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

Unique Project Identifier: NOAA6701 006-48-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:
The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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

The 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 NOAA6001 (NOS Enterprise Information System) for connection to NOS the campus networks, as well as Internet connectivity. NOAA6701 also interconnects with NOAA6702, the Office of Response and Restoration Products System (ORRPS) which hosts products developed and published by OR&R to support its mission. NOAA6701 provides the Government Furnished Equipment (GFE) and secured systems which are used to connect and manage ORPPS which is hosted in the Amazon Web Services (AWS) East/West FedRamp cloud. Much of the development for ORPPS is completed on NOAA6701 computing assets and then securely used to update and maintain content, user accounts, updates and security through the VPN connection and the AWS console interface.

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, use, 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) using to appropriate application to open, review, verify, and securely delete the information. Internal data is security 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 publically 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 publically 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. What is the status of this information system?

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

   This is a new information system. 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 not a SAOP approved Privacy Impact Assessment. Continue to answer questions and complete certification.

   This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015). Continue to answer questions and complete certification.

   This is an existing information system in which changes do not create new privacy risks.
risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later). Skip questions and complete certification.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?
   NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

   X  Yes. (Check all that apply.)

<table>
<thead>
<tr>
<th>Activities</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio recordings</td>
<td></td>
</tr>
<tr>
<td>Video surveillance</td>
<td>X</td>
</tr>
<tr>
<td>Building entry readers</td>
<td></td>
</tr>
<tr>
<td>Electronic purchase transactions</td>
<td></td>
</tr>
</tbody>
</table>

   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
   ___ National Institute of Standards and Technology Associates
   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?

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.

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.
impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.
CERTIFICATION

X   I certify the criteria implied by one or more of the questions above **apply** to the Office of Response and Restoration (OR&R) Local Area Network (LAN) NOAA6701 and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the Office of Response and Restoration (OR&R) Local Area Network (LAN) NOAA6701 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Dana Larson

Signature of ISSO or SO: LARSON.DANA.KARL.1369458805

Digitally signed by LARSON.DANA.KARL.1369458805
Date: 2020.08.25 16:36:02 -07'00'

Date: _____________

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

Signature of ITSO: PARKER.JOHN.D.1365835914

Digitally signed by PARKER.JOHN.D.1365835914
Date: 2020.08.28 09:50:53 -04'00'

Date: _____________

Name of Privacy Act Officer (PAO): Adrienne Thomas

Signature of PAO: THOMAS.ADRIENNE.M.1365859600

Digitally signed by THOMAS.ADRIENNE.M.1365859600
Date: 2020.09.10 17:20:08 -04'00'

Date: _____________

Name of Authorizing Official (AO): Scott Lundgren

Signature of AO: LUNDGREN.SCOTT.RICHARD.1271648894

Digitally signed by LUNDGREN.SCOTT.RICHARD.1271648894
Date: 2020.09.10 14:04:07 -04'00'

Date: _____________

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

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF.MARK.HYRUM.1514447892
Date: 2020.09.11 13:02:24 -04'00'

Date: _____________