SYSTEM NAME AND NUMBER:

SEC-22: Continuity Support Center (CSC)

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549.

SYSTEM MANAGER(S):

Assistant Director/Business Manager, Office of Support Operations, Business Management Office, SEC Headquarters, 100F Street, NE, Washington DC 20549

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301, Executive Order 12656 (Nov. 18, 1988), Assignment of Emergency Preparedness Responsibilities; National Security Presidential Directive 51/Homeland Security Presidential Directive 20; *National Continuity Policy,* May 9, 2007.

PURPOSE(S) OF THE SYSTEM:

1. To maintain emergency contact information for current members and employees of the Commission for use in developing and maintaining emergency contingency operations plans, such as a formal continuity of operations (COOP) plan, for the Commission.

2. To provide alert and notification, determine team and task assignments, develop and maintain an emergency contact system for general emergency preparedness programs and specific situations (including threat alerts, weather related emergencies or other critical situations).

3. To activate COOP for Commission wide response to threat alerts issued by the Department of Homeland Security (DHS).

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Members and employees of the Commission and contractors.

CATEGORIES OF RECORDS IN THE SYSTEM:

Name, job title, organizational code number, work and home addresses, work and personal electronic mail addresses, work, home, and cellular telephone numbers; pager numbers and Blackberry PIN numbers.

RECORD SOURCE CATEGORIES:

Records are obtained from the Emergency Notification System and from the individual.

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 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.

6. 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.

7. 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.

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

10. To any Federal government authority for the purpose of coordinating and reviewing agency continuity of operations plans or emergency contingency plans developed for responding to Department of Homeland Security threat alerts.

11. 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.

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:

These records are retrieved by individual's names, or by the categories listed above under "Categories of Records in the System."

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:

RECORD ACCESS PROCEDURES:

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: 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.

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 68 FR 23168 (April 30, 2003).