Template Version Number: 01-2021

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

Privacy Threshold Analysis for the
NOAA6701
Office of Response and Restoration (OR&R) Local Area Network (LAN) System (ORR LAN)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NOS/Office of Response and Restoration Local Area Network

Unique Project Identifier: NOAA6701 DOC Consolidated IT Infrastructure: 006-48-02-00-01-0511-00 (CSAM: 1283)

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:

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 Office of Response and Restoration's (OR&R) mission is to protect and restore ocean and coastal resources from the impacts of oil, chemical, marine debris, other hazards and disasters. The NOAA6701 OR&R Administrative LAN is a General Support System (GSS) with servers located in Seattle, WA and Mobile, AL which collects and maintains Personally Identifiable Information (PII) as part of it's Business Continuity and workforce planning purposes supporting both federal employees and contractors. This data includes the application and hiring of employees with electronic copies of resumes as well as other standard HR information. This data includes travel authorizations, vouchers, passports, (temporarily only and then deleted) international travel forms, information for security badging process, and performance appraisals. The information is in the form of PDF or MS Word documents in secure folders on the OR&R network system.

OR&R no longer receives credit card orders via secure facsimile for Oil Spill Job Aids. However, audio and video recordings of training events are new collections in NOAA6701.

Address the following elements:

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

NOAA6701 is a general support system.

b) System location

NOAA6701 staff and program offices are located on the Silver Spring Metro Center Campus in Silver Spring, MD, the Western Regional Center in Seattle, WA, and the Gulf of Mexico Disaster Response Center in Mobile AL.

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

describing any other systems to which it interconnects)

NOAA6701 interconnects with the following systems:

NOAA0100 – NOAA OCIO (NCSC/ESS/NCIRT)
NOAA0550 - NOAA Research Network (N-Wave)
NOAA0700 – NOAA High Availability Enterprise Services (HAES) (EDS/ICAM/NSD)
NOAA0900 - Consolidated Cloud Application includes UMS, GSuite and MaaS360
NOAA6001 - Active Directory, SCCM, FireEye, McAfee and other enterprise management applications
NOAA6702 – AWS system for high availability web hosting.

d) The purpose that the system is designed to serve

NOAA6701 provides services including help desk support, file sharing, data storage, development, maintenance, Internet connectivity, and print services for the organizational units within OR&R. Externally the system supports the web sites that support response, restoration, marine debris, and disaster preparedness. OR&R has several social media sites (Facebook, Twitter, Flickr) which are used to connect and different audiences like Federal, State, and university partners as well as the public.

e) The way the system operates to achieve the purpose

NOAA6701operates a network infrastructure with virtual and physical servers, workstations, storage area networks, and printers/faxes to support staff in meeting the mission. The NOAA6701 system has internal and external web servers. The internal servers are used for business processes such as the IT help desk, training, tracking budgets, development, etc. The external web sites support our primary mission featuring resources to some of the in house developed applications for supporting responses to oil and chemical spills with tools such trajectory forecasts and modeling (GNOME, ESI, TAP, etc.). In addition, OR&R also hosts sites which are used to report and track status of emergency responses (ResponseLink, IncidentNews). OR&R has several social media sites (Facebook, Twitter, Flickr) which are used to connect and different audiences like Federal, State, and university partners as well as the public.

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

The PII in NOAA6701 includes information on OR&Remployees HR documents such as resumes, information for security badges and travel documents like travel vouchers or passports may be collected. For non-NOAA and public (users who subscribe to ORR newsletters or take training classes offered by ORR) Name, address, email address and organization/affiliation data may be collected. For those who take surveys and in order to follow-up on the surveys to those who consent information (including age, level of education, numbers of adults and children in family, name and home address) may be collected. ResponseLink the primary site utilized by OR&R to communicate with partners and other federal agencies issues username/password to access the site. Email and phone numbers are also gathered to enable communication during an Oil or Chemical spills when

OR&R is requested to respond by one of the external partners. All these data types are stored in word or PDF documents. The NOAA6701 system enables OR&R in providing public outreach, communication, and employee/partner recognition on our public web sites as well as several social media accounts (Facebook, Twitter, Flickr) which may include photos, biographies, and award recognition.

NOAA6701 information sharing is limited: BII is not shared outside of the bureau. PII is shared with the State Department for official travel clearances. NOAA's Office of Human Capital Services (OHCS) handles OR&R's Human Resource (HR) PII. OR&R utilizes NOAA's Travel system NOAA Travel (E2) and does not operate a separate Travel division. Passport information is securely transmitted to the Department of State to obtain foreign travel clearances for employees traveling abroad for official duties. Commerce Business Systems (CBS) ORR utilizes NOAA's Budget and Finance system and does not operate a separate Budget/Finance division. Public surveys are not shared outside the bureau. PII is shared with the Department of Commerce and other Federal bureaus in case of security/privacy breach. Public data is hosted on publicly accessible web sites which are all hosted with SSL/TLS certificates for enhanced security. OR&R Outreach Office manages its social media sites from NOAA6701 workstations. OR&R shares information with NOAA security for the purpose of clearing personnel for hiring, and to receive Common Access Cards.

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

OR&R has dedicated staff assigned by duties such as travel preparers and managers whose access to the files are managed through role-based access controls for internal NOAA only information. For the public outreach, communication, and employee/partner recognition data is available to all users and the public.

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

All internal data is retrieved using Government Furnished Equipment (GFE) with approved applications to open, review, verify, and securely delete the information. Internal data security is achieved by defense in depth approach to security. (Physical access, Firewalls, Active Directory, Access Controls, etc.) Web sites that are only accessible to internal users include Jira, Training, Cost Recovery, GitLab, Trac, and Agreements. General public only have access to the public to response tools that are made available on public web sites. (GNOME, GOODS, CAMEO Chemicals, Incident News) NOAA6701 public web sites may include images, photographs, video and/or audio recordings, biographies, and award recognition. OR&R has several social media sites (Facebook, Twitter, Flickr) which are used for public outreach, communication, and employee/partner recognition. 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 is transmitted through secure e-mail (Kite Works), facsimile, or data is manually entered into online web applications such as E2 Travel Manager, HR-connect, CBS, etc. Google mail and G-Suite is used by NOAA6701 for email and data sharing as NOAA preferred provider. Internal data security is achieved by defense in depth approach to security. (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. OR&R Outreach Office manages its social media sites from NOAA6701 workstations.

Questionnaire:

1. Status of the Information System

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

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

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

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	X*
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): *NOAA6701 records some videoconference training and educational events. The new collections are audio/video recordings of such events.					

____ 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. *Continue to answer 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	*X	Electronic purchase transactions	
Other (specify): *The Disaster Response Center (DRC) utilizes a video surveillance system, which is managed by the DRC staff. Signs indicating that the facility is being monitored by video are posted. The facility does not have security guards and is open 8AM to 5:00PM. This is a stand-alone system which records onto disks which are overwritten every 60 days (or when full). Only the DRC manager and the one IT staff have access to the disks. NOAA6701 records some videoconference training and educational events. **The new collections are audio/video recordings of such events.			

____ 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
- ____ 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 NOAA6701 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 NOAA6701 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: Russell Worman Office: NOAA/NOS Phone: 206-496-8810 Email: Russell.Worman@noaa.gov Signature: WORMAN.RUSSELL.LOWELL.1153249918 Digitally signed by WORMAN.RUSSELL.LOWELL.1153249918 Date: 2023.01.04 09:08:37 -08'00' Date signed: 01/04/2023	**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: 2023.01.06 13:06:47 -05'00' Date signed: 01/06/2023
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: 2023.01.09 08:24:25 -05'00' Date signed: 01/09/2023	**Authorizing Official** Name: Scott Lundgren Office: NOAA/NOS Phone: 240-533-0408 Email: Scott.Lundgren@noaa.gov Signature: Digitally signed by LUNDGREN.SCOTT.RICHARD.1271648894 Date: 2023.01.04 15:20:24 -05'00' Date signed: 1/4/23
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: 2023.01.09 09:21:56 -05'00' Date signed: 4447892	