Version Number: 01-2021

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

Privacy Threshold Analysis
for the
NOAA0100

NOAA Cyber Security Center (NCSC)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/0100 Cyber Security Center

Unique Project Identifier: NOAA0100 (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: *Provide a brief 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 NOAA0100 System is an interconnected set of information resources under the direct management control that shares common functionality. The NCSC is the organization responsible for the management and operations of the NOAA0100 System. NCSC's mission is to protect NOAA networks, computers, programs, and data from cyber-attack, damage, and unauthorized access, enabled by the strategic shift of all NOAA FISMA identified systems to practicing continuous monitoring and real-time assessments.

Address the following elements:

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

The NOAA0100 Authorization Boundary consists of both a general support system and major applications.

b) *System location*

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.

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

NOAA0100 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. As part of the service provided to the NOAA enterprise by the NOAA Common Controls for the Auditing (AU) and Incident Response (IR) security control families, NOAA0100 provides the following services: centralized log management via ArcSight Security Information and Event Management (SIEM), threat analysis methodologies via the FireEye Core Platform Suite (Endpoint Security (HX), Malware Analysis (AX), Email Threat Prevention (ETP), Network (NX), FireEye Central Management (CMS)); to include FireEye's Proprietary Integration and Automation Solution (IX) and security incident response via the NOAA Incident Response Reporting Application (NIRRA). This allows NOAA organizations to utilize the security monitoring services of the NOAA0100 Security Operations Center (SOC), which is made up of two functions; e.g. Security Operations and Intrusion Analysis. Security Operations provides long-term log retention, security monitoring and analysis by its staff. Intrusion Analysis implements and maintains the NOAA cyber IR capability by serving as a central clearing-house for all reported Information Technology (IT) security incidents, alerts, bulletins, and other security related material. The NCSC Enterprise Security Services (ESS) provides centralized vulnerability scanning via Tenable Security Center (Nessus) and the Web Application Assessment Tool (WAAT) / MicroFocus WebInspect and web content filtering via McAfee Web Gateway (MWG). Additionally, NOAA0100 provides Trusted Internet Connection (TIC) Access Provider (TICAP) in-band and out-of-band services at various NOAA locations. These enterprise services are available to NOAA organizations following system onboarding completion and establishment of any necessary operational level agreements.

Additionally, NOAA0100 has established current terms and conditions via Interconnected Security Agreements (ISA's) between connecting DOC bureaus, which obtain Cyber Analytic (CA) services from ESOC within the Enterprise Support Service component. The external connections for which ISA's have been created are as follows: BAS, BEA, BIS, Census, ITA, NIST, NTIA, NTIS, OS and USPTO. The purpose of the interconnection is for the Customer to provide security events, logs, and alerts involving the Customer's information technology resources to the ESOC SIEM (Security Incident Event Management) system and the Log Aggregation Servers hosted within the Provider's infrastructure.

d) The purpose that the system is designed to serve

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.

e) The way the system operates to achieve the purpose

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

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:
The Security Operations Center (SOC) is made up of two functions, Security Operations and Intrusion Analysis.

- Security Operations, performed by Security Operators (SO): 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.

- Intrusion Analysis, performed by Intrusion Analysts (IA) 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, IA establishes what countermeasures are to be deployed to defend, contain, eradicate, and recover from the incident. During an IT security incident, the IA role is the authority overseeing and managing every phase of the incident response effort. IA focuses on maintaining and supporting the mission of the affected system(s) and recognizes when downtime tolerance is minimal or nonexistent. IA provides incident response (IR) for the affected site and works closely with the cooperation of System Owners and users. Cooperation between IA 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.

Enterprise Security Solutions (ESS): The ESS team works to engineer and manage a service-oriented security architecture for NOAA and then integrate 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.

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 Automated Security Information System (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.

Furthermore, ESOC operational efforts are delineated into two distinct functional services; e.g., ESOC-CA and ESOC-IR.

ESOC-CA:
Cyber Analytics (CA) is responsible for integrating threat intelligence with 24x7 near real-time monitoring for timely detection of Cybersecurity incidents. Cyber Analytics has four (4) primary functions:

- Log Collection (establishing the logging environment from log source to centralized SIEM)

- Threat Intelligence Harvesting and Curation (applying fidelity, confidence, and relevance values to ingested intelligence)
- Enterprise Event Correlation (applying correlation logic against ingested security logs for analysis and investigation).
- Intelligence and Awareness Sharing (distributing cyber intelligence to the constituency through the intelligence portal)

ESOC-IR:
Incident Response (IR) plays a critical role in protecting sensitive information. Incident response has four (4) primary functions:

- Incident Handling—the process of collecting information from the reporting entity, such as a Reporting BOU (Bureau Operating Unit) or CA. This process identifies necessary and/or applicable information.
- Incident Processing—the process through which an incident is triaged and routed to the appropriate department.
- Incident Reporting—the process of reporting to external agencies, communicating applicable CCIRs (Commerce Critical Incident Report), and coordinating updates and closures.

Incident Investigation—the process of malware analysis, data forensics, and additional dataset collection.

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

The NOAA0100 system contains the following Security Categorization of Service Delivery Support Information (NIST SP 800-60 Revision 1 Volume 2, Appendix C) and/or Mission Information (NIST SP 800-60 Revision 1 Volume 2, Appendix D). The default security impacts were selected for all NIST SP 800-60 mission and service delivery information types.

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.

An unauthorized disclosure of information from NOAA0100 would have a ***severe*** impact on NOAA and its mission.

Additionally, 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.

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

The users in question are the privileged administrative federal employees and contractors within the NCSC. Note: Non-privileged (general users without a need-to-know per cited roles/responsibilities) would not have access to DPI (Deep Packet Inspection) data.

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

NOAA0100 utilizes a role-based approach within 'NCSC User Onboarding' Standard Operating Procedures to determine how to enforce approved authorizations for logical access within each inventoried device or application. NOAA0700 provides the ICAM solution for Identity Credential Access and Federation Management (ICAM), which is leveraged for multifactor and single sign-on capability. NOAA0100 obtains enterprise compliant authentication services for the NIRRA, CASIS and CTIP components, respectively, from this solution.

Other NOAA0100 component use different methods of multifactor authentication for privilege user access. For example, the application called freeRADIUS supports NOAA0100 networking equipment with username + token one-time password (OTP) for privileged users to gain access to those devices. NCSC authentication requests are tied into the FreeIPA management server where the usernames, groups, and role-based access are administered/established. The configurations setup on network devices allow authentication requests to be sent to this RADIUS solution. Administrative access to TIC access point devices and Security Information Event Management (SIEM) are controlled by two-factor authentication via Common Access Card (CAC) hardware-based authentication.

i) How information is transmitted to and from the system

A firewall at each NOAA0100 site enforces a strict access control policy (ACL) on data transmitted via egress and ingress within the network. NOAA0100 implements a defense-in-depth strategy via deploy of FortiNet FortiGate Firewalls with IDS configured, McAfee Web Gateways for http/web filtering. FireEye web Malware Protection System for Web Malware Inspection. Cisco Stealthwatch for Network Intrusion Detection and Anomaly Detection. Additionally, there is regularly updated IPS/IDS built into the in-line FortiGate Firewalls of the TIC stack. It has numerous signatures for XSS, SQL injection, session tampering, buffer overflows, malicious web crawlers, and other web security vulnerabilities.

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.

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

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X 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
- X 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.

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.

Provide the legal authority which permits the collection of SSNs, including truncated form.
Executive Orders: 9397 – Numbering System for Federal Accounts Relating to Individual Persons, as amended by 13478, 9830, and 12107; 10450 – Security Requirements for Government Employment; 12656 – Assignment of emergency preparedness responsibilities; 5 U.S.C. § 301 – authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

____ 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 NOAA Cyber Security Center (NOAA0100) 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 [IT SYSTEM NAME] 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: Chi Y. Kang, NOAA0100 SO
Office: NOAA OCIO
Phone: 301-628-5738
Email: chi.y.kang@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: KANG.CHI.YUN.1246231652 Digitally signed by KANG.CHI.YUN.1246231652 Date: 2022.05.24 09:21:41 -04'00'

Date signed:

Information Technology Security Officer
Name: Ansaruddin Hasan
Office: NOAA OCIO
Phone:
Email: Ansaruddin.Hasan@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: HASAN.ANSARUDDIN.ISA.1376816210 Digitally signed by HASAN.ANSARUDDIN.ISA.1376816210 Date: 2022.05.24 09:49:51 -04'00'

Date signed:

Privacy Act Officer
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: 2022.05.25 10:28:19 -04'00'

Date signed:

Authorizing Official
Name: Douglas Perry
Office: NOAA OCIO
Phone: 301-706-8742
Email: douglas.a.perry@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: PERRY.DOUGLAS.ALLEN.1365847270 Digitally signed by PERRY.DOUGLAS.ALLEN.1365847270 Date: 2022.05.25 08:29:07 -04'00'

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.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2022.05.25 12:59:04 -04'00'

Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PTA.