SYSTEM NAME AND NUMBER:

SEC-23: Visitor Badge and Employee Day Pass System

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Securities and Exchange Commission, Office of Security Services, Office of Support Operations, 100 F Street, NE, Washington, DC 20549.

SYSTEM MANAGER(S):

Branch Chief of Physical Security and Emergency Management, Office of Security Services, Office of Support Operations Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301 and Executive Order 13231 of October 16, 2001 on Critical Infrastructure Protection; Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004. Securities and Exchange Commission Administrative Regulation, Privacy Policy and Compliance, December 2017.

PURPOSE(S) OF THE SYSTEM:

This system is primarily designed as a physical and operational security system to control access to Commission facilities by visitors and representatives from other Federal agencies. It is also used to issue temporary badges for Commission staff or contractors who are not in possession of their badge and are authorized to enter SEC facilities. Records are for physical

and operational security and can only be used for purposes compatible with the purpose for which it was collected as cited in the Privacy Act of 1974, 5 U.S.C. 552(a)7.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Authorized visitors and Commission employees who access Commission facilities are covered by this system.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records may include the name, photograph; country represented the number of the printed barcode issued for each badge, visitor category, the location, date, and time of entry to the secure Commission facility. Records may include the following information from scanned driver's licenses and passports: First and last name. Further information contained within the system will be the name of the person being visited and the reason for the visit. The system may maintain check in and check out times, current status of visitor, and a barcode assigned by the system software for each visitor record.

RECORD SOURCE CATEGORIES:

Information is provided by the visitor seeking access to Commission facilities to meet with Commission employees or contractors, by Commission employees who pre-register visitors, and by Commission employees or contractors with badges, who on that occasion do not have their access badge and seek access to SEC facilities.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the Commission as a routine use pursuant to 5 U.S.C. 552 a(b)(3) as follows:

1. To appropriate agencies, entities, and persons when (1) the SEC suspects or has confirmed that there has been a breach of the system of records,· (2) the SEC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the SEC (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the SEC's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
2. To other federal, state, local, or tribal law enforcement agencies; to assist in or coordinate law enforcement activities with the SEC.
3. In any proceeding where the federal securities laws are in issue or in which the Commission, or past or present members of its staff, is a party or otherwise involved in an official capacity.
4. To any persons during the course of any inquiry, examination, or investigation conducted by the SEC's staff, or in connection with civil litigation, if the staff has reason to believe that the person to whom the record is disclosed may have further information about the matters related therein, and those matters appeared to be relevant at the time to the subject matter of the inquiry.

5. To interns, grantees, experts, contractors, and others who have been engaged by the Commission to assist in the performance of a service related to this system of records and who need access to the records for the purpose of assisting the Commission in the efficient administration of its programs, including by performing clerical, technical, or data analysis functions, or by reproduction of records by electronic or other means. Recipients of these records shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a.
6. To members of advisory committees that are created by the Commission or by Congress to render advice and recommendations to the Commission or to Congress, to be used solely in connection with their official designated functions.
7. To any person who is or has agreed to be subject to the Commission's Rules of Conduct, 17 CFR 200.735-1 to 200.735-18, and who assists in the investigation by the Commission of possible violations of the federal securities laws (as such term is defined in section 3(a)(47) of the Securities Exchange Act of 1934, 15 U.S.C. 78c(a)(47)), in the preparation or conduct of enforcement actions brought by the Commission for such violations, or otherwise in connection with the Commission's enforcement or regulatory functions under the federal securities laws.
8. To a Congressional office from the record of an individual in response to an inquiry from the Congressional office made at the request of that individual.
9. To respond to subpoenas in any litigation or other proceeding.
10. To the Office of Inspector General or the Office of Human Resources for investigative purposes.

11. Records may be used by staff of the Commission's Security Branch, the Office of Human Resources, and the Office of the Inspector General in routine reports or investigations to review access to SEC facilities and to assess compliance with established security procedures and policies.
12. To another Federal agency or Federal entity, when the SEC determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained in electronic and paper format. Electronic records are stored in computerized databases, magnetic disc, tape and/or digital media. Paper records and records on computer disc are stored in locked file rooms and/or file cabinets.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by the Individual's name, person visited, date of visit and/or barcode number (as printed in the form of a barcode on the badge).

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

These records will be maintained until they become inactive, at which time they will be retired or destroyed in accordance with the SEC's records retention schedule, as approved by the National Archives and Records Administration.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Access to SEC facilities, data centers, and information or information systems is limited to authorized personnel with official duties requiring access. SEC facilities are equipped with security cameras and 24-hour security guard service. The records are kept in limited access areas during duty hours and in locked file cabinets and/or locked offices or file rooms at all other times. Computerized records are safeguarded in a secured environment. Security protocols meet the promulgating guidance as established by the National Institute of Standards and Technology (NIST) Security Standards from Access Control to Data Encryption and Security Assessment & Authorization (SA&A).

Records are maintained in a secure, password-protected electronic system that will utilize commensurate safeguards that may include: guards, alarms, and monitored physical access points to the facility where information systems reside 24 hours per day, 7 days per week, firewalls, intrusion detection and prevention systems, and role-based access controls. Additional safeguards will vary by program. All records are protected from unauthorized access through appropriate administrative, operational, and technical safeguards. These safeguards include: restricting access to authorized personnel who have a "need to know"; using locks; and password protection identification features. Contractors and other recipients providing services to the Commission shall be required to maintain equivalent safeguards.

RECORD ACCESS PROCEDURES:

Persons wishing to obtain information on the procedures for gaining access to or contesting the contents of these records may contact the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549.

CONTESTING RECORD PROCEDURES:

See Record Access Procedures above.

NOTIFICATION PROCEDURES:

All requests to determine whether this system of records contains a record pertaining to the requesting individual may be directed to the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

This SORN was last published in full in the Federal Register at 71 FR 3907 (January 24, 2006).