Version Number: 01-2019

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

Privacy Impact Assessment
for the
137-01 Emergency Services Office System

Reviewed by: Matt Wilkinson, 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

Jennifer Goode 02/22/2021

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: 137-01

<u>Introduction</u>: 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
(b) System location
(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
(d) The way the system operates to achieve the purpose(s) identified in Section 4
(e) How information in the system is retrieved by the user
(f) How information is transmitted to and from the system
(g) Any information sharing conducted by the system
(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

a) *Whether it is a general support system, major application, or other type of system*
The Emergency Services Office System is a major application comprised of the following components: Physical Security Systems at Boulder, Physical Security System at Gaithersburg, Visitor Registration System including Visitor's Center Application, Emergency Notification System (ENS), and Report Exec. These components collectively provide the tools necessary to fulfill its mission to deliver emergency and physical security services for the protection of personnel, property, and activities on NIST facilities.

b) System location
The ENS component is hosted in Burbank, California. The remaining 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 Physical Security Systems (Boulder and Gaithersburg) are standalone systems on an isolated network that do not interconnect with other NIST systems.**
- **The Visitor Registration System interconnects with the NAIS (one-way transmission only) for foreign national visitor processing.**
- **The Emergency Notification System (ENS) is hosted and maintained externally by the service provider and interconnects with NIST System 183-01.**
- **Report Exec does not interconnect with other NIST systems.**

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

- **The Physical Security Systems (Boulder and Gaithersburg) support physical security operations at NIST Boulder and Gaithersburg campuses. These systems include digital video camera and closed-circuit television monitoring of the campus and facilities.**
- **The Visitor Registration System is an internally hosted application for pre-registering visitors to the NIST campus. The application is used for printing NIST temporary visitor badges using registered data and images captured from scanned identification at check-in for all visitors.**
- **The Emergency Notification System (ENS) is an externally hosted solution that provides tools for reaching pre-defined contacts during an emergency. The method of communication may include phone, text, email, paging device number, and other communication devices to enable NIST to rapidly and efficiently reach staff during emergencies.**
- **Report Exec is an incident reporting and records management software to assist the Police Services Group in Boulder and Gaithersburg in writing detailed investigative reports, tracking daily dispatch calls, and recording other law enforcement activities.**

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

The information is retrieved by name of the individual or other unique identifier.

f) How information is transmitted to and from the system

- **Physical Access Control Systems (Boulder and Gaithersburg): Information is inherited from existing data sources and is manually input into the system by ESO staff.**
- **Visitor Registration System: Data is entered by a NIST employee or associate through a web-based interface during pre-registration. When the visitor arrives, their identification is scanned. The pre-registration data and an image captured from the scanned identification are used to print a NIST temporary visitor badge at check-in.**
- **Emergency Notification System (ENS): Personal contact data is provided voluntarily by NIST staff via the secure ENS member portal that requires login or through NIST System 183-01.**

- **Report Exec: Information is collected by the police officers and/or dispatch operators directly from the data subject and manually entered into the system for investigation and follow up purposes.**

g) Any information sharing conducted by the system
The ENS component shares information with NIST System 183-01. All other components within this system do not share information with other internal NIST business units, other than on a case-by-case basis. Information is shared with the Department of Commerce, the Office of Security for background checks. Information within the system components will be shared (in the form of reports) on a case-by-case basis with the federal, state or local government agencies, including law enforcement, as the need arises, when a legitimate need to know exists.

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.
27 Stat. 395 and 31 Stat. 1039, and all existing, applicable NIST and Department policies, regulations and directives concerning the tracking, security processing, and support of NAs during their tenure at NIST.

5 U.S.C. 301 and 15 U.S.C. 271 et seq.; 44 U.S.C. 3101.

35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075.

Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987; 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.**

Section 1: Status of the Information System

1.1 The status of this information system:
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).

Changes That Create New Privacy Risks (CTCNPR)

Other changes that create new privacy risks:

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated.

Identifying Numbers (IN)
Social Security **File/Case ID** **Driver's License** **Passport** **Alien Registration** **Vehicle Identifier**
Other identifying numbers:
Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:
The use of the social security number is for making a positive identification to prevent identification fraud. The individual's social security number will not be disclosed external to NIST except as required by law.

General Personal Data (GPD)
Name **Maiden Name** **Alias** **Gender** **Age** **Race/Ethnicity** **Date of Birth** **Place of Birth** **Home Address** **Telephone Number** **Email Address** **Physical Characteristics**
Other general personal data:

Work-Related Data (WRD)
Work Address **Work Telephone Number** **Work Email Address**
Other work-related data:

Distinguishing Features/Biometrics (DFB)
Fingerprints **Photographs** **Scars, Marks, Tattoos** **Other distinguishing features/biometrics**
Other distinguishing features/biometrics:
Weight, height, eye color, and hair color

System Administration/Audit Data (SAAD)
User ID Date/Time of Access Contents of Files
Other system administration/audit data:

Other Information

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

Directly from Individual about Whom the Information Pertains
In Person Telephone Online
Other:

Government Sources
Other
Other:

Non-government Sources
Other:

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

System has built-in functionality to perform validation on fields to ensure that data input meets certain criteria. Accuracy of the data is dependent on the individuals providing self: identifying information or individuals providing accurate data on behalf of the visitor. **Accuracy of information is ensured through multiple reviews (e.g.. HR. background checks). Accuracy is verified within the context of granting the physical access.**

2.4 Is the information covered by the Paperwork Reduction Act?

No, the information is not covered by the Paperwork Reduction Act.
The OMB control number and the agency number for the collection:

2.5 Is there any technology used that contain PII/BII in ways that have not been previously deployed?

No

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)
Other:

Section 3: System Supported Activities

3.1 Are there any IT system supported activities which raise privacy risks/concerns?
Yes

The IT system supported activities which raise privacy risks/concerns.

Activities
Building entry readers **Other**
Other:
Video surveillance.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.

Purpose
For administrative matters **For civil enforcement activities** **For criminal law enforcement activities**
Other:

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).

Physical Security Systems (at Boulder and Gaithersburg): The identifying Numbers, General Personal Data, Work-Related Data, and Distinguishing Features/Biometrics are used for identification purposes to control physical access to NIST buildings and facilities, and provide a secure work environment for NIST employees, associates, and visitors.

Visitor Registration System: The General Personal Data are used to positively identify visitors and manage all visitor traffic entering NIST facilities.

Report Exec: The Identifying Numbers, General Personal Data, Work-Related Data, and Distinguishing Features/Biometrics are collected for incident reporting, investigation and follow up purposes.

Emergency Notification System: The Work-Related Data are used for contacting NIST staff in the event of an emergency. If disclosed by a staff person, General Personal Data (e.g., telephone number) may also be utilized and shared with NIST System 183-01.

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.)

There are associated privacy risks any time PII is made available to or used by users. A potential threat to privacy exists if the identity of an individual were to be disclosed to an unauthorized person. Role-based access controls are in place to minimize this threat. The system maintains access roles that restrict and grant access to information and functionality to support the business process need of the particular user. These individuals have undergone annual mandatory security awareness training.

Section 6: Information Sharing and Access

6.1 Will the PII/BII in the system be shared?

Yes, the PII/BII in the system will be shared

The recipients the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared.

Case-by-Case - DOC bureaus **Case-by-Case - Federal Agencies** **Case-by-Case - State, local, tribal gov't agencies** **Case-by-Case - Within the bureau** **Other (specify) below**
Other:
Case-by-Case: Investigative and court-Report exec.

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 receive information from another IT system(s) authorized to process PII and/or BII (ENS component only).
The name of the IT system and description of the technical controls which prevent PII/BII leakage:
NIST System 183-01

6.3 Identify the class of users who will have access to the IT system and the PII/BII.

Class of Users
Government Employees **Contractors**
Other:

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.

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.** **Yes, notice is provided by other means.** **No, notice is not provided.**
The Privacy Act statement and/or privacy policy can be found at:
The Privacy Act statement and/or privacy policy can be found at: https://www.nist.gov/privacy-policy
The reason why notice is/is not provided:
Physical Access Control Systems: Notice is provided through collection of data in Human Resource and NIST Associate processes. **Visitor Registration: Notification regarding inputting information into the NIST Visitor Registration component is generally stated at https://www.nist.gov/about-nist/visit/campus-access-and-security. For conference participants, notification is provided at the point of registration. Notice is also provided with instruction mechanisms for facility access (e.g., public web).** **ENS: NIST staff are notified through internal communications, and a notice is displayed on the ENS member login page.** **Report Exec: Notice is verbally provided at the time of an incident from the individual, witness, and/or during a call for some of the data.** **No:** **Report Exec: Notice is not provided for some data as the component supports law enforcement activities (i.e. violations, arrests).**

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. **No, individuals do not have an opportunity to decline to provide PII/BII.**
The reason why individuals can/cannot decline to provide PII/BII:
Physical Access Control Systems: Individuals may decline providing the required data to NIST staff, however failure to do so will result in denying access to the facilities. **Visitor Registration: Individuals may decline providing the required data to NIST staff, however failure to do so will result in denying access to the facilities.** **ENS: Individuals have an opportunity to decline providing information by not completing a profile within the component.** **No:** **Report Exec: Individuals do not have opportunity to decline providing information as the component supports law enforcement (i.e. investigations, arrests).**

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

Yes, individuals have an opportunity to consent to particular uses of their PII/BII.
The reason why individuals can/cannot consent to particular uses of their PII/BII:
ENS: Individuals have an opportunity to consent to particular uses of their information by completing a profile within the component. **No:**

Physical Access Control Systems: Individuals do not have opportunity to consent to particular uses as the information is required for processing the individual for facility access.

Visitor Registration: Individuals do not have opportunity to consent to particular uses as the information is required for processing the individual for access.

Report Exec: Individuals do not have opportunity to consent to particular uses as the component supports law enforcement activities (i.e. investigations, arrests).

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

Yes, individuals have an opportunity to review/update PII/BII pertaining to them.

The reason why individuals can/cannot review/update PII/BII:

Physical Access Control Systems: Individuals have the opportunity to update their information by contacting their Administrative staff to process the change.

Visitor Registration: Individuals have the opportunity to update information by contacting their NIST sponsor, who will then need to contact the Visitors Center to make changes/updates to their visitor's record.

ENS: NIST staff may update their information profile in the component, or through NIST System 183-01.

No:
Report Exec: Data are collected by police officers and dispatchers at the time of an incident from the individual or during a dispatch call. Only authorized personnel have access to the data. Individuals wishing to update their records may contact Police Services.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system.

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.

Staff (employees and contractors) received training on privacy and confidentiality policies and practices.

Access to the PII/BII is restricted to authorized personnel only.

Access to the PII/BII is being monitored, tracked, or recorded.

The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.

The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.

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).

A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.

Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.

Reason why access to the PII/BII is being monitored, tracked, or recorded:

Access is restricted only to employees and contractors with a “need to know" and is tracked and recorded through system logs.

The information is secured in accordance with FISMA requirements.

Is this a new system? No
Below is the date of the most recent Assessment and Authorization (A&A).
04/01/2020

Other administrative and technological controls for the system:

8.2 General description of the technologies used to protect PII/BII on the IT system. *(Includes data encryption in transit and/or at rest, if applicable).*

Physical Access Control System (at Boulder and Gaithersburg) is on an isolated network. Servers, workstations, and network devices employ access controls, and are in controlled physical spaces. Unauthorized use of the system is restricted by user authentication. Access logs are kept and reviewed for anomalies. The communications between the server and access panels are encrypted. Data at rest is encrypted.

Visitor Registration System and Visitor's Center Application are accessible on internal NIST networks protected by multiple layers of firewalls. Unauthorized use of the system is restricted by user authentication. Access logs are kept and reviewed for anomalies. Databases fully implement and enforce encryption of data in transit and at rest.

Emergency Notification System is hosted in Burbank, California. The application is served over Transport Layer Security (TLS) connection. Data at rest is encrypted. Access is controlled through enforcement of NIST credentials and session time-outs. Information is shared with a NIST system using an API.

Report Exec: Hardware access controls are employed (e.g., restricting IP addresses to only those authorized). The application server and database are hosted and accessible on internal NIST networks protected by multiple layers of firewalls. Unauthorized use of the system is restricted by user authentication. Access logs are kept and reviewed for anomalies.

<u>Section 9</u>: Privacy Act

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

Yes, the PII/BII is 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.”

Yes, this system is covered by an existing system of records notice (SORN).
SORN name, number, and link:
Commerce/NIST-1, NIST Associates **Commerce/NIST-7, NIST Emergency Locator System** **Commerce/Dept-6, Visitor Logs and Permits for Facilities Under Department Control** **Commerce/Dept-7, Employee Accident Reports** **Commerce/Dept-18, Employee Personnel Files Not Covered by Notices of Other Agencies** **Commerce/Dept-25, Access Control and Identity Management System** **GSA/GOVT-7, Personal Identity Verification Identity Management System (PIV IDMS)**
SORN submission date to the Department:

Section 10: Retention of Information

10.1 Are these records are covered by an approved records control schedule and monitored for compliance?

Yes, there is an approved record control schedule.
Name of the record control schedule:
GRS 5.6. Security Records
The stage in which the project is in developing and submitting a records control schedule:
No, retention is not monitored for compliance to the schedule.
Reason why retention is not monitored for compliance to the schedule:
The final implementation plan to use the GRS has been drafted, but not yet finalized with management review and approval.

10.2 Indicate the disposal method of the PII/BII.

Disposal
Shredding **Deleting**
Other disposal method of the PII/BII:

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.)*

Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

11.2 The factors that were used to determine the above PII confidentiality impact levels.

Factors that were used to determine the above PII confidentiality impact levels	**Explanation**
Identifiability **Quantity of PII**	**Identifiability-The data in aggregate can uniquely identify an individual.**

Data Field Sensitivity **Obligation to Protect Confidentiality**	**Quantity of PII-A large quantity of Pll regarding NIST employees, associates, and visitors.** **Data Field Sensitivity-The data is considered more sensitive in aggregate form.** **Obligation to Protect Confidentiality-Based on the data which could be within the 137-01 system, 137- 01 must protect (e.g.. via encryption) the BII/PII of each individual in accordance with the Privacy Act of 1974.**

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.)

In light of the information collected, there is a potential threat to privacy related to the inadvertent disclosure of sensitive information to persons not authorized to use or possess it. Another potential risk is that the system may collect and/or maintain more information than is necessary for official business purposes.

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

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

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

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