

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



**Privacy Threshold Analysis
for the
137-01 Emergency Services Office System**

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

Unique Project Identifier: 137-01

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

- 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 purpose that the system is designed to serve*
- e) *The way the system operates to achieve the purpose*
- f) *A general description of the type of information collected, maintained, use, or disseminated by the system*
- g) *Identify individuals who have access to information on the system*
- h) *How information in the system is retrieved by the user*
- i) *How information is transmitted to and from 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 (Boulder and 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 functions 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.**
- **Visitor Registration System interconnects with the NIST Associate Information System (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 does not interconnect with other NIST systems.**
- **Report Exec does not interconnect with other NIST systems.**

d) The purpose that the system is designed to serve

The components collectively provide the tools necessary to deliver emergency and physical security services for the protection of personnel, property, and activities on NIST facilities.

e) The way the system operates to achieve the purpose

- **The Physical Security Systems (Boulder and Gaithersburg) support physical security operations at NIST Boulder and Gaithersburg campus. 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.**

f) A general description of the type of information collected, maintained, use, or disseminated by the system

The type of information includes: identifying numbers, general personal data, work-related data, distinguishing features/biometrics, and system administration/audit data.

g) Identify individuals who have access to information on the system

Only authorized, role-based access exists given the sensitive mission nature.

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

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

i) How information is transmitted to and from the system

- Physical Security 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): The initial contact data was imported into Everbridge ENS from existing NIST data sources. Personal contact data is provided voluntarily by NIST staff via the secure ENS member portal that requires login.**
- 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.**

Questionnaire:

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:

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Activities
Other activities which may raise privacy concerns:

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the submitter has a commercial interest” and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)”

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 17-12: “The term PII refers to information that can be used to distinguish or trace an individual’s identity either alone or when combined with other information that is linked or linkable to a specific individual.”

The IT system collects, maintains, or disseminates PII about:

If the answer is “yes” to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Is a PIA Required?	Yes
--------------------	------------

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PIA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

 X I certify the criteria implied by one or more of the questions above **apply** to the 137-01 Emergency Services Office System and as a consequence of this applicability, I will perform and document a PIA for this IT system.

 I certify the criteria implied by the questions above **do not apply** to the 137-01 Emergency Services Office System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Charles Couch

Signature of SO: _____ Date: _____

Name of Information Technology Security Officer (ITSO):

K. Robert Glenn

Signature of ITSO: _____ Date: _____

Name of Privacy Act Officer (PAO):

Catherine Fletcher

Signature of PAO: _____ Date: _____

Name of Co-Authorizing Official (Co-AO):

Kevin Kimball

Signature of AO: _____ Date: _____

Name of Co-Authorizing Official (Co-AO):

Chandan Sastry

Signature of AO: _____ Date: _____

Name of Bureau Chief Privacy Officer (BCPO):

Susannah Schiller

Signature of BCPO: _____ Date: _____