SYSTEM NAME AND NUMBER:

SEC-33: General Information Technology Records

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Securities and Exchange Commission, Headquarters, 100 F Street, NE, Washington, DC 20549 and the SEC's Regional Offices.

SYSTEM MANAGER(S):

Chief Information Officer, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549-2736.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. §302, Delegation of Authority; 44 U.S.C. §3534; Federal Information Security Act (Pub. L. 104-106, section 5113); Electronic Government Act (Pub. L. 104-347, section 203); and E.O. 9397 (SSN), as amended by E.O. 13487.

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to (1) provide authentication and authorization to individuals with access to SEC-controlled information and information system networks; (2) collect, review, and maintain any logs, audit trails, or other such security data regarding the use of SEC information or information systems; and (3) to enable the Commission to detect, report, and take appropriate action against improper or unauthorized access to SEC-controlled information and information systems networks. The records will also enable the SEC to provide individuals access to certain programs and meeting attendance and, where appropriate, allow for sharing of information between individuals in the same operational

program to facilitate collaboration. SEC management personnel may use statistical data, with all personal identifiers removed or masked, for system efficiency, workload calculation, or reporting purposes.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Records are maintained on all individuals who are authorized to access SEC information or information systems; including: employees, contractors, students, interns, volunteers, affiliates, others working on behalf of the SEC, and individuals formerly in any of these positions. Records may also include individuals who voluntarily join an SEC-owned and operated web portal for collaboration purposes; individuals who request access but are denied, and/or who have had access revoked.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system of records may include: users' names; social security numbers; business telephone numbers; cellular phone numbers; pager numbers; levels of access; physical and email addresses; titles; departments; division; contractor/employee status; computer logon addresses; password hashes; user identification codes; dates and times of access; IP addresses; logs of internet activity; types of access/permissions required; failed access data; archived transaction data; historical data; and justifications for access to SEC computers, networks, or systems. For individuals who telecommute from home or a telework center, the records may contain the Internet Protocol (IP) address and telephone number at that location. For contractors, the system may contain the company name, contract number, and contract expiration date. The system may also contain details regarding: programs; databases; functions; and sites accessed and/or used, dates and times of use, information products created, received, or altered during use, and access or functionality problems reported for

technical support and resolution.

RECORD SOURCE CATEGORIES:

Information is supplied by the record subject, their supervisors, and the personnel security staff. Logs and details about access times and functions used are provided by the system.

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 foreign law enforcement agencies; securities self-regulatory organizations; and foreign financial regulatory authorities to assist in or coordinate regulatory or 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 a federal, state, local, tribal, foreign, or international agency, if necessary to obtain information relevant to the SEC's decision concerning the hiring or retention of an employee; the issuance of a security clearance; the letting of a contract; or the issuance of a license, grant, or other benefit.

5. To a federal, state, local, tribal, foreign, or international agency in response to its request for information concerning the hiring or retention of an employee; the issuance of a security clearance; the reporting of an investigation of an employee; the letting of a contract; or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

6. To produce summary descriptive statistics and analytical studies, as a data source for management information, in support of the function for which the records are collected and maintained or for related personnel management functions or manpower studies; may also be used to respond to general requests for statistical information (without personal identification of individuals) under the Freedom of Information Act.

7. 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.

8. 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, stenographic, 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.

9. To respond to subpoenas in any litigation or other proceeding.

10. 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.

11. To members of Congress, the Government Accountability Office, or others charged with monitoring the work of the Commission or conducting records management inspections.

12. To a commercial contractor in connection with benefit programs administered by the contractor on the Commission's behalf, including, but not limited to, supplemental health, dental, disability, life and other benefit programs.

13. 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:

Information may be retrieved, sorted, and/or searched by an identification number assigned by the computer, the last 2 digits of a social security number, email address, or by the name of the individual, or other employee data fields previously identified in this SORN.

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 4 (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: 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 20549-2736.

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 20549-2736.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

This SORN was last published in full in the Federal Register at 79 FR 30661 (May 28, 2014). Subsequent notices of revision can be found at the following citations:

By the Commission.

Brent J. Fields

Secretary

Date: