Version Number: 01-2017

U.S. Department of Commerce
National Institute of Standards and Technology
(NIST)

Privacy Impact Assessment
for the
Office of Safety, Health, and Environment (OSHE) System

Reviewed by: Susannah Schiller, Acting, 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

09/30/2019

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

U.S. Department of Commerce Privacy Impact Assessment
National Institute of Standards and Technology (NIST)

Unique Project Identifier: 150-01

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.
The Office of Safety, Health, and Environment (OSHE) supports NIST in carrying out its mission safely and in maintaining safety as an integral core value and vital part of the NIST culture. The OSHE information system supports this role and includes the following components:

- The Radiation Monitoring System (RMS) is used to monitor radioactive sources above a certain level. The RMS has detectors, processors, cameras, and network connectors monitoring sensitive equipment and their surrounding physical locations. The monitoring provides unidirectional information to Physical Security consoles.
- The Health Physics System (a.k.a., HAPPY) provides inventory of radioactive material, ionizing machines, radiation equipment, physical radiation laboratories, safety training, and tracking of radiation doses that NIST staff receive. An additional system, AREV, has the same functionality, but serves as an archive from 2006 and prior.
- A Health Unit Database tracks NIST staff health scheduling (e.g., frequency) and audiometer and spirometer test results.
- The Health Unit Intake procedures require completion of an intake form from any NIST staff or visitor for identification purposes, and personal health information.

(a) Whether it is a general support system, major application, or other type of system
NIST 150-01 is a General Support System.

(b) System location
The components are located at the NIST Gaithersburg, Maryland and Boulder, Colorado facilities within the continental United States.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
The RMS systems can only communicate with systems located in the physical security guard's offices via a private network in Buildings 101 and 318 over the isolated Research Equipment Network (184-12).

All system connectivity to Happy and all the Health Unit data is via TCP/IP across the NIST Network Infrastructure (SSP 181-04) to the encrypted file share (184-12). The NIST

Network Infrastructure system provides all services for physical cabling, network frame synchronization/flow control/error checking, routing, switching, and DNS. Data is encrypted with FIPS 140-2 compliant technologies in transit and at rest. The Health Unit intake forms are standalone and not interconnected.

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

The RMS provides continuous monitoring capabilities via a live video feed for physical security to prevent unauthorized access to radioactive material.

Access to and inventory of radioactive material are stored in a database application, HAPPY. Owners of material access and update the database via secured, authorized computers.

Physical test results are stored in applications via specialized software attached to diagnostic machines. When an existing patient visits the Health Unit, a patient's file may be retrieved by name.

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

The RMS is viewed by NIST police on a continuous basis.

HAPPY data is retrieved by authorized individuals by opening the database and retrieving the source by identifier. Source owners can be retrieved by name.

Health Unit information is retrieved by patient name.

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

RMS data is only transmitted over an isolated network and encrypted during transit.

Happy and Health Unit data are transmitted via encrypted channels.

(g) Any information sharing conducted by the system

Since it is personal health information (PHI), data is shared minimally. In support of licensing, NIST is required to share information in HAPPY with the Nuclear Regulatory Commission (NRC).

Health Unit Intake procedures provide patients an explanation of how information collected is used. Occupational Health Records (OHR) are owned by NIST, but regulated by the Occupational Safety and Health Administration, and shared with other internal DOC and NIST business units. Personal health information is shared as a circumstance or situation warrants, only with the consent of the patient.

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

The National Institute of Standards and Technology Act, as amended, 15 U.S.C. 271 et seq. (which includes Title 15 U.S.C. 272) and section 12 of the Stevenson-Wydler Technology Innovation Act of 1980, as amended, 15 U.S.C. 3710a.;

5 U.S.C. 5701-5709 and 5721-5739, 28 U.S.C. 3101-3105, Debt Collection Act of 1982 (Pub. L. 97-365); 26 U.S.C. 6402(d); and 31 U.S.C. 3711, The "Federal Information Security Management Act of 2002 (FISMA).

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system is Moderate. The RMS component is deemed low.

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.

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	
b. Taxpayer ID	X	f. Driver's License	X	j. Financial Account	
c. Employer ID		g. Passport	X	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: *The collection of SSN is required for reporting to the Nuclear Regulatory Commission, and for archiving patient					

records to the National Archives and Records Administration (NARA).

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name	X	h. Place of Birth		n. Financial Information	
c. Alias	X	i. Home Address	X	o. Medical Information	X
d. Gender	X	j. Telephone Number	X	p. Military Service	
e. Age	X	k. Email Address		q. Physical Characteristics	X
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	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	
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 Describe how the accuracy of the information in the system is ensured.

OSHE has several checks through the patient interaction process including involvement from the data source (patient) to verify accuracy.

The RMS systems are inspected and calibrated quarterly by Department of Energy staff.

Information entered into HAPPY is collected from the source and integrity controls are built into the database.

The spirometer and audiometer software have built-in calibration mechanisms that are run each time the software is launched. Additionally, the manufacturer comes annually to ensure proper calibration.

The Health Unit collects the intake form directly from individuals and each visit they are asked to update it.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB number 0693-0080 (expires 7/31/2021)
	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):			

	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	
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 components of the system collection information for administrative matters.

The Health Physics System collects information about NIST employees and associates. The radioactive materials inventories are tracked to assure security and control of radioactive materials and to demonstrate license limit compliance. The instrument calibration and QA data are maintained to assure functionality and reliability of the safety related monitoring equipment. Radiation Monitor inspection reports are collected to document safety and regulatory compliance, and personnel training records are maintained to assure authorized users have received appropriate training and to document regulatory compliance.

The Health Unit Databases collects information about NIST employees and associates. The frequency of a person's examinations and need for treatment is in part determined by their age, requiring the tracking of DOB. This file tracks when someone has been examined, their organization, and the test(s) performed.

The Health Unit Intake collects information about NIST employees, associates, or visitors. The intake form requires NIST employees provide their SSN, so their medical records can be sent to National Archives and Records Administration (NARA). Associates or visitors provide their driver's license, non-driver identification, or passport number so their records can be retrieved from archives that are stored on NIST property. If they do not have their identification, they can provide their mother's maiden name as a unique identifier. Additional information is obtained to provide medical treatment.

5.2 Describe any potential threats to privacy 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.)

Unauthorized access could result in a breach of users' information. Information system security controls used to protect this information are implemented, validated, and continuously monitored. NIST user access is restricted to authorized users. Annual training and rules of behavior are provided to internal users on the appropriate handling of PII. The components have records schedules and procedures in place to dispose of data accordingly.

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 (NRC)	
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):	X (Health Intake)		

	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	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: https://www.nist.gov/privacy-policy The Health Unit Intake form (NIST-986) includes a statement about collection and use. In addition, NIST Associates and Visitors sign a HIPAA consent form that describes the collection.	
X	Yes, notice is provided by other means.	Specify how: Individuals are notified about the collection for HAPPY through the NIST Request for Personal Radiation Monitoring Services (NIST-366A).
	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: For HAPPY, individuals have an opportunity to decline providing information by not completing the requisite NIST Request for Personal Radiation Monitoring Services (NIST-366A). However, access to radioactive material will be denied. For Health Unit Intake, individuals have opportunity to decline providing information, however, care may be affected and future retrievability will be impacted.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: For RMS, individuals do not have an opportunity to decline surveillance. If an individual enters the area, their actions are recorded. For Health Unit Databases, individuals do not have opportunity to consent to particular uses as the databases are utilized for managing scheduling and test results. Due to these reasons, individuals do not have opportunity to decline.

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: For HAPPY, a letter of request with a signature authorization is required before the data can be released to any third-party entity other than the established regulatory agencies (NRC). Authorization of release to the NRC is part of NIST Request for Personal Radiation Monitoring Services (NIST-366A). For Health Unit Intake, individuals have opportunity to consent to particular uses of their information on the Intake form (NIST-986). In addition, NIST Associates and Visitors sign a HIPAA consent form which obtains consent for the collection.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: For RMS, individuals do not have an opportunity to consent to particular uses as this is a monitoring system for individuals entering the area and for equipment. For Health Unit Databases, individuals do not have opportunity to consent to particular uses as the databases are utilized for managing scheduling and test results. Due to these reasons, individuals do not have opportunity to consent.

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: For HAPPY, individuals have opportunity to review/update their information by submitting a service request through safety.nist.gov For Health Unit Databases, individuals have opportunity to review/update their information by contacting the Health Unit. For Health Unit Intake, individuals have opportunity to review/update their information by contacting the Health Unit.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: For RMS, individuals do not have an opportunity to review/update their information as this is a monitoring system for individuals entering the area and for equipment.

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: Access logs are kept and reviewed for anomalies. The Health Unit intake forms and patient charts are continuously monitored when not locked in secured file cabinets.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 4/1/19 ☐ 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 supporting 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 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).*

The RMS, HAPPY, and Health Unit Database components are administered on internal NIST networks protected by multiple layers of firewalls. Automated audit reduction, monitoring, and reporting is employed on each component. The components are located at the NIST Gaithersburg, Maryland facility within the continental United States.

Unauthorized use of the components is restricted by user authentication, and role-based access is employed.

For information sharing, PII/BII is transferred in a secure fashion using FIPS 140-2 encryption. Databases are maintained on secure file shares.

Physical security controls are employed on Health Unit Intake forms.

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, number, and link. *(list all that apply)*: NIST-4: Employee External Radiation Exposure Records Commerce/DEPT-18: Employees Personnel Files Not Covered by Notices of Other Agencies OPM/GOVT-10: Employee Medical File System Records
	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: NIST Records Schedules 103, Health Physics NIST Records Schedules 104 – 107, Nuclear Reactor Program Records GRS-2.7, Employee Health and Safety 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 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 levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Identifying numbers can uniquely identify an individual.
X	Quantity of PII	Provide explanation: Personal Health information is documented in paper records within the Health Unit
X	Data Field Sensitivity	Provide explanation: Personal Health Information coupled with identifying numbers can present risk of disclosure.
	Context of Use	Provide explanation:
X	Obligation to Protect Confidentiality	Provide explanation: Personal Health Information is entrusted to NIST for patient care, and by its nature requires confidentiality.
X	Access to and Location of PII	Provide explanation: Personal health information is documented in paper records within the Health Unit.
	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.)

The threat of unauthorized access and/or misuse exists but is reduced by effective security controls, internal user training and requiring internal users to sign relevant rules of behavior agreements. Threats could arise from collecting more data than is necessary by not employing data minimization. Threats could exploit data secondary use (using personal information for a purpose other than the purpose for which it was collected). Only data required for the OSHE mission is used in OSHE.

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.