Privacy Threshold Analysis

NESDIS Center for Satellite Applications and Research (STAR) LAN
NOAA5018
U.S. Department of Commerce Privacy Threshold Analysis

NOAA/STAR LAN

Unique Project Identifiers: 006-48-01-16-01-3201-00 and 006-48-01-16-01-3202-00

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:

NOAA5018 is the main scientific IT system for the NESDIS Center for Satellite Applications and Research (STAR).

STAR is the science arm of the National Environmental Satellite, Data, and Information Service (NESDIS), which acquires and manages the nation's environmental satellites for the National Oceanic and Atmospheric Administration (NOAA). STAR research activities, integral to the implementation of NOAA's research priorities, are aligned with and carried out in direct support of NOAA and NESDIS programs, strategic goals, and performance objectives.

STAR's mission is to accelerate the transfer of satellite observations of the land, atmosphere, ocean, and climate from scientific research and development into routine operations, and offer state-of-the-art data, products and services to decision-makers.

NOAA5018 consists of approximately 265 CentOS and RedHat Linux workstations and servers, connected to Cisco/IOS switches and a Cisco ASA firewall. NOAA5018 also contains one Oracle Solaris server, a few OpenBSD systems, a few Apple Mac OS-X systems, a large amount of disk storage systems from Dell, NetApp, and Supermicro, and VMware ESXi hypervisors.

NOAA5018 resides on a private firewalled network, located at the NOAA Center for Weather and Climate Prediction (NCWCP), in College Park, MD 20740.

NOAA5018 is primarily used for scientific research and development. In this respect, it primarily contains scientific data, code, documentation, publications, etc. NOAA5018 does not facilitate e-commerce or other similar transactions. Rather, typical NOAA5018 “transactions” include scientific processes, and scientific data input, output, and production.
a) Whether it is a general support system, major application, or other type of system

NOAA5018 is a General Support System.

b) System location

NOAA5018 is physically located at 5830 University Research Ct Building: NCWCP, College Park, MD 20740

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

NOAA5018 interconnects with the following systems:
- NOAA0100 – NOAA Security Operations Center (SOC)
- NOAA0200 – NOAA Network Operations Center (NOC)
- NOAA0550 – NOAA N-Wave network
- NOAA5006 – NESDIS Headquarters
- NOAA8860 – NWS/Weather and Climate Computing Infrastructure System (WCCIS)

d) The purpose that the system is designed to serve

NOAA5018 is the primary IT system facilitating NOAA/NESDIS/STAR’s mission.

e) The way the system operates to achieve the purpose

NOAA5018 consists mainly of approximately 275 Dell and Supermicro servers running the CentOS Linux operating system; approximately 14 PetaBytes of Dell, NetApp, and Supermicro disk storage, contained within, and external to, the above servers; all on a 10 Gbit LAN consisting of Cisco firewalls and switches, in the Data Center of the NOAA Center for Weather and Climate Prediction (NCWCP), located at 5830 University Research Ct, College Park, MD, 20740.

NOAA5018 also includes a few servers running Mac OS X, OpenBSD, and one Solaris server.
NOAA5018 also utilizes a VMware ESXi, vSphere, and vCenter virtualization environment, within which run approximately 100 virtual CentOS servers.

Major software applications utilized within NOAA5018 include PostgreSQL, Intel and Portland Group Compilers, IDL, Matlab, McIDAS, HDF, NetCDF.

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

NOAA18 handles scientific data - remote-sensing satellite observations of the land, atmosphere, ocean, and climate data provided by Earth-orbiting satellite observing systems.

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

Approximately 300 individuals utilize NOAA5018. 10 of those individuals are privileged IT Administrators of the system. The remainder are non-privileged scientists and developers.

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

Users connect to NOAA5018 from their desktop computers via SSH and use SCP to retrieve information from the system.

i) How information is transmitted to and from the system

Information is transmitted to and from NOAA5018 via SSH, SCP, FTP, FTPS, SFTP, HTTP, HTTPS.
Questionnaire:

1. 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)**
   
<table>
<thead>
<tr>
<th>a. Conversions</th>
<th>d. Significant Merging</th>
<th>g. New Interagency Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>b. Anonymous to Non-Anonymous</td>
<td>e. New Public Access</td>
<td>h. Internal Flow or Collection</td>
</tr>
<tr>
<td>c. Significant System Management Changes</td>
<td>f. Commercial Sources</td>
<td>i. Alteration in Character of Data</td>
</tr>
<tr>
<td>j. Other changes that create new privacy risks (specify):</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   ____ 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 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.

   ____ Yes. **Please describe the activities which may raise privacy concerns.**

   ____ 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.).**
Yes, the IT system collects, maintains, or disseminates BII about: (Check all that apply.)

Companies
Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information
4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: “The term ‘personally identifiable information’ refers to information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc...”

Yes, the IT system collects, maintains, or disseminates PII about: (Check all that apply.)

DOC employees
Contractors working on behalf of DOC
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 PII other than user ID?

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.

4c. 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.

____ 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, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PLA 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 NOAA5018 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 NOAA5018 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): Joseph Brust, SO

Signature of ISSO or SO: 

Date:

Name of Information Technology Security Officer (ITSO): Frank Menzer

Signature of ITSO: 

Date: 8/2/2018

Name of Authorizing Official (AO): Harry Cikanek

Signature of AO: 

Date:

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

Signature of BCPO: 

Date: