U.S. Department of Commerce
National Oceanic and Atmospheric Administration (NOAA)

Privacy Threshold Analysis
For the
NOAA0100, NOAA Cyber Security Center
U.S. Department of Commerce Privacy Threshold Analysis
NOAA0100, NOAA Cyber Security Center

Unique Project Identifier: 006-48-02-00-01-3511-00

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: Provide a general description of the information system and its purpose in a way that a non-technical person can understand. 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.

NOAA0100, the NOAA Cyber Security Center (NCSC) is a functional body of technologies, processes, and practices designed to support the NCSC mission to protect NOAA networks, computers, programs, and data from cyber-attack, damage, and unauthorized access, enabled by the strategic shift of all NOAA Federal Information System Management Act (FISMA) identified systems to practicing continuous monitoring and real-time assessments. NOAA0100 NCSC monitors NOAA security from four locations, Silver Spring, MD; Boulder, CO; Seattle, WA; and Fairmont, WV. All locations receive mirrored traffic of data feeds both incoming and outgoing for all NOAA internal offices. Silver Spring, MD; Boulder, CO; Seattle, WA; and Fairmont, WV receive two mirrored feeds. The sub-components of NOAA0100 NCSC are:

Trusted Internet Connection Access Point (TICAP)
NOAA0100 provides Trusted Internet Connection (TIC) Access Provider (TICAP) services grouped together in a physical TIC stack at each of the NOAA TICAP Locations. The physical TIC stack is comprised of the following:

a) Web Content filtering
b) Netflow
c) Packet Capture
d) Firewall Services
e) Intrusion Detection Sensor
f) Network System Information and Event Manager (SIEM) for logging, monitoring, and event correlation.
g) Network Time Protocol (NTP) Stratum 1 system
h) NCPS (Einstein 2)
i) Malware analysis/detection Tools
General Support Systems (GSS)

The NOAA0100 GSS is an interconnected set of information resources under the same direct management control that shares common functionality. It includes all inventoried hardware, software and communication mediums utilized to support the NOAA0100 mission.

System Administration Support (SAS): The SAS team works to ensure that the technologies supported by NOAA0100 are maintained. SAS ensures that all components, hardware and software, within the NOAA0100 are authorized, configured, and managed appropriately; to include patch management implementation activities via ECMO (BigFix), SCCM and RedHat Satellite.

Enterprise Support Services

Security Operations Center (SOC): The SOC monitors, detects, responds to security events and works with Security Information and Event Management (SIEM) technology and an integrated workflow to identify events of interest hidden in mountains of log data to consistently improve security intelligence capabilities. SOC provides NOAA0100 with a complete picture of security incidents and the ability to make informed security decisions. The SOC leverages existing NOAA0100 monitoring tools and intelligence to collect and accurately analyze logs produced by application, system or network devices coupled with SIEM content to detect possible incidents by employing security intelligence, workflow, repeatable processes and procedures. SOC team members work with NOAA to further understand the threat landscape, the associated risks to the organization, the ability to employ proper security controls and content to generate events of interest which are then triaged and analyzed.

NOAA Computer Incident Response Team (NCIRT): The NCIRT responds to suspected or verified information technology (IT) security incidents. This includes determining if an IT security incident has taken place; how the incident occurred; what the root cause of the incident is; and what is the scope of the incident. Once root cause and scope are determined, NCIRT establishes what countermeasures are to be deployed to defend, contain, eradicate, and recover from the incident. During an IT security incident, the NCIRT role is the authority overseeing and managing every phase of the incident response effort. The NCIRT focuses on maintaining and supporting the mission of the affected system(s) and recognizes when downtime tolerance is minimal or nonexistent. The NCIRT provides incident response (IR) for the affected site and works closely with the cooperation of System Owners and users. Cooperation between NCIRT and customers is paramount to the development of a successful containment plan, effective corrective actions and eradication, and, if warranted, a holistic and effective recovery. NCIRT utilizes the NOAA Incident Response Reporting Application (NIRRA), which provides an Incident Response solution capable of tracking and reporting IT security incidents of all types throughout the response life cycle. This system provides a highly customizable automatic response tasking, permissions, content, reporting and metrics.

Enterprise Security Solutions (ESS): The ESS team works to engineer and manage a services oriented security architecture for NOAA and then integrating the architecture in a multi-layered approach. The ESS team members look at the NOAA enterprise environment to determine how
to layer web content filtering; deploying, managing and running vulnerability scanner tools; i.e. Tenable Nessus Security Center. The ESS task of integrating enterprise services builds for NOAA a holistic security reporting and monitoring operations capability. TICAP is a functional component of ESS. Enterprise Security Operations Center (ESOC): The DOC ESOC provides a comprehensive understanding of cybersecurity posture and threat activity across the Department. It provides Commerce executive leadership with a holistic understanding of cyber risk on a near real time basis and provides recommendations on both immediate and long-term actions which should be taken to reduce risk. It is also responsible for facilitation of cyber intelligence information sharing and coordination of threat monitoring across the Commerce and its OUs.

**Enterprise Security Operations Center (ESOC):** The DOC ESOC provides a comprehensive understanding of cybersecurity posture and threat activity across the Department. It provides Commerce executive leadership with a holistic understanding of cyber risk on a near real time basis and provides recommendations on both immediate and long-term actions which should be taken to reduce risk. It is also responsible for facilitation of cyber intelligence information sharing and coordination of threat monitoring across the Commerce and its OUs.

The ESOC is staffed on a 24x7 basis with personnel skilled in cyber intelligence analysts, network analysis, vulnerability management, and malicious code analysts. ESOC personnel utilize multiple tools such as Security Information and Event Management (SIEM) tools, distributed security analytics capabilities, Enterprise Governance Risk and Compliance (EGRC) tools and other similar technologies which centralize and prioritize security posture and threat information. ESOC has access to multiple levels of classified systems to ensure better collection and sharing of all levels of cyber threat intelligence. The ESOC facilitates the collection and use of information about cyber threats and vulnerabilities which could impact the cyber risk posture of DOC systems. It prioritizes sharing of actionable cyber intelligence with all appropriate network defenders and ensuring that cyber threat indicators are effectively managed and actioned within the DOC environment. ESOC utilizes the Commerce Threat Intelligence Portal (CASIS), which provides an Incident Response solution capable of tracking and reporting IT security incidents of all types throughout the response life cycle.

Although the ESOC is concerned with any cyber-attacks against the DOC or its OUs, it places emphasis on targeted attacks that specifically seek to infiltrate Commerce systems to steal information, disrupt operations, compromise data integrity, or use the Department as a launching pad for other attacks. Threat monitoring efforts focus on detecting Indicators of Compromise (IOC), malicious code, and patterns of malicious activity at the Internet gateway level as this generally provides the best coverage for detection without interfering with ongoing mission critical systems at the OU level. Additionally, efficiency can be gained by launching sources for unique IOCs from a single source that covers internet traffic from multiple OUs. The ESOC does not have any view into encrypted traffic supporting either Commerce activities or employee’s limited personal use of the Internet. The ESOC relies on collected information from Trusted Internet Connection Access Provider (TICAP), Managed Trusted Internet Protocol Service (MTIPS), Enterprise Cybersecurity Monitoring and Operations (ECMO), OU SOCs and other sources.
Although NOAA0100 does not solicit, collect, maintain, or disseminate PII/BII, it is possible for individuals to voluntarily make such information available. Typical examples of the types of PII/BII that may become available to NOAA0100 include names of individuals and businesses, images from photos or videos, screen names, email addresses, etc. NOAA0100 does not ask individuals to post information on its SM/W2.0 websites or applications. Information that individuals voluntarily submit as part of the investigative process is entered as evidence for the NOAA Cyber Security Center [NOAA0100].

As part of NOAA’s Continuous Monitoring Operations, sensitive PII is subject to capture, maintenance, and dissemination as part of the NCSC functions. This collection includes Deep Packet Inspection (DPI) inspected within TICAP, and is consented to at the time of user login.

PII/BII from any government or non-government source may be in the system as evidence of a breach.

NOAA shares all breach incident information with DOC and United States Computer Emergency Readiness Team (US-CERT), as well as law enforcement if applicable.

The applicable authority is for civil employment, 5 U.S.C. 301.

The applicable authority for collection of PII as part of a breach investigation is the Privacy Act of 1974.

This is a HIGH impact system.

Questionnaire:
1. 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.

   ___ This is an existing information system in which changes do not create new privacy risks. Continue to answer questions, and complete certification.

<table>
<thead>
<tr>
<th>Changes That Create New Privacy Risks (CTCNPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Conversions</td>
</tr>
<tr>
<td>b. Anonymous to Non-Antonymous</td>
</tr>
<tr>
<td>c. Significant System Management Changes</td>
</tr>
<tr>
<td>d. Significant Merging</td>
</tr>
<tr>
<td>e. New Public Access</td>
</tr>
<tr>
<td>f. Commercial Sources</td>
</tr>
<tr>
<td>g. New Interagency Uses</td>
</tr>
<tr>
<td>h. Internal Flow or Collection</td>
</tr>
<tr>
<td>i. Alteration in Character of Data</td>
</tr>
<tr>
<td>j. Other changes that create new privacy risks (specify): New incident reporting platform and Trusted Internet Connection Access Provider architecture.</td>
</tr>
</tbody>
</table>

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. Please describe the activities which may raise privacy concerns.

All information transmitted on NOAA networks is subject to network monitoring tools, inspection, continuous monitoring operations, and collection as part of the NCSC mission, and may involve voluminous collections of sensitive PII, including SSNs. As part of a computer incident response inquiry, the NOAA0100 system may have PII data to include Social Security Numbers included in its investigation that may have been part of the original incident. For example, if an individual transmits a list of social security numbers in violation of NOAA PII policies, this original list may be part of the investigation supporting artifacts. Additionally, if a disk image or file contains PII, the retention is pertinent to the collection of incident information from the affected system.

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 about: (Check all that apply.)

X Companies
X 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.)

X DOC employees
X Contractors working on behalf of DOC
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 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.

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.

X 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.
CERTIFICATION

___ X ___ I certify the criteria implied by one or more of the questions above apply to the NOAA0100 NCSC 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 NOAA0100 NCSC 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): Jovan Lovelace

Signature of ISSO or SO: LOVELACE.JOVAN.ANTONIO.1405670930 Digitally signed by LOVELACE.JOVAN.ANTONIO.1405670930 Date: 2018.05.08 14:33:33 -04'00'

Name of Information Technology Security Officer (ITSO): Jean Apedo

Signature of ITSO: APEDO.JEAN .1188076064 Digitally signed by APEDO.JEAN .1188076064 Date: 2018.07.05 07:16:23 -04'00'

Name of Authorizing Official (AO): Douglas Perry

Signature of AO: PERRY.DOUGLAS.A.1365847 Digitally signed by PERRY.DOUGLAS.A.1365847270 Date: 2018.07.05 18:04:00 -04'00'

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

Signature of BCPO: GRAFF.MARK.HYRUM.1514 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.07.09 07:06:36 -04'00'