Version Number: 01-2015

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

Privacy Impact Assessment
for
NOAA0100, NOAA Cyber Security Center (NCSC)

Reviewed by: _____, Bureau Chief Privacy Officer
Mark Graff

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2017.12.01 14:03:46 -05'00'

11/09/2017

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA0100 - NCSC

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

Introduction: System Description

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.

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 integration of 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.

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.

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. The users in question are the privileged administrative users within 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. Warning banners have been implemented on the designated NOAA0100 devices per DOC mandates with the following text in order to give users proper notification: "You are accessing a U.S. Government information system, which includes: 1) this computer, 2) this computer network, 3) all computers connected to this network, and 4) all devices and storage media attached to this network or to a computer on this network. You understand and consent to the following: you may access this information system for authorized use only; you have no reasonable expectation of privacy regarding any communication of data transiting or stored on this information system; at any time and for any lawful Government purpose, the Government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system; and any communications or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose."

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 (Department of Justice).

The applicable authority for is 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.

Additional authorities from DEPT-18: 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

From DEPT-13: Executive Orders 10450, 11478, 12065, *5 U.S.C. 301* and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.

From DEPT-25: 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075.

This is a FIPS 199 high impact system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
_X___ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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): New incident reporting platform.					

_ This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	e. File/Case ID	X	i. Credit Card	X
b. Taxpayer ID	X	f. Driver's License	X	j. Financial Account	X
c. Employer ID	X	g. Passport	X	k. Financial Transaction	X
d. Employee ID	X	h. Alien Registration	X	l. Vehicle Identifier	X

m. Other identifying numbers (specify):
*Explanation for the need to collect, maintain, or disseminate the Social Security number, 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.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	X
b. Maiden Name	X	h. Place of Birth	X	n. Financial Information	X
c. Alias	X	i. Home Address	X	o. Medical Information	X
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	X
f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	X
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates	X		
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X	d. Photographs	X	g. DNA Profiles	X
b. Palm Prints	X	e. Scars, Marks, Tattoos	X	h. Retina/Iris Scans	X
c. Voice Recording/Signatures	X	f. Vascular Scan	X	i. Dental Profile	X
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

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

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation	X	For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): X – Networking Monitoring for security threats and PII policy violations.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

NOAA0100 does not solicit, collect, maintain, or disseminate PII/BII; however, it is possible for individuals to voluntarily make such information available. PII/BII may become available to NOAA0100 as part of investigation of PII policy violations and criminal law enforcement. These may include names of individuals and businesses, images from photos or videos, screen names, email addresses, etc. Information that individuals voluntarily submit as part of the investigative process is entered as evidence for the NOAA Cyber Security Center [NOAA0100] (NCSC).The NCSC does not solicit this information. There is no purpose for this information, unless it is retained as part of a breach investigation.

PII/BII is collected and monitored via network monitoring tools for security threats, incident response, law enforcement activities, and network protection. This information may be in the system as evidence of a breach and retained as part of a breach investigation. The only purpose for this information is if it is retained as part of a breach investigation.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared

	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify): Law enforcement	X		

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found on the NIRRA Web page, *but it is accessible only to NOAA personnel. The PAS is included in the cover email for this submission.*	
X	Yes, notice is provided by other means.	Specify how: For those reporting a breach, NIRRA states: "This is a United States Federal Government computer system, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil and/or administrative action. All information on this computer system may be intercepted, recorded, read, copied or disclosed by and to authorized personnel for official purposes, including criminal investigations. Access or use of this computer system by any person, whether authorized or unauthorized, CONSTITUTES

		CONSENT to these terms."
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: An employee/contractor enters his/her credentials through NIRRA and NEMs authenticates the user to allow access to the reporting system. An employee/contractor can decline to provide PII by not logging into the NIRRA platform.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Consent is granted prior to log-in. A warning notice includes "Access or use of this computer system by any person, authorized or unauthorized, constitutes consent to these terms. If you do not agree, click on cancel to avoid continuing to the site."
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: A NIRRA user can view all the information in the User Profile by selecting the drop down list next to their name in the upper right hand corner and selecting User Profile. Users who would like change their general account information in NIRRA, such as first name, last name or username would be required to send a request to ess@noaa.gov. Users have the ability to change non-general settings in their user profile such as email address, time zone and password.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.

X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Any PII/BII collected through the NOAA0100 system for computer security incident investigations is restricted to access by NOAA Computer Incident Response Team (NCIRT) personnel. Access to records is monitored and recorded within system event logs.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 12/08/2016 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM) to mitigate any controls that are not appropriately implemented.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
N/A	Contracts with customers establish ownership rights over data including PII/BII.
N/A	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Discretionary access controls are implemented throughout NOAA0100 for access to forensic data. The NIRRA platform 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 response tasking, record permissions, content uploading, reporting and querying for metrics. Any sensitive PII on NIRRA is redacted from end user views, and copies maintained on the database are only shared for law enforcement activities. The storage of any sensitive PII is encrypted in transit and at rest. NCSC Network Monitoring may pick up sensitive PII and monitoring is only conducted by privileged users who sign a confidentiality or non-disclosure agreement. Access to physical enclaves is implemented as a physical security control to NOAA0100 resources; this would include access to physical articles in evidence that may include PII/BII.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: COMMERCE/DEPT-13, Investigative and Security Records; COMMERCE/DEPT-18, Employees Information Not Covered by Notices of Other Agencies; COMMERCE/DEPT-25, Access Control and Identity Management System.

	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NARA General Records Schedule 24, Item 7: Computer security incident handling: Destroy/delete 3 years after all necessary follow-up actions have been completed. (N1-GRS-03-1 item 7)
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: With the information available, large volumes of individuals may be identified.

X	Quantity of PII	Provide explanation: The quantity of PII will vary, but depending on the number and size of breaches, disclosure could have a serious adverse effect on the organization or on individuals.
X	Data Field Sensitivity	Provide explanation: There may be large volumes of sensitive PII in the system, as a result of both continuous monitoring, and voluntary sensitive PII submissions retained for law enforcement purposes.
X	Context of Use	Provide explanation: Voluminous Sensitive PII, including SSNs may be retained for law enforcement purposes, collected through Network Monitoring Tools as well as voluntary submissions of Sensitive PII incident to NIRRA, the new reporting application.
	Obligation to Protect Confidentiality	Provide explanation: N/A
X	Access to and Location of PII	Provide explanation: Access to the Sensitive PII through NCSC Network Monitoring is restricted to privileged users who have signed a non-disclosure agreement.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: The storage of any sensitive PII is encrypted in transit and at rest.
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: The storage of any sensitive PII is encrypted in transit and at rest.
	No, the conduct of this PIA does not result in any required technology changes.