT.1500946381 Date: 2021.11.04 08:25:56 -04'00' Date signed:	**Information Technology Security Officer** Name: John D. Parker Office: NOAA/NOS Phone: 240-533-0832 Email: John.D.Parker@noaa.gov Signature: PARKER.JOHN.DARYL.1365835914 Digitally signed by PARKER.JOHN.DARYL.1365835914 Date: 2021.11.04 09:17:29 -04'00' Date signed:
Privacy Act Officer Name: Adrienne Thomas Office: NOAA OCIO Phone: 240-577-2372 Email: Adrienne.Thomas@noaa.gov Signature: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2021.11.12 15:08:31 -06'00' Date signed:	**Authorizing Official** Name: Dr. Steven Thur Office: NOAA/NOS/NCCOS Phone: 240-533-0146 Email: Steven.Thur@noaa.gov Signature: Digitally signed by THUR.STEVEN.M.1365841299 Date: 2021.11.05 06:51:31 -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: 2021.11.16 09:22:48 -05'00' Date signed:	