U.S. Securities and Exchange Commission

PRIVACY IMPACT ASSESSMENT (PIA)
ELECTRONIC BLUESHEET SYSTEM (EBS)

September 15, 2006

Office of Market Surveillance
Division of Enforcement

Privacy Impact Assessment

CONTACT INFORMATION

- **Project Manager** [redacted]
  Office of Information Technology
  Office Application Software Development; Content Management
  [redacted]
- **System Owner:** [redacted]
  Office of Market Surveillance
  Division of Enforcement
  [redacted]

GENERAL SYSTEM/PROJECT INFORMATION

1. **Name of System or Collection.** Electronic Bluesheet System (EBS)
2. **Description of System or Collection.**
   The EBS issues and tracks Commission requests for, and receipt of, securities transaction information from the registered broker dealer (BD) community and securities self-regulatory organizations (SROs).

3. **What is the purpose of the system or Collection?**
   To request, track and analyze securities transaction information for investigative, regulatory oversight and market reconstruction purposes.

4. **Requested Operational Date?**
   4.1 In responding to this question refer to the date in the Life Cycle Plan of the IT Investment Plan. This will assist in establishing a timeline for a System of Records Notice, if required.

5. **System of Records Notice (SORN) number?**
   SEC-42
   5.1 Not Applicable.
   5.2 Not Applicable

6. **Is this an Exhibit 300 system/project? If yes, this PIA must be submitted to OMB**. No

7. **What specific legal authorities, arrangements, and/or agreements defined the collection of data?** Section 17 (a) of the Securities Exchange Act of 1934 and rules 17a-1, 17a-3, 17a-4 and 17a-25 thereunder.

SECTION I – Data in the System

The following questions address *Section 208 requirements at C.1.a.i and C.1.a.ii;* and define the scope of the data collected as well as the reasons for its collection as part of the system and/or technology being developed.

1. **What data is to be collected?**
   Securities transaction data. File format and descriptions attached.

2. **What are the sources of the data?**
   Data is received from BD's and/or SRO's.

3. **Why is the data being collected?**
   To request, track and analyze securities transaction information for investigative regulatory oversight and market reconstruction purposes.

4. **What technologies will be used to collect the data?**
   Bluesheet requests are submitted electronically, faxed or by U.S. Mail to the broker dealers clearing firms. Trade information is received electronically via an electronic feed and/or electronically via a secure web portal.

5. **Does a personal identifier retrieve the data?**
   Data may be sorted by any field in the record including personal identifiers.

SECTION II – Attributes of the Data (use and accuracy)

1. **Describe all uses of the data.**
   To request, track and analyze securities transaction information for investigative regulatory oversight and market reconstruction purposes.

2. **Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining).** Yes.

3. **How will the data collected from individuals or derived by the system be checked for accuracy?** The system has built in edit criteria that will ensure that the required fields are received in the format specified. If errors are found while processing the data, an email is sent to the broker submitting the data indicating what specific errors were found. No data is accepted and updated to the system that does not pass the edit checks.

SECTION III – Sharing Practices

1. **Will the data be shared with any internal or external organizations?**
   Yes. Access may be granted to persons, including State, Federal and Foreign Governmental authorities. See SECR 19-1, dated August 21, 1999 attached.

   1.1 Sections 21(a) (2) and 21(d) (1) of the Securities Exchange Act of 1934.

1.2 Yes.
1.3 Not Applicable.
1.4 Yes.

2. **How is the data transmitted or disclosed to the internal or external organization?**
   2.1 Data is transmitted by paper or CD-ROM.

3. **How is the shared data secured by external recipients?**
   3.1 See access letter attached.
   3.2 Not Applicable.

SECTION IV – Notice to Individuals to Decline/Consent Use

The following questions address *Section 208 requirements at C.1.a.v and C.1.a.vii.*

1. **Was notice provided to the individual prior to the collection of data? A notice may include a posted privacy policy, a Privacy Act notice on forms, or a System of Records Notice published in the Federal Register. If notice was not provided, explain why not.** All requests are sent to registered entities and are accompanied by a Privacy Act notice.

2. **Do individuals have the opportunity and/or right to decline to provide data?** No. Requests for this data are sent directly to registered securities broker dealers and not to individuals. Broker dealers are statutorily required to provide such information to the Commission.

3. **Do individuals have the right to consent to particular uses of the data? If so, how does the individual exercise the right?**
   No. See #2 above.

SECTION V – Access to Data (administrative and technological controls)

The following questions address *Section 208 requirement at C.1.a.vi;* and to describe administrative controls, technical safeguards and security measures.

1. **Has the retention schedule been established by the SEC Records Officer? If so, what is the retention period for the data in the system?**
   1.1 The retention periods of data/records that the SEC manages are contained in its General Records Schedule (GRS). For the particular data being created or maintained in this system/project, the GRS is the authoritative source for this information. For more information on the GRS, contact the SEC Records Officer.

2. **What are the procedures for identification and disposition of the data at the end of the retention period?** Request and/or Trade data is kept at the SEC production servers indefinitely. Trade data in particular is maintained in a data warehouse and has not been archived since 1988. Request records are kept indefinitely.

3. **Describe the privacy training provided to users either generally or specifically relevant to the program or system**? Yes, all employees and contractors are required to submit a signed non-disclosure form, background checks are conducted as well. All employees and contractors are required to attend and/or complete computer based training exercises on a quarterly basis.

4. **Will SEC Contractors have access to the system?** Yes, SEC contractors are required to complete and sign a non-disclosure form; in addition, SEC contractors only have access to test data, and do not have production passwords.

5. **Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?** Yes, Second quarter 2006

6. **Which user group(s) will have access to the system?** Enforcement OCIE and Market Regulation staff at SEC headquarters, Region and District offices. Other offices will be given authorization to access the system upon request with proper justification. User list include managers, system administrators (Enforcement; Office of Market Surveillance only), developers and staff as defined above.

7. **How is access to the data by a user determined? Are procedures documented?** The system uses roles, there is a user role that can create, update and cancel a request. The administrator role has the same access as a user role and also maintains the look up tables.

8. **How are the assignments of roles and rules verified?**
If an employee leaves the Commission, their user id and passwords are terminated. If an administrator leaves the Office of Market Surveillance their administrative role is terminated, if the user capacity still requires him/her to maintain a user role, the user is required to submit a request for access via the Request Management System (RMS).

9. **What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of the data?** All users are required to have an active Sybase userid and password. Passwords are set to expire every 90 days. Users are alerted when their password is about to expire, however if a user is not an active user of the system he/she will be required to submit a request via the RMS system to have their password re-activated.

SIGNATURE PAGE

Project Manager/Date

System Owner/Date

Endorsement

Chief Security Officer/Date

Chief Privacy Officer/Date

Approval

Chief Information Officer/Date