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)

Version Number: 01-2021

U.S. Department of Commerce Privacy Threshold Analysis

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

Unique Project Identifier: NOAA6701

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 (OR&R) mission is to "To protect and restore ocean and coastal resources from the impacts of oil, chemicals, marine debris, and other hazards. We provide expert leadership, training, and time-critical services that benefit the environment, public, and economy ". The OR&R vision "The Nation's oceans and coasts are healthy for future generations, protected and restored from pollution and other environmental threats.

ORR Mission(s) Supported

The OR&R organization consists of the following mission and business areas:

1. OR&R Headquarters is the support of managing the business such as funding appropriations development and management, personnel management to include human resources, time management, payroll, and office supplies. OR&R headquarters mission is to work with Congress on appropriations as it applies to all OR&R mission. OR&R headquarters also includes General Counsel, the General Counsel for Natural Resources (GCNR), which provides legal advice to the NOAA Fisheries and the NOAA Ocean Service. General Counsel seeks restoration from responsible parties for injuries caused to our Nation's natural resources by releases of hazardous substances; and physical impacts (i.e., vessel grounding) to unique resources in National Marine Sanctuaries.
2. Emergency Response Division (ERD) responds to oil spills, chemical spills, and significant environment incidents. Under the National Contingency Plan, NOAA has responsibility for providing scientific support to the Federal On-Scene Coordinator (FOSC) for oil and hazardous material spills. When spills occur, NOAA Scientific Support Coordinators (SSCs) coordinate scientific information and provide critical information to the FOSC. ERD scientists are multidisciplinary team that includes oceanographers, modelers, biologists, chemists, and geologists. ERD scientists work in Seattle and support the SSCs during spill events, as well as for drills, exercises, and contingency planning. SSCs are strategically located around the country, often within U.S. Coast Guard (USCG) offices, effectively providing local services to

a range of users in public and private sectors. ERD services include:

a. Supporting emergency response activities
b. Support environment contingency plans
c. Develop tools for local decision makers
d. Provide training

ERD facilitates spill prevention, preparedness, and response at national and local levels, and provides expertise on such issues as dispersant use, response countermeasures, and alternative response technologies. ERD's scope encompasses the entire U.S. coastline, including the Great Lakes, Alaska, Hawaii, and U.S. territories. In the last twenty-five years, ERD has responded to almost every major marine spill in the U.S and often sought international environment incidents. In addition, ERD support incidents such as but to limited to downed aircraft, search and rescue, and tracking floating objects.

The Emergency Response Division typically responds to 150-200 incidents annually. Descriptions of some recent responses by ERD are available in our Significant Incidents section. News, photos, and other information about current and historical spill incidents is available at OR&R IncidentNews site at ***incidentnews.noaa.gov***.

3. Assessment Restoration Division (ARD) also support of oil spills, chemical spills, and significant incidents. ARD is responsible for the plan and implement a coordinated, agency-wide damage assessment program to meet the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA), the federal Water Pollution Control Act (Clean Water Act), the Oil Pollution Act of 1990, and the National Contingency Plan. The Damage Assessment Center is responsible to:

   a. Prepare an infrastructure capable of planning and conducting the damage assessment process
   b. Determine injury to natural resources from oil and hazardous substances
   c. Calculate the claim compensation for the public from the potentially responsible parties for those injured resources.

4. Marine Debris Division (MDD) manages waste of consumer materials manufactured or processed disposed or abandoned into the oceans or USA Great Lakes. MDD serves as a centralized program within NOAA to coordinate, strengthen, and promote marine debris activities within the agency and among its partners and the public.

   Research is beginning to show the scope of the issue, and this knowledge, along with new technologies, can lead solutions that are more effective to the problem. Marine debris has many harmful impacts on ecosystems, such as habitat degradation, entanglement, ingestion, and transportation of non-native species. Debris can even affect human health and navigation safety. MDD focuses its efforts to reduce and prevent marine debris decrease not only the quantities but also the impacts of debris, and over time, create an overall change in the behaviors that lead to debris. MDD works with U.S. and international partners to solve the problem of marine debris.

5. Business Operations Division (BOD) is the Budget and Financial Management, Employee Resources, Cost Recovery, and Information Technology. BSG is responsible for the day-to-day operations of the Program Office to include budgets, travel, timekeeping, human resources, information technology (IT), records management, and internal policy and processes. The BSG IT team also supports other OR&R divisions' software development.

6. Disaster Preparedness Program (DPP) is a new program to prepare NOS and partners to respond to and recover from pollution events and natural disasters. The Gulf of Mexico Disaster Response Center (DRC) is a facility as a collaboration hub for NOAA offices in the Gulf of Mexico region to develop and coordinate response plans and to develop collaboration capabilities of a better response community.

   The Center provides two major functions in support of the NOAA mission:

   a. First, the Center provides National Ocean Service (NOS) OR&R management and operations a place to give support staff users with work space for day-to-day business activities; host regional preparedness planning workshops; incident response training activities; and a coordination hub to plan for emergencies. The Center provides NOAA OR&R collaboration users outside of the DRC with the ability to collaborate on business activities.
   b. Second, the Center provides NOAA with a facility that can withstand weather conditions and available for standard users, such as Federal, State, and local environment incident responders. Intended to serve as a safe and ready command center during major disaster responses in the Gulf, the DRC also offers facilities for drills, trainings, workshops, and planning activities.

No information/applications that collect, store, transmit PII/BII have been added/removed from the system.

Address the following elements:

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

The NOAA6701 Administrative LAN is a General Support System (GSS), with a server located in Seattle, Washington, which collects and maintains Personally Identifiable Information (PII) as part of the application and hiring of employees (electronic copies of resumes are stored temporarily during the hiring phase), as well as standard HR information (such as Travel authorization and vouchers, passports (temporarily only and then deleted) and international travel forms, information for security badging process, and performance appraisal ranking). The system receives, via secure facsimile transmission, credit card orders for OR&R products identified for recovery of User Fees (Oil Spill Job Aids), which are processed for payment through the pay.gov website by OR&R staff (i.e. no credit card information is resident on the system or its computers) and is only produced in printed form. The printed forms are kept long enough to process payment and then are securely shredded. OR&R employee and contractor data is collected, stored and maintained for internal OR&R Business Continuity, Human Resource, and workforce planning purposes (federal employee/contractor). The storage is in the form of PDF forms or MS Word documents in a secure folder on the OR&R network.

b) System location

NOAA6701 staff and program offices are located on the Silver Spring Metro Center Campus, Western Regional Center campus, Gulf of Mexico Disaster Response Center, and regional staff located remote offices around the U.S.

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

describing any other systems to which it interconnects)

NOAA6701 interconnects to the following systems:

NOAA6001- Active Directory, and various enterprise management applications.

NOAA0100- Cybersecurity and Incident Response

NOAA0550- Network connectivity

NOAA0700- Authentication services

NOAA0900- g-suite, MaaS360, Microsoft Power BI

NOAA6702- secure connection to AWS environment for administration.

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

NOAA6701 operates with network infrastructure, virtual server infrastructure, physical servers, workstations, and 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&R employees HR documents such as resumes or 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.

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) suing to appropriate application to open, review, verify, and securely delete the information. Internal data is security is provided by defense in depth with layered security for internal data. (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 will 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 is 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. 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.*

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

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_X_ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment. *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

_X_ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to

those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

X Yes. *(Check all that apply.)*

Activities			
Audio recordings		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.			

____ 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: Dana Larson Office: NOAA/NOS Phone: 206-526-6690 Email: Dana.Larson@noaa.gov Signature: LARSON.DANA.KARL.1369458805 Digitally signed by LARSON.DANA.KARL.1369458805 Date: 2022.01.18 10:57:14 -08'00' Date signed: 1/18/2022	**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: 2022.01.20 07:38:50 -05'00' 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: 2022.01.20 12:15:40 -06'00' Date signed: 59600	**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: 2022.01.20 11:24:48 -05'00' Date signed: _____
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov Signature: GRAFF.MARK.HYRUM.15144 Digitally signed by GRAFF.MARK.HYRUM.15144 Date: 2022.01.27 10:33:46 -05'00' Date signed: 47892	