Version Number: 01-2019

U.S. Department of Commerce
NOAA

Privacy Impact Assessment for the
National Weather Service Pacific Region
NOAA8883

Reviewed by: 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

Jennifer Goode 03/10/2021

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/National Weather Service Pacific Region (NOAA8883)

Unique Project Identifier: 006-00035110400-48-03-00-06-00

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

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

General Support System

(b) System location

RHQ Pacific Region (Honolulu, HI), WFO Honolulu (Honolulu, HI), WFO Guam (Barrigada, GU), WSO Pago Pago (Pago Pago, AS), DCO Lihue (Lihue, HI), DCO Hilo (Hilo, HI), and the Caribbean Tsunami Warning Program (Mayaguez, PR).

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

The NWS PR interconnects with the NWS Enterprise Mission Enabling System (NOAA8850) for centralized user authentication, National Oceanic and Atmospheric Administration Corporate Services (NOAA1200) for audit collection of automated information technology records such as computer application security logs, and the NWS Weather and Climate Computing Infrastructure Services (NOAA8860) as its WAN provider.

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

The NWS PR (FIMSA ID: NOAA8883) information technology general support system is composed of various field and headquarter office local area networks (LANs) and their directly connected information systems such as workstations, servers, printers, etc. which are linked together by a wide area network (WAN) used to support weather forecasting throughout the

Pacific Ocean. The system is primarily used to provide administrative support and supplemental operational services and specifically excludes from its accreditation boundary systems deemed as major applications or programs of records as well as various partner systems, though transit may be provided in some cases.

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

Users are identified and authenticated using DoD issued Common Access Card (CAC) and only with Government Furnished Equipment (GFE) computers. Their CACs and respective PIN are required to access the employee's Windows Domain account

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

Information transmitted to and from the system is via the NOAA 8883 N-Wave\TICAP system. If a data transmission involves a privacy consideration, a PR employee would use the DOC provided secure file transmission system. PR employee personnel recommend the DOC secure file transfer method as standard practice to receive sensitive data into the system.

(g) Any information sharing conducted by the system

Federal civil servants and private contractors under contract with the NWS working on behalf of the Pacific Region access parts of the system in support of its mission. Select PII is shared with Department of the Defense Joint Base Pearl Harbor-Hickam Pass and ID Office, the Department of Commerce Western Region Security Office, and various National Oceanic and Atmosphere Administration administrative offices such as Human Resources or Finance as applicable.

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

The statutory authority for collection of information addressed in this privacy impact analysis is 5 U.S.C. § 301. Additional authorities:

44 U.S.C.; 3101; 5 U.S.C. 4101 et seq., 5 U.S.C. 1302, 3302, E.O. 10577, 3 CFR 1954-1958 Comp. p. 218, E.O. 12107, 3 CFR 1978 Comp. p264; and Federal Personnel Manual and related directives of the agencies cited above; Budget and Accounting Act of 1921; Accounting and

Auditing Act of 1950; and Federal Claim Collection Act of 1966.

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

Moderate

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.
_____ 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):					

____ 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.

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 (version 01-2015).

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

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		h. Alien Registration		l. Vehicle Identifier	

d. Employee ID		i. Credit Card	X**	m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: New employees that are in-processing will include SSN on their SF-2809 Health Benefits Registration Form, SF-1152 Beneficiary Form, etc. **These are government cards, accounts, and records, to streamline accounting for reimbursement.					

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	
c. Alias		j. Home Address	X	q. Military Service	X
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	
g. Citizenship	X	n. Religion			
u. Other general personal data (specify):					

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

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X	d. Photographs	X	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
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		f. Contents of Files	X
g. Other system administration/audit data (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	X		
Other (specify):					

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

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

It is the responsibility of the submitter to assess the data that is collected and verify the accuracy with the receiving system personnel processing the data in the case of cyclic personnel related data.

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		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			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		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):			

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).

- GPD, IN, and WRD information is collected from employees during in processing in order to complete various human resources and administrative requirements such as the employee's Declaration for Federal Employment (OF-306 form), Employment Eligibility Verification Form (I-9 form), driver's license/passport information, Employee's Withholding Allowance Certificate (W-4 form), Hawaii Employee Withholding Allowance Certificate (HW-4 form), Employee Address (CD-525 form), Health Benefits Registration Force (SF-2809), Direct Deposit Form (SF-1199A), Employee Benefits, etc. All said forms can be found on the NOAA "New Employees" website (https://www.noaa.gov/new-employees).
- DFB information is collected from employees during in processing in order to complete initial hire security background checks as part of the package sent to the Department of Commerce Office of Security.
- GPD and WRD information maintained on employees and used to create detailed administrative employee profiles and maintained for reference.
- WRD information is collected from subordinate employees by supervisors to develop and maintain employee performance plans.
- GPD information is collected from employees for emergency contact purposes.
- SAAD information is collected from information technology system users for operations and maintenance, security, and human resources activities.
- WRD and GPD information is collected, maintained, and disseminated from employees and contractors to create information technology authentication credentials which are used to access Pacific Region information technology systems.

- GPD and IN information, including passport numbers, is collected from foreign nationals and visitors to determine facility and/or site access.
- IN information is collected, maintained, and distributed by individual GSA SmartPay account holders to meet records retention requirements under the Federal Acquisition Regulation.

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.)

Potential threats to the privacy of sensitive information residing in the NOAA8883 information system include insider threats, employees with excessive access permissions, and accidental information disclosure. Controls that have been put in place to reduce the likelihood of occurrence include initial and refresher training on the appropriate handling of sensitive information, periodic reviews of user access permissions, security background investigations, timely removal of system access for terminated employees, and maintaining/proper disposal of information in accordance with NOAA Records Schedules.

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		X
DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	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	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: - PR makes use of Microsoft Active Directory Services to provide centralized authentication and authorization capabilities across the system. Within the National Weather Service each region is an individual domain which is part of the NWS Enterprise Mission Enabling System (EMES/NOAA8850) Government Owned National Active Directory Service (GONADS), a unified forest. Due to the inherent way Active Directory Services work, there is no effective way to control or prevent SAAD data from leaking nor its directly associated WRD and GPD between the two organizations. - PR interconnects for network transit purposes with other IT systems which are authorized to process PII, such as NOAA1200, National Oceanic and Atmospheric Administration Corporate Services Local Area Network and NOAA8860, National Weather Service Weather and Climate Computing Infrastructure Services. While PII should never transit these interconnections in unencrypted format, no effective controls are in place to prevent said leakage.
	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 all federal-wide forms	
X	Yes, notice is provided by other means.	Specify how: Authorized users of PR information technology systems are notified both in the NOAA rules of behavior and system usage consent warning banner that there is no expectation of privacy while using these systems which includes SAAD and directly associated WRD, and GPD information. Unauthorized users have no reasonable expectation of notification.
	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: All individuals have the opportunity to decline, verbally or in writing to the person requesting the information,

		to provide information when individually requested, though failure to provide it may result in adverse administrative actions such as site access denial or loss of employment/contract. Individuals may decline to provide SAAD information, but they would not be able to use Pacific Region technology assets. SAAD information is automatically generated and captured by using Pacific Region information technology assets.
	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: Individuals are given the opportunity to consent, in writing, to their supervisors, to only particular uses of their PII/BII, at the point at which the supervisor asks for the information. The supervisor explains the purpose of the collection, if it is voluntary or if lack of provision will affect their employment or access to services, and how/if the information will be shared. If there is a form, this information is also provided on the form. However, completion of each form or compliance with other specific requests for information, is for a specific purpose only, e.g. human resources, COOP, travel.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: SAAD information and directly associated WRD and GPD is generated, maintained, and disseminated automatically via system usage and correlated among various IT and IT security applications, often real-time, hence it is not possible for users to consent to its usage outside their inherent consent simply by virtue of use.

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: System Wide: - Authorized information technology users can always review or update their individual credential related GPD and WRD information via submitting an IT service request ticket through the system or by contacting their local information technology operations and maintenance staff. Pacific Region Headquarters - Administrative Management Division: - Employees have the opportunity to review and update their information any time they receive a earning and leave statement, electronic fund transfer, or travel documents.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: It is not possible to allow individuals to update SAAD information pertaining to them given the automated and often immutable nature of the audit logs.

Section 8: Administrative and Technological Controls

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

	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 access to PII in electronic form is recorded via automated operating system audit logging mechanisms for a minimum period of one hundred and eight days
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): 05/19/2020 ☐ 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.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	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).*

Pacific Region personnel with access to PII use the Department of Commerce secure file transfer web application to exchange sensitive PII with relevant external system entities per agency direction on an individual transfer basis.

Internally the system does not allow for the protection of sensitive PII commensurate with agency and bureau policy

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)*: DEPT-6, Visitor Logs and Permits for Facilities Under Department Control (https://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-6.html) DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons (https://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-9.html) DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies. (https://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html)
	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: - NOAA Records Control Schedule Chapter 200-09. - NOAA Records Control Schedule Chapter 200-23. - NOAA Records Control Schedule Chapter 207 - NOAA Records Control Schedule Chapter 304 - NOAA Records Control Schedule Chapter 309 - NOAA Records Control Schedule Chapter 2300 - NOAA Records Control Schedule Chapter 2400
	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.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	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: Identity may be discovered by compiling contact information, SSN and/or passport number
X	Quantity of PII	Provide explanation: There is a significant amount of PII and some BII, primarily pertains to local Federal employees and a minimal number of vested contractor, interns, intended visitors, and volunteers.
X	Data Field Sensitivity	Provide explanation: There are several sensitive data fields.
X	Context of Use	Provide explanation: Data is collected only for the stated purpose.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: All PII collected is only accessible internally within the line office.
	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.)

Threats to privacy would primarily be insider threat, whether malicious or unintended. There have been instances where individuals have sent their own or another person's privacy data via Bureau email instead of secure file transfer. The individuals are counseled and re-trained when this occurs and is reported or was detected.

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

	Yes, the conduct of this PIA results in required business process changes.
	Explanation:
X	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.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.