

U.S. Department of Commerce NOAA



Privacy Impact Assessment for the NOAA5032 Wallops Command and Data Acquisition Station (WCDAS) Administrative Local Area Network (LAN)

Reviewed by: _____, 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: 2016.06.06 14:25:39 -04'00'

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

Date

U.S. Department of Commerce Privacy Impact Assessment NOAA WCDAS Administrative LAN

Unique Project Identifier: NOAA5032 (not affiliated with an Exhibit 300).

Introduction: System Description

The WCDAS (Wallops Command and Data Acquisition Station) Administrative LAN (NOAA5032) is located within the WCDAS computer facility in Wallops Island, VA. The WCDAS Administrative LAN supports the NESDIS mission by providing IT resources to WCDAS personnel. Although the system does not collect or store PII (other than employee contact information) or BII, the system does support office functions that distribute PII and BII such as electronic mail, purchasing, logistics, facility management, inventory, human resource, and contract administration. These functions use paper files as the source of the PII and BII distributed; for purchasing and human resources functions, information from paper files is typed into portals or emails.

WCDAS Administrative Local Area Network (LAN) is a standard office automation environment that relies on the NOAA NOC (NOAA 0200) for e-mail, VPN access to the NSOF Administrative LAN (NOAA5044), and Internet connectivity.

Email is addressed in the NOAA1200 PIA revision in process.

Employee PII is collected for Emergency Contact information.

The WCDAS Administrative LAN does not share this information with any agency. The Federal Information Processing Standard (FIPS) 199 security impact category for the system is 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.
 This is an existing information system with no changes.

(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		f. Commercial Sources		i. Alteration in Character	

Management Changes				of Data	
j. Other changes that create new privacy risks (specify):					

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*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
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:					

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	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address		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	
b. Job Title	X	e. Email Address	X	h. Work History	
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	

g. Other system administration/audit data (specify):

Other Information (specify)

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

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

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

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

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

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

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

Section 3: System Supported Activities

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

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

--

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

Section 4: Purpose of the System

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

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	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).

The Business Continuity Plan (BCP) is used for emergency contact of WCDAS employees. This information is collected from Federal Employees only.

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

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

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

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

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

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

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.*)

	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found on the	
X	Yes, notice is provided by other means.	Specify how: Notification is provided in writing by the employee's supervisor or by the administrative staff.
	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: Federal employees have an opportunity to decline to provide PII to their supervisors, in writing, but they would not be contacted during an emergency. Consent in general to the provision of PII is implied through continued employment by the individual in that position requiring the PII collection.
	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 may choose not to be contacted during an emergency, by declining in writing to their supervisors. This is the only use of the information.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals may consult administrative personnel who have access to their PII and provide updates to them. This information is conveyed in writing as part of the employee orientation.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

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

	All users signed a confidentiality agreement or non-disclosure agreement.
	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.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>_8/11/2015_____</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
	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.

PII/BII on this IT system is protected through the use of hardware and software firewalls, Cisco ASA Firewalls, Cisco IPS; Windows software firewalls; Tripwire Enterprise; Tripwire Log Center; ArcSight deployed and reporting back to NOAA Enterprise Security Services; HSPD-12 compliant with two factor authentication; McAfee Data Loss Prevention enabled, blocking all unauthorized USB drives and external hard drives.

Section 9: Privacy Act

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

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

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number (list all that apply): DEPT-18, Employees Personnel Files not Covered by Notices of Other Agencies.
	Yes, a SORN has been submitted to the Department
	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 Chapter 200-01
	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	
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.

X	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.
	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.)*

	Identifiability	Provide explanation:
X	Quantity of PII	Provide explanation: Contact information only is maintained for a BCP.
	Data Field Sensitivity	Provide explanation:
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 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.

12.2 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.

Points of Contact and Signatures

<p>Information System Security Officer or System Owner Name: Van D. Crawford Office: NESDIS/OSPO/WCDAS Phone: 757-824-7375 Email: van.d.crawford@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="font-size: small;">Digitally signed by CRAWFORD.VAN.D.1128805105 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=CRAWFORD.VAN.D.1128805105 Date: 2016.01.27 07:58:00 -05'00'</p> <p>Signature: _____</p> <p>Date signed: <u>1/27/2016</u></p>	<p>Information Technology Security Officer Name: Nancy DeFrancesco Office: NESDIS ACIO-S Phone: 301-713-1312 Email: nancy.defrancesco@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="font-size: small;">Digitally signed by DEFRANCESCO.NANCY.A.1377370917 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=DEFRANCESCO.NANCY.A.1377370917 Date: 2016.01.27 09:55:32 -05'00'</p> <p>Signature: <u>DEFRANCESCO.NANCY.A.1377370917</u></p> <p>Date signed: <u>01/27/2016</u></p>
<p>Authorizing Official Name: Vanessa Griffin Office: NESDIS/OSPO Phone: 301-713-7311 Email: vanessa.griffin@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="font-size: small;">Digitally signed by GRIFFIN.VANESSA.L.1204308663 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRIFFIN.VANESSA.L.1204308663 Date: 2016.01.27 11:06:36 -05'00'</p> <p>Signature: <u>GRIFFIN.VANESSA.L.1204308663</u></p> <p>Date signed: <u>January 27, 2016</u></p>	<p>Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p style="font-size: small;">Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2016.01.27 15:05:17 -05'00'</p> <p>Signature: <u>GRAFF.MARK.HYRUM.1514447892</u></p> <p>Date signed: _____</p>

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