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

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

Catrina D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2017.05.12 12:14:04 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
National Oceanic and Atmospheric Administration National Weather Service Pacific Region (NOAA8883)

Unique Project Identifier: 006-00035110400-48-02-00-02-00

Introduction:

The National Weather Service (NWS) Pacific Region (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.

As a course of operations contact information is collected on local Federal employees to support emergency contact rosters. In addition, various amounts of work related information as well as basic personal information is collect on employee's to support day-to-day administrative efforts such as travel documents, performance plans, in and out processing of new and current employees, system user accounts, procurement records, etc. and are stored by the employees themselves and as well as various support staff such as supervisor or administrative assistants, in addition to automatic collection by IT staff and system logs as part of day-to-day operation and maintenance such as usernames, addresses, system and network activity logging, etc.

Various amount of PII to establish identity such as passport numbers, nationality, contact information, etc. are collected from foreign national visitors and guests on a transitory basis and transmitted to the applicable security office for building and installation access as well as for the purpose of protecting deemed exports and controlled technology.

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.

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.SC. 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.

This system is classified as a moderate system under the Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.

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):					

__X__ This is an existing information system for which there is not a recent PIA.

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		i. Credit Card	X**
b. Taxpayer ID	X	f. Driver's License	X	j. Financial Account	X**
c. Employer ID		g. Passport	X	k. Financial Transaction	X**
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. 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	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
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			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		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):					

Other Information (specify)
Predecisional contract documents (offerors' responses for proposals or for information).

2.2 Indicate sources of the PII/BII in the system.

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 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	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): For operational purposes in support of the watch, warning, and advisory process.			

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.
- 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.

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):			

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 NWS each region is an individual domain which is part of the NWS 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, 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. This will be remediated in May 2017.
	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 each relevant form. *All federal-wide forms have PA statements, and the only form that is not federal-wide is the travel form, to which a PAS has been added. This form is included in this PIA, just before the signature page.*	
X	Yes, notice is provided by other means.	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.

	Yes, individuals have an opportunity to decline to provide PII/BII.	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 the 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.	

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.	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. Given 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 it is not possible for users to consent to its usage. However, there is only one use of this information in this context.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	

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.	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. 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.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	

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 by policy.
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 FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): _4/29/2016_____ ☐ 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 as determined by the Agency and Bureau Common Controls policy; or have an approved Plan of Action and Milestones (POAM).
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 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.

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 though this is being actively addressed and estimated to be in place by May 1, 2017.

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: DEPT-18, Employees Information not covered in other system of record notices, DEPT-6, Visitor Logs and Permits for Facilities Under Department Control; DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons.
	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:

	- 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 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.
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: 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 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: As a result of this PIA, a deficiency was discovered in that the Pacific Region was not appropriately encrypting PII in transit contrary to agency policy. Upon discovery an initiative was immediately embarked upon to upgrade all systems within the region to support server message block version three which resolves deficiency with an expected completion date of May 1, 2017.
	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: As a result of this PIA, a deficiency was discovered in that the Pacific Region was not appropriately encrypting PII in transit contrary to agency policy. Upon discovery an initiative was immediately embarked upon to upgrade all systems within the region to support server message block version three which resolves deficiency with an expected completion date of October 1, 2016.
	No, the conduct of this PIA does not result in any required technology changes.

REQUEST FOR OFFICIAL TRAVEL BY PACIFIC REGION PERSONNEL

Name of Traveler:	Signature:
Home Duty Station:	Request Date:

Purpose of Travel:

Itinerary (TDY): Specify Dates at Each Location:

~~Itinerary (Personal-A/L or Non-Duty Stopover): Specify Dates, Destination(s), and Contact #s while in travel status.~~

Type of Travel: Domestic Foreign Both Country Clearance Required: Yes No

Gifted Travel: Yes No

Sponsor:

Gift Description:

Length of Travel: Start Date:

End Date:

What Do You Require: Travel Representative will make all reservations unless otherwise specified in Remarks. Please check appropriate boxes.	Yes	No	Remarks – Clarify Special Requirements
SATO Reservations			
~~Airport Departure Fees~~			
~~Hotel~~			
Hotel Room Taxes and Fees			
Rental Car			

Taxi Airport Parking POV Roundtrip miles _____

Official Phone Calls (Use calling card whenever possible)

Hire Local Labor Materials Estimated $

Authorized Expenses: Hardware Parts Excess Baggage

Conference/Registration Fees

Other/Comments

Travel Funding (Use Complete Accounting Code)

PRH:

NWSH:

OTHER:

Supervisor/MIC/OIC Authorization:

Signature:

Date:

For PRH Use Only

Division Chief:	Approval: Yes	No	Signature:	Date:
Reason for Disapproval:				
AMD Chief:	Approval: Yes	No	Signature:	Date:
Reason for Disapproval:				
Regional Director:	Approval: Yes	No	Signature:	Date:
Reason for Disapproval:				

Attach all supporting documentation from outside (inviting) agencies, IF ANY. If foreign travel, check with Division ASA before submitting request. Obtain all signature approvals before submitting.

Privacy Act Statement

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: The principal purpose of this form is to obtain travel approval for National Weather Service/Pacific Region (hereinafter referred to as "NWS/PR") personnel and invitational travelers who have been assigned to temporary duty locations.

Routine Uses: This information will be used by NWS/PR travel preparers to complete travel authorizations. Travel approvers and budget personnel will use this information to confirm that there is sufficient funding for requested travel and to track the funding source.

Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among NOAA staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice, Commerce DEPT-18, Employees Information not covered by notices of other agencies.

Disclosure: Furnishing this information is voluntary; however, failure to provide accurate information may delay or prevent completion of required travel documentation.