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

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

Reviewed by: Robin Burress for Mark Graff, Bureau Chief Privacy Officer

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

NICHOLAS CORMIER Digitally signed by NICHOLAS CORMIER
Date: 2026.06.01 11:04:15 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/OCIO/ NCSC

Unique Project Identifier: NOAA0100 (006-48-02-00-01-3511-00

Introduction: System Description

The National Oceanic & Atmospheric Administration (NOAA) Cyber Security Center (NCSC) manages the NOAA0100 System, a primary component of NOAA's Trusted Internet Connection (TIC) Access Provider (TICAP) infrastructure, protecting NOAA and Department of Commerce (DOC) networks. NCSC provides continuous monitoring, threat detection, and incident response to safeguard critical assets. NOAA0100 is a General Support System and major application that has been labeled both as a Mission Essential Function (MEF) and a High Value Asset (HVA). NOAA0100 is approved to process Controlled Unclassified Information (CUI).

Key Cybersecurity Functions:

- 24/7 Threat Monitoring & Response – Detecting and mitigating cyber risks in real time.
- Endpoint & Network Security – Strengthening defenses against unauthorized access.
- Security Information and Event Management (SIEM) – Centralized log analysis and automation.
- Compliance & Risk Management – Supporting federal cybersecurity regulations.
- Security Incident Response and Evaluation Nexus (SIREN) – a workflow that encompasses NOAA0100's Security Orchestration, Automation, and Response (SOAR) platform and NOAA0900's Google Workspace for Incident Response Reporting. The SIREN workflow automates Incident Response activities, collaboration and artifact collection. As a result, Incident information previously stored on NOAA0100 systems is now stored within the NOAA0900's cloud environment which decreases the NOAA0100 privacy footprint.
- Deep Packet Inspection (DPI): Network traffic is actively inspected when traversing the Trusted Internet Connection Access Provider (TICAP) infrastructure.

NCSC collaborates with partners like Cybersecurity Infrastructure Security Agency (CISA), DOC Enterprise Security Operations Center (ESOC), and law enforcement to enhance security awareness and incident handling. By aligning cybersecurity efforts with NOAA's mission, NCSC ensures resilient information technology (IT) operations and proactive threat defense.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system
The NOAA0100 Authorization Boundary is considered a General Support System and major application.

(b) System location
NOAA0100 NCSC operates in a mirrored configuration from two locations, Fairmont, West Virginia, which serves as the primary location, and Boulder, Colorado. Both locations receive mirrored traffic of incoming and outgoing data feeds for all NOAA internal offices and

numerous other connections.

(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 unified direct management control, sharing common functionality. It includes all inventoried hardware, software, and communication mediums supporting the NOAA0100 mission.

As part of the services provided to the NOAA enterprise through the NOAA Federal Information System Modernization Act (FISMA) Common Controls for the Auditing and Accountability (AU) and Incident Response (IR) security control families, NOAA0100 offers:

- Centralized log management- via the designated SIEM. NOAA0100 is responsible for providing a SIEM interface that is capable of allowing the system interconnections to process, sort, and search audit records for events of interest based on the following content, including, but not limited to: source time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. The SIEM team is responsible for validating that the log data is processed correctly. The SIEM team is also responsible for assisting system interconnections to find a solution if the current tools are unable to be properly configured or provide guidance on how to format the data correctly.
- Threat analysis is performed by the NOAA Security Operations Center (SOC) across NOAA systems utilizing endpoint security tools, malware analysis tools, email threat prevention software, network security tools and a central management software.
- For enhanced security coordination the NOAA SOC uses a proprietary integration and automation solution for enhanced security coordination.
- Security incident response is via NCSC's SIREN which is a workflow that encompasses NOAA0100's SOAR and NOAA0900's Google Workspace for Incident Response Reporting and the storage of those incidents.

<u>Security Services & Functions</u>

NOAA0100's security monitoring services are available to NOAA offices through the following key entities:

- NCSC SOC – Comprising two primary functions: Security Operations and Intrusion Analysis.
  - Security Operations manages long-term log retention, security monitoring, and data analysis.
  - Intrusion Analysis oversees NOAA's cyber incident response capability, serving as a central clearinghouse for reported IT security incidents, alerts, bulletins, and other security-related information.

- NCSC Enterprise Security Services (ESS) – Provides centralized vulnerability scanning and enterprise security tool support.
- Trusted Internet Connection (TIC) Access Provider (TICAP) – Offers in-band and out-of-band services at various NOAA locations.

Interconnection & Agreements

The connections listed in CSAM represent a current snapshot of interconnections associated with NOAA0100. These connections may establish or terminate without prior notice, reflecting their dynamic nature.

System Name	Classification	Data Flow
NOAA0301 - Traffic Coordination System for Space	Sensitive But Unclassified	Incoming
NOAA0500 - R&D High-Performance Computer System	Sensitive But Unclassified	Incoming
NOAA0520 - NOAA Enterprise Data Centers	Unclassified	Incoming
NOAA0550 - NOAA Enterprise Network (N-Wave)	Unclassified	Incoming
NOAA0700 - High Availability Enterprise Services	Sensitive But Unclassified	Incoming
NOAA0900 - Consolidated Cloud Applications (H) GoCo	Sensitive But Unclassified	Bidirectional
NOAA1200 - Corporate Services (M)	Unclassified	Incoming
NOAA2220 - Fleet Support System (FSS)	Sensitive But Unclassified	Incoming
NOAA3000 - OAR Headquarters	Sensitive But Unclassified	Incoming
NOAA3030 - Atlantic Oceanographic and Meteorological laboratory	Sensitive But Unclassified	Incoming
NOAA3040 - Air Resources Laboratory	Unclassified	Incoming

NOAA3070 - Geophysical Fluid Dynamics Laboratory	Sensitive But Unclassified	Incoming
NOAA3090 - National Severe Storms Laboratory Scientific Computing Facility	Sensitive But Unclassified	Incoming
NOAA3100 - Pacific Marine Environmental Laboratory Local Area Networks	Sensitive But Unclassified	Incoming
NOAA3500 - OAR Boulder Laboratories	Sensitive But Unclassified	Incoming
NOAA4000 - Fisheries WAN and Enterprise Services	Sensitive But Unclassified	Incoming
NOAA4100 - Greater Atlantic Regional Office (GARO) Network	Sensitive But Unclassified	Incoming
NOAA4200 - Northeast Fisheries Science Center (NEFSC) Network	Sensitive But Unclassified	Incoming
NOAA4300 - Southeast Regional Office (SERO) Network	Sensitive But Unclassified	Incoming
NOAA4400 - Southeast Fisheries Science Center (SEFSC) Network	Sensitive But Unclassified	Incoming
NOAA4500 - West Coast Region (WCR) Network	Sensitive But Unclassified	Incoming
NOAA4600 - Northwest Fisheries Science Center (NWFSC) Network	Sensitive But Unclassified	Incoming
NOAA4700 - Alaska Regional Office (AKRO) Network	Sensitive But Unclassified	Incoming
NOAA4920 - Pacific Islands Regional Office (PIRO) Network	Sensitive But Unclassified	Incoming
NOAA4930 - Southwest Fisheries Science Center	Sensitive But Unclassified	Incoming

(SWFSC) Network		
NOAA4960 - Pacific Islands Fisheries Science Center (PIFSC) Network	Sensitive But Unclassified	Incoming
NOAA5004 - Data Collection System	Unclassified	Incoming
NOAA5006 - NESDIS Administrative Local Area Network (NESDIS Admin LAN)	Unclassified	Incoming
NOAA5006-01 - NESDIS Cloud System (NCS) Development & Sandbox	Controlled Unclassified Information	Incoming
NOAA5009 - National Climatic Data Center Local Area Network	Unclassified	Incoming
NOAA5023 - Search and Rescue Satellite Aided Tracking	Unclassified	Incoming
NOAA5040 - Comprehensive Large Array-data Stewardship System	Unclassified	Incoming
NOAA5042 - Joint Polar Satellite System	Unclassified	Incoming
NOAA5044 - Mission Support Local Area Network	Unclassified	Incoming
NOAA5045 - NOAA Environmental Satellite Processing Center	Unclassified	Incoming
NOAA5047 - Partner Antenna Access Network (PAAN)	Unclassified	Incoming
NOAA5050 - Geostationary Environmental Operational Satellite Series-R Ground System	Sensitive But Unclassified	Incoming
NOAA5050-01 - Geostationary	Sensitive But Unclassified	Incoming

Operations Cloud		
NOAA5065 - NESDIS Cloud System (NCS)	Unclassified	Incoming
NOAA8100 - Configuration Branch Information Technology System (CBITS)	Sensitive But Unclassified	Incoming
NOAA8102 - Automated Surface Observing System (ASOS)	Unclassified	Incoming
NOAA8106 - Upper Air Observing System (UAOS)	Unclassified	Incoming
NOAA8107 - Advanced Weather Interactive Processing System (AWIPS)	Unclassified	Incoming
NOAA8202 - Office of Water Prediction (OWP)	Sensitive But Unclassified	Incoming
NOAA8203 - National Weather Service Performance Management System (N-PMS)	Sensitive But Unclassified	Incoming
NOAA8501 - NWS Dissemination Enterprise Cloud (NDEC)	Sensitive But Unclassified	Incoming
NOAA8850 - NWS Enterprise Mission Enabling System (EMES)	Unclassified	Incoming
NOAA8860 - Weather and Climate Computing Infrastructure Services (WCCIS)	Unclassified	Incoming
NOAA8861 - Aviation Weather Center (AWC)	Unclassified	Incoming
NOAA8864 - Space Weather Prediction Center (SWPC)	Unclassified	Incoming
NOAA8865 - NOAA Tsunami Warning System (NTWS)	Unclassified	Incoming

NOAA8868 - Storm Prediction Center (SPC)	Unclassified	Incoming
NOAA8872 - NWS Virtual Lab (NWS VLAB)	Unclassified	Incoming
NOAA8873 - National Data Buoy Center (NDBC)	Unclassified	Incoming
NOAA8880 - AK Region (AKHQ)	Unclassified	Incoming
NOAA8881 - CR Kansas City (CRHQ)	Unclassified	Incoming
NOAA8882 - ER Bohemia (ERHQ)	Unclassified	Incoming
NOAA8883 - Pacific Region (PR)	Unclassified	Incoming
NOAA8884 - SR Fort Worth (SRHQ)	Unclassified	Incoming

(d) The way the system operates to achieve the purpose(s) identified in Section 4

The NOAA0100 system leverages a suite of integrated technologies and specialized teams to secure and sustain its cybersecurity infrastructure across NOAA and DOC bureaus. At each TICAP location, NOAA0100 deploys security, auditing and networking tools to deliver real-time network protection and compliance enforcement.

The System Administration Support (SAS) team ensures all technologies within NOAA0100 are properly authorized, configured, and maintained. This includes executing patch management and configuration controls through platforms designated by NOAA to meet vulnerability and compliance requirements.

The NOAA SOC serves as a critical component in the agency's cybersecurity framework, providing continuous surveillance, threat detection, and incident response capabilities across its digital infrastructure. Structured into two specialized divisions, Security Operations and Intrusion Analysis, the SOC leverages centralized SIEM technologies to aggregate and analyze vast volumes of log data. This centralized approach facilitates the early identification of anomalous behavior, potential indicators of compromise (IOCs), and emerging threats, thereby enabling NOAA0100 to make timely, data-driven decisions regarding risk mitigation.

When security incidents arise, the Intrusion Analysis team assumes a leadership role in orchestrating investigative and remediation efforts. These analysts conduct in-depth

forensic examinations, determine the scope and impact of the breach, and coordinate with internal and external stakeholders to execute containment, eradication, and recovery procedures. Their efforts ensure that affected systems are restored securely and that lessons learned are incorporated into future defensive strategies.

Complementing the SOC's operational mandate, ESS is responsible for the strategic design, implementation, and management of NOAA's multi-layered cybersecurity architecture. ESS integrates a suite of enterprise-grade security tools and technologies to uphold a defense-in-depth model, ensuring that protective measures span across network boundaries, endpoints, applications, and data repositories. This holistic approach fortifies NOAA's resilience against a broad spectrum of cyber threats and supports the agency's mission-critical operations with robust, scalable security infrastructure.

The SIEM Team is responsible for administering NOAA's centralized log management infrastructure through the development of custom rulesets, connectors, and monitoring logic to track threats across NOAA's landscape. It also manages the SOAR platform, enabling automated detection and response processes.

The Security Tools Engineering (STE) team enhances NCSC's capabilities through custom development ranging from Palo Alto's Security Orchestration and Automation platform (xSOAR) playbooks and scripts to application and integration support ensuring seamless collaboration across SOC, ESS, and SIEM functions.

(e) How information in the system is retrieved by the user

NOAA0100 employs a role-based access control approach, as defined in the NCSC User Onboarding Standard Operating Procedures, to enforce approved authorizations for logical access to each inventoried device or application. Identity Credential Access and Management (ICAM) services are provided through NOAA0700, enabling multifactor and single sign-on (SSO) capabilities.

Additional NOAA0100 components utilize alternative multifactor authentication (MFA) mechanisms for privileged user access. For instance, the Remote Authentication Dial-In User Service (RADIUS) supports networking equipment by requiring username and token-based one-time password (OTP) authentication for authorized users. These authentication requests are integrated with the Free Identity, Policy, and Access (IPA) management server, which manages user credentials, group memberships, and role-based access settings. Network device configurations are designed to forward authentication requests to the RADIUS platform.

Furthermore, administrative access to TIC access point devices and the SIEM system is protected through two-factor authentication using Common Access Card (CAC) hardware-based credentials.

(f) How information is transmitted to and from the system

A firewall at each NOAA0100 site enforces a strict access control policy on data transmitted via egress and ingress within the network. NOAA0100 implements defense-in-depth strategies compliant with CISA HVA Binding Operational Directive (BOD) compliant policies, and appropriate security controls. NOAA0100 NCSC undergoes frequent assessment of these controls to ensure compliance and adherence to policies.

(g) Any information sharing conducted by the system

The information below is passed through NCSC NOAA0100 in the form of audit logs or potential incident data:

- Network Traffic & Communications Monitoring
  - All information transmitted on NOAA networks is subject to inspection, logging, and continuous monitoring.
  - This may include extensive volumes of sensitive Personally Identifiable Information (PII), such as Social Security Numbers (SSNs).
- Incident Response Data
  - PII, including SSNs, may be collected during incident response investigations if they were involved in the original event (e.g., unauthorized transmission of SSNs).
  - Disk images or files containing PII may be retained when necessary for analyzing affected systems.
- Deep Packet Inspection (DPI) Content
  - Network traffic is inspected through DPI processes within the TICAP infrastructure.
  - This inspection is acknowledged and consented to at the time of user login.
- Evidence of Security Breaches
  - The system may hold PII from both government and non-government sources if such data is discovered as part of a cybersecurity breach investigation.
- Impact Sensitivity
  - Unauthorized disclosure of data managed by NOAA0100 would result in severe impact to NOAA operations and its mission.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

Type of Information Collected	Applicable SORNS	Programmatic Authorities
Breach Investigation	COMMERCE/DEPT-13	Privacy Act of 1974, 5 U.S.C. 552a(e)(10)
		Federal Information Security Modernization Act of 2014 (FISMA 2014)
		OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information

Security Investigations	COMMERCE/DEPT-13	Executive Orders 10450, 11478
		5 U.S.C. 7531-332
		28 U.S.C. 533-535
Building Entry/Access & Surveillance	COMMERCE/DEPT-25	5 USC 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
System Administration/ Audit Data (SAAD)	COMMERCE/DEPT-25	5 USC 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
		Electronic Signatures in Global and National Commerce Act, Public Law 106-229
		28 U.S.C. 533-535
Collection & Use of SSN	COMMERCE/DEPT-18	44 U.S.C. 3101
		Executive Order 12107
	COMMERCE/DEPT-25	5 USC 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
Public Health Emergency Info & Reasonable Accommodation	COMMERCE/DEPT-18	Executive Order 13164
(includes medical and religion accommodation requests)	COMMERCE/DEPT-31	Rehabilitation Act, 29 U.S.C. 701 et. seq
		Americans with Disabilities Act of 1990, as amended, 102(d), 42 U.S.C. 12112(d)
		29 CFR parts 1602, 1630, 1904, 1910, and 1960
		29 USC chapter 15 (e.g., 29 U.S.C. 668)
		Executive Order 12196
		5 U.S.C. 7902

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

High

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: The system has converted to only utilizing SIREN which is a workflow that is built-in to NOAA0100's SOAR platform and NOAA0900's Google Workspace for Incident Response Reporting. Information is no longer stored within the NOAA0100 boundary in regards to Incident Response. This reduces the risk to NOAA0100 by containing the information in the NOAA0900 boundary and not on physical devices.					

____ 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.

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

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	f. Driver's License	X	j. Financial Account	X
b. Taxpayer ID	X	g. Passport	X	k. Financial Transaction	X
c. Employer ID	X	h. Alien Registration	X	l. Vehicle Identifier	X
d. Employee ID	X	i. Credit Card	X	m. Medical Record	X
e. File/Case ID	X				
n. Other identifying numbers (specify):					
*Explanation for the business 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	h. Date of Birth	X	o. Financial Information	X
b. Maiden Name	X	i. Place of Birth	X	p. Medical Information	X
c. Alias	X	j. Home Address	X	q. Military Service	X
d. Sex	X	k. Telephone Number	X	r. Criminal Record	X
e. Age	X	l. Email Address	X	s. Marital Status	X
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	X
g. Citizenship	X	n. Religion	X		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	X
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	X
c. Work Address	X	g. Work History	X	k. Procurement/contracting records	X
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X	f. Scars, Marks, Tattoos	X	k. Signatures	X
b. Palm Prints	X	g. Hair Color	X	l. Vascular Scans	X
c. Voice/Audio Recording	X	h. Eye Color	X	m. DNA Sample or Profile	X
d. Video Recording	X	i. Height	X	n. Retina/Iris Scans	X
e. Photographs	X	j. Weight	X	o. Dental Profile	X
p. 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		Hard Copy: Mail/Fax		Online	X
Telephone	*X	Email	X		

Other (specify): * Via telephone if online access is not available.

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

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

2.3 Describe how the accuracy of the information in the system is ensured.

Data integrity is ensured for both the TICAP and SIREN/SOAR through privilege access controls that provide users with the ability to view and/or modify information assigned to their respective roles / responsibilities. Video data is read-only as received by transmitting devices and cannot be altered based on integrity checks and timestamps.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 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	x	Electronic purchase transactions	
Other (specify):*GSA Building - PII obtained by the video surveillance cameras is only accessible by Federal employees and NOAA0100 support contractors for the monitoring of the enclosed networking equipment racks. These racks are located in a physically secure location with access only by authorized NOAA0100 personnel. This information is collected as part of a service level agreement with NOAA0520.			

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			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	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	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify):			

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 or disseminate PII/BII; however, it is possible for individuals to voluntarily make such information available. This incidental collection occurs routinely through continuous network monitoring, Deep Packet Inspection (DPI) of traffic traversing NOAA networks,

and during the course of incident response investigations where affected systems, disk images, or network logs are analyzed for threat mitigation.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Common threats to the privacy of TICAP or SIREN/ SOAR operational data includes data leakage due to compromised chain of custody within the environments designated to store / process sensitive information. The continuously monitored and implemented control, leveraged to ensure data is handled, retained and disposed, relates to designated roles required to comply with DOC Enterprise Cybersecurity Policy (ECP); i.e., Incident Responders and Information System Security Officers (ISSO)s. Both roles have successfully met and maintained the credential / training requirement via qualified certifying organization and the associated Continuing Professional Education (CPE) programs, which sustain a working knowledge of industry standard and best practices.

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	X*		
Private sector			
Foreign governments			
Foreign entities			
Other (specify): Law enforcement if needed	X		

* If needed for victim notification, pursuant to the DOC Breach Notification Plan. PII would be provided to the Privacy Office, which may be provided to impacted individuals.

	The PII/ BII in the system will not be shared

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

X	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

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

X	**Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.** **Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:** NOAA0100 is an interconnected set of information resources, under the same direct management control, intended to meet the TIC Requirements of a Multi-agency TICAP as described by CISA. Additionally, NOAA0100 includes all inventoried hardware, software and communication mediums utilized to support the NCSC managed enterprise services which fulfil NOAA Common Controls for the Audit and Accountability (AU) and Incident Response (IR) security control families. NCSC managed enterprise services include: Centralized log management via NCSC's SIEM, data pipeline solutions and storage solution, threat analysis methodologies via the NOAA Endpoint Detection and Response (EDR), Malware Analysis, Email Threat Prevention (ETP), TICAP Next Generation Firewalls (IDS/IPS/Web Filtering/Network Analytics), Netflow, and security incident response, via the SIREN workflow, which is processed and stored in NCSC's SOAR solution, aligning to the NOAA Incident Response Plan. This allows NOAA organizations to utilize the security monitoring services of the NOAA0100 SOC, which is made up of three primary functions; Cybersecurity Analysis, Threat Intelligence, and IR. The SOC provides long-term log retention, security monitoring and analysis by its staff. IR implements and maintains the NOAA Cyber IR capability by serving as a central authority on all IT security incidents, alerts, bulletins, and other security related material. Threat Intelligence provides Cybersecurity Threat Research, Attack Surface monitoring, Threat hunting and detection capabilities, and process improvements. The NCSC ESS provides centralized vulnerability scanning via Tenable Security Center (Nessus) and web content filtering via Next Generation Firewalls. Additionally, NOAA0100 is a Multi-agency TICAP utilized for in-band and out-of-band services at various NOAA locations. These enterprise services are available to NOAA organizations following system onboarding and establishment of any necessary operational level agreements. NOAA0100 has established current terms and conditions via ISAs between connecting DOC bureaus. The external connections for which ISAs 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 SIEM system and the Log Aggregation Servers hosted within the Provider's

	infrastructure. These connections are configured in a secure manner and does not allow access to any PII/BII.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 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 at: NOAA0100 (NCSC) Privacy Act Statement (PAS)	
X	Yes, notice is provided by other means.	Specify how: For those reporting a breach, When accessing any NOAA IT System, end users are prompted with a banner, where they agree to the following: *You have no reasonable expectation of privacy when you use this information system; this includes any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may, without notice, monitor, intercept, search and seize any communication or data transiting or stored on this information system. The government may disclose or use any communications or data transiting or stored on this information system for any lawful government purpose, including but not limited to law enforcement and national security purposes* Individuals may opt out of this agreement by refusing to use NOAA IT equipment. This policy is derivative of Executive

		Order No. 12968 and succeeded by Executive Order 13587 and comply with National Insider Threat Minimum Standards. The NCSC enforces the monitoring and compliance to these executive orders and standards through the use of Security Information and Event Management tool, Endpoint Detection and Response tool, Security Orchestration, Automation, and Response and may store sensitive information of any kind as part of its Incident Response obligations to CISA, Department of Commerce, NOAA, or the United States Federal Government. Additionally, all telemetry captured by the NCSC as part of its role as a TIC Access Provider are used to comply with and other Executive Memorandums, Orders, and Directives (e.g. M-19-26), and legislation (e.g. CIRCIA). For the video surveillance, there is a sign posted on the door to the area that states "Notice this area is under 24-hour video surveillance. You are warned."
	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: When accessing any NOAA IT System, end users are prompted with a banner, where they agree to the following: *You have no reasonable expectation of privacy when you use this information system; this includes any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may, without notice, monitor, intercept, search and seize any communication or data transiting or stored on this information system. The government may disclose or use any communications or data transiting or stored on this information system for any lawful government purpose, including but not limited to law enforcement and national security purposes* Individuals may opt out of this agreement by refusing to use NOAA IT equipment. This policy is derivative of Executive Order No. 12968 and succeeded by Executive Order 13587 and comply with National Insider Threat Minimum Standards. The NCSC enforces the monitoring and compliance to these executive orders and standards through the use of Security Information and Event Management tool, Endpoint Detection and Response tool, Security Orchestration, Automation, and Response and may store sensitive information of any kind as

		part of its Incident Response obligations to CISA, Department of Commerce, NOAA, or the United States Federal Government. Additionally, all telemetry captured by the NCSC as part of its role as a TIC Access Provider are used to comply with and other Executive Memorandums, Orders, and Directives (e.g. M-19-26), and legislation (e.g. CIRCIA). For the video surveillance, there is a sign posted on the door to the area that states "Notice this area is under 24-hour video surveillance. You are warned."
	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: When accessing any NOAA IT System, end users are prompted with a banner, where they agree to the following: *You have no reasonable expectation of privacy when you use this information system; this includes any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may, without notice, monitor, intercept, search and seize any communication or data transiting or stored on this information system. The government may disclose or use any communications or data transiting or stored on this information system for any lawful government purpose, including but not limited to law enforcement and national security purposes* Individuals may opt out of this agreement by refusing to use NOAA IT equipment. This policy is derivative of Executive Order No. 12968 and succeeded by Executive Order 13587 and comply with National Insider Threat Minimum Standards. The NCSC enforces the monitoring and compliance to these executive orders and standards through the use of Security Information and Event Management tool, Endpoint Detection and Response tool, Security Orchestration, Automation, and Response and may store sensitive information of any kind as part of its Incident Response obligations to CISA, Department of Commerce, NOAA, or the United States Federal Government. Additionally, all telemetry captured by the NCSC as part of its role as a TIC Access Provider are used to comply with and other Executive Memorandums, Orders, and Directives (e.g. M-19-26), and legislation (e.g. CIRCIA).

		For the video surveillance, there is a sign posted on the door to the area that states "Notice this area is under 24-hour video surveillance. You are warned."
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Once data is procured as a part of an ongoing investigation that data is retained as part of an incident record. Individuals have no direct ability to request the deletion or modification of Incident Data. This data is stored in compliance with minimum data retention periods outlined in NOAA's Records Retention Policy and comply with NARA requirements. No Sensitive PII is requested from users during the course of our investigations and/or data log collection, however, if present on a system that is being investigated forensic images are required to remain forensically sound which prohibits their modification. BII such as system information or asset details, may be requested if it provides context to an ongoing investigation. BII obtained in this manner will be retained as part of the Incident record.

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

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Information that is collected is done so through general log collection or through collection of incident data. This information is kept in its entirety and is unable to be reviewed or altered. For the video surveillance, there is a sign posted on the door to the area that states "Notice this area is under 24-hour video surveillance. You are warned." Those entering the room have been alerted that they could be on camera. NOAA0520 is responsible for reviewing the video footage on a need-to-know basis.

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:** All activity for NOAA0100 is tracked and monitored within the SIEM
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 12/07/2025 ☐ 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 controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
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 DOC 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. *(Include data encryption in transit and/or at rest, if applicable).*

Discretionary access controls are implemented throughout NOAA0100 for access to forensic data. NOAA0100 utilizes SIREN, which is a workflow that encompasses NOAA0100's SOAR platform and NOAA0900's Google Workspace, for Incident Response Reporting and provides an IR 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 within SIREN/SOAR is redacted from end user views, and copies maintained on the database are only shared for law enforcement activities. The TICAP infrastructure processes sensitive PII on port mirrors of egress/ ingress traffic to conduct security analysis of systems. 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. Methods and technologies employed to protect PII, including video data, consist of physical security of the facility and room where the data is maintained with limited access to authorized contract personnel.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?

X Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 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, number, and link. *(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; COMMERCE/DEPT-31 Public Health Emergency Records of Employees, Visitors, and other Individuals at Department Locations.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

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: GRS 3.1: General Technology Management Records GRS 3.2: Information System Security Records GRS 5.3: Continuity and Emergency Planning Records GRS 5.6: Security Management Records GRS 6.3: Information Technology Records NOAA Records Management Schedules: NOAA RS Chapter 2200: Records of the CIO NOAA RS Chapter 2300: Gen. IT Management Records NOAA RS Chapter 2400: Information System Security Records
	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 Level

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. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	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 level. *(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 the submission of forms and information as directed by the Privacy Office.
X	Obligation to Protect Confidentiality	Provide explanation: As part of its cybersecurity mission, the NOAA0100 system may collect BII and Sensitive PII during incident response activities. This includes information that may have been compromised, intentionally or inadvertently transmitted, or identified during forensic analysis of affected systems. The collection and use of such data is conducted strictly in support of detecting, analyzing, and mitigating security incidents that pose a risk to NOAA's information systems and operations. NOAA has a critical responsibility to safeguard the confidentiality of BII and Sensitive PII. Access to this data through NCSC's network monitoring, including deep packet inspection and log analysis, is strictly limited to authorized personnel with a demonstrated need-to-know. These individuals

		must hold appropriate clearances and are required to sign and adhere to non-disclosure agreements (NDAs) governing the handling of sensitive data. NOAA0100 ensures that all BII and Sensitive PII collected through security operations are protected throughout its entire lifecycle, from initial identification and handling through secure storage, use, and disposition. This protection includes the implementation of access controls, encryption, auditing, and secure data retention practices in accordance with NOAA, DOC, and federal privacy and security regulations ensuring that the obligation to protect confidentiality is met.
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 an NDA and validated need-to-know.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

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 SSNs 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. Information associated with incidents is collected by NOAA0100, but is not stored within the NOAA0100 boundary. Incident information is stored within the NOAA0900 boundary as a part of Google Workspaces.

12.2 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: Previously, incident information was both collected and stored within the NOAA0100 boundary. Since NIRRA and CASIS are no longer a part of NOAA0100, incident information is collected by NOAA0100 but is stored within the NOAA0900 boundary.

	No, the conduct of this PIA does not result in any required business process changes.

12.3 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: Data is no longer stored on physical hardware but within the NOAA0900 cloud environment.
	No, the conduct of this PIA does not result in any required technology changes.