Template Version Number: 01-2020

U.S. Department of Commerce
U.S. Patent and Trademark Office

Privacy Threshold Analysis
for the
Siemens Physical Access Control System (PACS)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Siemens Physical Access Control System

Unique Project Identifier: PTOC-039-00

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).

The Siemens Physical Access Control System (PACS) is an electronic security system that provides the capability to restrict and/or control physical access to USPTO facilities, equipment, and resources. This system is used by authorized security personnel to manage and monitor multiple entry points, intrusion detection, and video surveillance at the USPTO Headquarters in Alexandria Virginia and satellite offices in San Jose, California; Denver, Colorado; Dallas, Texas; and Detroit, Michigan.

The following 4 components comprise PACS:

1. CCURE9000
2. Genetec Security Center
3. Briefcam Enterprise Video Analytics
4. Commend Intercom System

a) Whether it is a general support system, major application, or other type of system

Siemens PACS is a major application system.

b) System location

The system is located at the Alexandria campus and Dallas, San Jose, Denver and Detroit satellite offices

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

PACS is a system on a private security network and connects to the USPTO Network and Security Infrastructure (NSI). PACS receives files from the HSPD-12 Personal Identity Verification System Card Management System (HSPD-12) PIVS/CMS badging system during the PIV badging process but does not have the capability to send any data to the

HSPD-12 system. It also forwards non PII badging data regarding employees on a daily basis to a middleware server for eventual use in the Corporate Administrative Office System (CAOS), the Agency's Records Sharing Platform (RSP).

- **Network and Security Infrastructure System (NSI) -** NSI is an infrastructure information system that facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO IT applications.
- **Corporate Administrative Office System (CAOS) -** an Application information system and Records Sharing Platform (RSP) which supports all activities associated with the recruitment and management of USPTO personnel.
- **Personal Identity Verification System/Card Management System (HSPD-12-PIVS/CMS)** provides the personalization and issuance of the smart card identification credentials under HSPD-12 and is used to gather biometrics (fingerprints) and other identity data (name, contact information, birth history and photo of applicant) for the issuance and life cycle management of secure credentials.

d) The purpose that the system is designed to serve

The Siemens PACS purpose is to restrict and/or control physical access to USPTO facilities, equipment and resources.

e) The way the system operates to achieve the purpose

PACS implements a private, closed network with servers located physically onsite accessed by desktop workstations. Authorized security personnel manage and monitor multiple entry points, intrusion detection, and video surveillance

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

The PII includes such information as Employee ID, Name, Date of Birth, Place of Birth, Date\Time of Access, physical characteristics, telephone number, photo ID, etc.

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

Authorized security personnel and managers

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

The user retrieves information by logging into the system and looking up data, having the monitoring portion of the system up and running which provides displays ongoing badging information or by running reports to pull data. Users can also display the video monitoring system or search for specific archived footage based on temporarily saved video monitoring footage (approximately 30-60 days).

i) How information is transmitted to and from the system

A one-way connection from HSPD-12 to Siemens PACS is used to transmit data, Siemens PACS transmits data to the RSP system using a one-way connection.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

☐ This is a new information system. *Continue to answer questions and complete certification.*

☐ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*

☐ 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 01-2020). *Continue to answer questions and complete certification.*

☐ 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 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

☐ Yes. This is a new information system.

☐ Yes. This is an existing information system for which an amended contract is needed.

☐ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

☒ No. This is not a new information system.

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.

☒ Yes. *(Check all that apply.)*

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

☐ No.

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.)."

☐ Yes, the IT system collects, maintains, or disseminates BII.

☒ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate 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."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- ☒ DOC employees
- ☒ Contractors working on behalf of DOC
- ☒ Other Federal Government personnel
- ☒ Members of the public

☐ No, this IT system does not collect any PII.

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?

☐ Yes, the IT system collects, maintains, or disseminates 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.

☒ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

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

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

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.

☐ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☒ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

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 PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ I certify the criteria implied by one or more of the questions above **apply** to the Siemens Physical Access Control System (PACS) 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 Siemens Physical Access Control System (PACS) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Joseph Burns Office: Office of Security/ OAS Security Phone: (571) 272-1537 Email: Joseph.Burns@uspto.gov Signature: Users, Burns, Joseph Digitally signed by Users, Burns, Joseph Date: 2021.07.08 13:59:51 -04'00' Date signed: _____	**Chief Information Security Officer** Name: Don Watson Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-8130 Email: Don.Watson@uspto.gov Signature: DON R Watson Digitally signed by DON R Watson Date: 2021.07.12 06:53:55 -04'00' Date signed: _____
Privacy Act Officer Name: John Heaton Office: Office of General Law (O/GL) Phone: (571) 270-7420 Email: Ricou.Heaton@upsto.gov Signature: Users, Heaton, John (Ricou) Digitally signed by Users, Heaton, John (Ricou) Date: 2021.06.28 18:00:02 -04'00' Date signed: _____	**Bureau Chief Privacy Officer and Co-Authorizing Official** Name: Henry J. Holcombe Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-9400 Email: Jamie.Holcombe@uspto.gov Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2021.07.12 15:27:47 -04'00' Date signed: _____
Co-Authorizing Official Name: Frederick Steckler Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-9600 Email: Frederick.Steckler@uspto.gov Signature: Users, Steckler, Frederick W. Digitally signed by Users, Steckler, Frederick W. Date: 2021.08.02 11:57:59 -04'00' Date signed: _____	