U.S. Securities and Exchange Commission

Electronic Data Gathering, Analysis, and Retrieval System (EDGAR)
PRIVACY IMPACT ASSESSMENT (PIA)

January 29, 2016

Office of Information Technology

Privacy Impact Assessment

Electronic Data Gathering, Analysis, and Retrieval System (EDGAR)

Publishing History

Document Publication Number	Revision	Date	Changes Made
Initial Document	Initiation	8/6/08	Document Creation
Document update	1	1/6/16	New Regulated Entities and Technology
Document update	2		
Document update	3		
Document update	4		
Document update	5		
Document update	6		

Privacy Impact Assessment

Electronic Data Gathering, Analysis, and Retrieval System (EDGAR)

General Information

1. Name of Project or System.
   Electronic Data Gathering, Analysis, and Retrieval System (EDGAR)

2. Describe the project and its purpose or function in the SEC's IT environment.
   EDGAR is the Securities and Exchange Commission's (SEC's) electronic filing system that provides an individual, company, or agent who registers with the SEC the capability to transmit legally required submissions. It automates collecting, validating, indexing, analyzing, and disseminating greater than 2 million submission documents (e.g., registration statements, reports, and other filings) received each year from over 168,000 registered entities. The system is composed of a complex and highly integrated collection of hardware, software, tools, and databases.

3. Operational Date?
   The EDGAR PIA was last completed on August 6, 2008. This PIA update reflects the new collection of information in the system, including information on new regulated entities, and changes in technology, controls and functionality. In addition, this PIA assesses the privacy risks and vulnerabilities of EDGAR's processes related to PII and other information related to individuals.

4. System of Records Notice (SORN) number?
   Documents and filings made via EDGAR may be covered by one or more of the SORNs listed below:
   - SEC-01 "Registration Statements Filed Pursuant to Provisions of the Securities Act of 1933, Securities Exchange Act of 1934, Public Utility Holding Company Act of 1935, and Investment Company Act of 1940"
   - SEC-02 "Applications for Registration or Exemption under the Investment Company Act of 1940"
   - SEC-03 "Notification of Exemption from Registration under the Securities Act of 1933"
   - SEC-04 "Beneficial Ownership, Acquisition, Tender Offer, and Solicitation Records Filed under the Securities Exchange Act of 1934"
   - SEC-05 "Ownership Reports and Insider Trading Transactions Records Filed under the Securities Exchange Act of 1934, Public Utility Holding Company Act of 1935, and Investment Company Act of 1940"
   - SEC-06 "Periodic Reports Filed under the Securities Act of 1933, Securities Exchange Act of 1934, Public Utility Holding Company Act of 1935, and Investment Company Act of 1940 and Investment Advisors Act of 1940"
   - SEC-07 "Proposed Sale of Securities Notices Filed under the Securities Act of 1933"
   - SEC-08 "Proxy Soliciting Material Filed under the Securities Exchange Act of 1934, Public Utility Holding Company Act of 1935, and Investment Company Act of 1940"
   - SEC-09 "Correspondence Files Pertaining to Registered Broker-Dealers"
   - SEC-10 "Correspondence Files Pertaining to Registered Investment Advisers"
   - SEC-11 "Correspondence Files Pertaining to Registered Investment Companies"
   - SEC-20 "Division of Corporation Finance Index for Filings on Schedule 13D and Filings under Regulations A and B"
   - SEC-49 "Broker-Dealer Records"
   - SEC-50 "Investment Adviser Records"
   - SEC-61 "Municipal Advisor Records"
   - SEC-62 "Correspondence Files Pertaining to Municipal Advisors; Municipal Advisor Logs"

5. Is this an Exhibit 300 project or system? ☐ No ☒ Yes

6. What specific legal authorities, arrangements, and/or agreements allow the collection of this information?
   15 U.S.C. 77a et seq., 78a et seq., 80a-1 et seq., 80b-1 et seq.; and rules and regulations adopted by the Commission under the Securities Act of 1933, the Securities Exchange Act of 1934, the Investment Company Act of 1940, the Investment Advisors Act of 1940 and Section 975(a) of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

Specific Questions

SECTION I - Data in the System

1. What data about individuals could be collected, generated, or retained?
   EDGAR may contain the PII of individuals associated with Regulated Entities to include: the associated person's name, date of birth, address, telephone number, Social Security number, citizenship, educational information, past and present employment history, disciplinary history, email address, the individual's role in the transaction, tax identification number, and financial information. The records may also describe the individual's relationship to a Regulated Entity, their compliance with provisions of the federal securities laws and other applicable rules, and any other relevant material business information about the individual that may be included in submission documents.

2. Does the project/system use or collect the social security number (SSN)? (This includes truncated SSNs)
   ☐ No.
   ☒ Yes. If yes, provide the function of the SSN and the legal authority to collect. Executive Order 9397, as Amended; Section 15B(a) of the Securities Exchange Act [15 U.S.C. § 78o-4(a)].

3. What are the sources of the data?
   Data sources include Regulated Entity filings to include: registration statements, periodic reports, applications for registration or exemption, and proxy statements filed pursuant to the applicable sections of the Securities Act of 1933, Securities Exchange Act of 1934, the Investment Company Act of 1940, and Investment Advisors Act of 1940. The data sources are information obtained from filers (both companies and individuals), filing agents, training agents, Transfer Agents, securities exchanges, and Broker Dealers. Third parties, usually filing agents or law firms, may file on behalf of companies or individuals when authorized by the EDGAR filers. These parties send their documents to the Commission through EDGAR. There are approximately 657 different form type variants that may be submitted to the SEC or generated by EDGAR, including 432 electronic and paper form types, 144 paper-only form types and 47 electronic-only form types. Additionally, documents generated by SEC staff such as examination reports, correspondence with the filer, and accounting reports may be uploaded into the EDGAR system.

4. Why is the data being collected?
   Filers submit documents to fulfill their obligations under the federal securities regulations.
   The SEC staff uses EDGAR to ensure that the documents provided by the companies meet disclosure requirements in that they provide investors with material information with regard to disclosure and the financial condition of the company and offerings of securities to public investors.

   In general, PII about individuals associated with Regulated Entities is used:

- To identify individuals acting as Transfer Agents, Broker Dealers, Investment Advisers, Municipal Advisors, or individuals associated with regulated entities in other capacities, for the EDGAR registration process;
- To communicate with Transfer Agents, Broker Dealers, Investment Advisers, Municipal Advisors, or individuals associated with regulated entities in other capacities, regarding their filing submissions;
- By the SEC and other enforcement agencies in any enforcement or disciplinary proceedings or complaint-related inquiries concerning Transfer Agents, Broker Dealers, Investment Advisers, Municipal Advisors, or individuals associated with regulated entities in other capacities; and
- By the SEC or SEC-regulated institutions that employ Transfer Agents, Broker Dealers, Investment Advisers, Municipal Advisors, or individuals associated with regulated entities in other capacities, for taking disciplinary actions or making employment decisions.

5. What technologies will be used to collect the data?
   EDGAR consists of multiple subsystems. Key subsystems are as follows:
   - Receipt and Acceptance (R&A)
     The R&A subsystem allow filers to access the EDGAR system via the Internet to file their submissions and related documents. After filings have been accepted, the system distributes each filing to the appropriate division and offices for review.

   - EDGARLink
     EDGARLink is an online application system that supports filers online form submissions. Filers use this subsystem to validate the various fielded data on their computers before transmitting filings to the EDGAR system.

   - EDGAR Enterprise Data Repository (EDR)
     EDR is composed of multiple databases, including Filings, Submission and Entity Database, Conseillers en Gestion et Informatique (CGI) Momentum Fee Database, Company Database, and Text Management System Data Repository. EDGAR production databases are replicated for use by downstream applications. Users of downstream applications do not have the capability to update, delete, or modify the EDGAR production databases. EDR contains all the filing, submission, and entity data collected by the subsystems; and data related to users' access and privilege rights, and user authentication.

   - EDGAR Workstation
     A web-based application utilized by SEC staff to access EDGAR from their desktop. Through an internal Workflow system, EDGAR assists the SEC Staff in performing analysis and review tasks. Non-reviewing divisions and offices can do research on submissions and receive notifications of the receipt of submissions in support of their missions. These users have read only access. Staff designated under “OFIS users” support the filing process through the EDGAR workstation.

   - Momentum Financials
     Momentum Financials, a commercial-off-the shelf product, is an accounting system that is integrated with EDGAR as the Fee Subsystem in processing fees for fee-bearing submissions.

<u>SECTION II - Attributes of the Data (use and accuracy)</u>

1. Describe the uses of the data.

SEC staff uses the data to: (1) perform analysis and review of disclosure documents submitted to the SEC; (2) investigate and research submissions; (3) disseminate data, including under the Freedom of Information Act (FOIA); (4) create reports; and (5) perform workflow management. Externally, EDGAR filing data is disseminated to the public on the SEC.gov website and provides the public an accurate, complete and fast method of obtaining all accepted and valid EDGAR filings. EDGAR Data is also transferred to the EDGAR Public Dissemination Service (PDS). This privatized PDS System is the primary source to receive a dedicated feed of all public EDGAR filings. Subscribers to the PDS System are required to enter into a paid Subscription Agreement to access this service.

2. Does the system analyze data to assist users in identifying previously unknown areas of note, concern or pattern? ☒ No ☐ Yes If yes, please explain.

3. How is the data collected from individuals or derived by the system checked for accuracy?
Individuals submitting filing in the EDGAR System are responsible for submitting accurate information. The system allows electronic filers to transmit their submissions in test mode before they commit to a live version to provide iterative error analysis and feedback. Because the individual, or their designated third party, provides the information about him or herself directly, the likelihood of erroneous PII is greatly reduced. EDGAR has internal application business rules and syntactic processing in place to verify all transmissions into EDGAR.

SECTION III - Sharing Practices

1. Will the data be shared with any internal organizations?
☐ No ☒ Yes If yes, please list organization(s):
EDGAR is an enterprise system. Internally, each division or office may share non-public information, in the form of reports or through access to the system, with authorized agency users who demonstrate a bona fide need to know the information. All SEC divisions and offices may use EDGAR data, but the Division of Investment Management (IM), Division of Corporation Finance (CF), Division of Trading and Markets (TM), Division of Economic and Risk Analysis (DERA), Division of Enforcement (ENF) and Office of Compliance Inspections and Examinations (OCIE) are the primary users.

2. Will the data be shared with any external organizations?
☐ No ☒ Yes If yes, please list organizations(s):
Data that should be made publicly available is disseminated to the public and to subscribers via the SEC website and the Public Dissemination System (PDS). Additionally, some data is shared with Financial Industry Regulatory Authority (FINRA) and to other external entities that are consistent with the routine uses stated in the various SEC SORNs for EDGAR data.

How is the data transmitted or disclosed to external organization(s)?
The data is transmitted electronically to the SEC's public site through the SEC's network, and to disseminators and FINRA through the Internet and secured network connections. Data may also be transmitted via a secured encrypted manner, including encrypted email and encrypted File Transfer Protocol.

3. How is the shared data secured by external recipients?
Any information shared with organizations outside the SEC is required to be appropriately secured per Office of Management and Budget Memorandums 06-15, Safeguarding Personally Identifiable

Information, and 06-16, Protection of Sensitive Agency Information. Each subscriber determines their own internal procedures for securing the data.

4. Does the project/system process or access PII in any other SEC system?
   ☐ No
   ☒ Yes. If yes, list system(s).
   (1) Momentum, (2) Public Dissemination System, (3) SEC.Gov, (4) Company Business Database, (5) SECProd0, (6) Active Directory, (7) Enterprise Data Warehouse

SECTION IV - Notice to Individuals to Decline/Consent Use

1. What privacy notice was provided to the different individuals prior to collection of data? (Check all that apply)
   ☒ Privacy Act Statement ☒ System of Records Notice ☒ Privacy Impact Assessment
   ☒ Web Privacy Policy ☐ Notice was not provided to individuals prior to collection

2. Do individuals have the opportunity and/or right to decline to provide data?
   ☒ Yes ☐ No ☐ N/A
   Please explain: Information is obtained from individuals pursuant to the requirements of federal securities laws. To fulfill those requirements, filers must submit certain data on individuals and as such, it is not optional. Information on individuals is collected only where the SEC has specific legal authority to do so in order to administer its responsibilities under the federal securities laws. When personal information from individuals is collected they are advised of the agency's legal authority for requesting the information, the purposes for which the information will be used and disclosed, and the consequences of their not providing any or all of the requested information.

3. Do individuals have the right to consent to particular uses of the data?
   ☐ Yes ☒ No ☐ N/A
   Please explain: Individuals are advised that the SEC will disclose their information without their prior written consent only when the SEC has specific legal authority to do so and pursuant to a routine use described in a SORN.

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

1. Has the retention schedule been established by the National Archives and Records Administration (NARA)?
   ☐ No If no, please explain:
   ☒ Yes If yes, list retention period: The retention schedule is commensurate with the System of Records Notice applicable to the filing type as delineated in the SEC Program Records List (for SEC-specific records), and the General Records Schedule prescribed by the National Archives and Records Administration (NARA).

2. What are the procedures for identification and disposition of the data at the end of the retention period?
   The procedures for identification and disposition of the data at the end of the retention period are commensurate with the System of Records Notice applicable to the filing type as delineated in the SEC Program Records List (for SEC-specific records), and the General Records Schedule prescribed by the National Archives and Records Administration (NARA).

The SEC Records Schedules and NARA General Records Schedule provide mandatory instructions (disposition instructions) to all NARA staff regarding how to maintain the Commission's operational records and what to do with them when they are no longer needed for current business. The disposition instructions state whether individual series of records are permanent or temporary, as well as how long to retain the records. Records with historical value, identified as permanent, are transferred to the National Archives of the United States. All other records are identified as temporary and are eventually destroyed in accordance with the Records Schedule.

3. Describe the privacy training provided to users, either generally or specifically relevant to the program or system?
   The Privacy Office thru General Privacy Awareness Training, which all SEC employees and contractors must complete yearly, provides training. The training outlines their roles and responsibilities for properly handling and protecting PII. EDGAR Filer Technical Support team also provides training on the EDGAR functionality.

4. Has a system security plan been completed for the information system(s) supporting the project?
   ☒ Yes If yes, please provide date SA&A was completed: August 2015
   ☐ No If the project does not trigger the SA&A requirement, state that along with an explanation

5. Is the system exposed to the Internet without going through VPN?
   ☐ No
   ☒ Yes If yes, Is secure authentication required? ☐No ☒Yes; and
   Is the session encrypted? ☐ No ☒Yes

6. Are there regular (i.e. periodic, recurring, etc.) PII data extractions from the system?
   ☒ No
   ☐ Yes If yes, please explain:

7. Which user group(s) will have access to the system?
   The user groups for EDGAR are:
   - Filers - An individual, company, or agent who files their legally required submission documents with the SEC;
   - Subscribers - Entities that receive all accepted, live and public information in EDGAR via a paid subscription to a real-time feed from the SEC's public dissemination service;
   - Public - Viewers of company submissions to make investment decisions with timely information via SEC.gov;
   - SEC Staff - (1) perform analysis and review; (2) research submissions (3) upload documents (exam reports, correspondence, accounting reports) (4) disseminate data (FOIA) (4) create reports (5) workflow management (primary user staff designated under OFIS, as well as staff in Divisions of Corporation Finance and Investment Management). Staff users see only the data assigned to them or their user group;
   - Managers - Access data assigned to their staff members, themselves, and their user groups; and
   - System administrators - View any information available in the database for administration purposes.

8. How is access to the data by a user determined?

Filers typically gain access when the filer submits the automated Form ID online to create a company profile within EDGAR. The EDGAR Filer Manual provides instructions to filers on the use and functionality of the system. SEC "OFIS Users" create company profiles in EDGAR for paper-only filers. SEC staff, division and offices control user access. Data access is restricted based on the principles of least privilege and separation of duties; access by staff is granted on a need-to-know basis. The EDGAR User Manual provides instructions to SEC users on the use and functionality of the system. Divisions and offices establish and document additional procedures for their specific use of the data.

Are procedures documented? ☒ Yes ☐ No

9. How are the actual assignments of roles and rules verified?
   The various SEC divisions and offices own the procedures and control user access within their respective organizations.

10. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data?
    Controls are audited regularly to prevent misuse of data, i.e., application-level controls, physical controls, database-level controls, network-level controls. EDGAR data is replicated in an alternate database that is used by the public via the public Web site; and SEC staff that do not require access to the original data. Data is made available for use by downstream applications and their users via the alternate database, to protect the original data from the impact of other applications and their processes.

SECTION VI - Privacy Analysis

Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

Privacy risks:
Risk of unauthorized or inadvertent disclosure of non-public data, unauthorized access.
To mitigate these risks, numerous system-based controls are in place to protect the data collected. The system uses role-based security to control access to data within the system. These roles are based on position descriptions and appropriate levels of access are granted based on the type of work the individual performs. Additionally, replicated data is used in downstream applications to carry out functions of the users of those applications. The general public, subscribers, and SEC staff not requiring access to modify data can view data in read-only view.

Risk to data accuracy and integrity.
Mitigation: Data is collected to the extent possible directly from filers.

A privacy risk was identified as it relates to registrants who are required or may inadvertently provide personal information in public filings that could possibly lead to identity theft. In order to mitigate possible risks various rules were amended to include language requesting that filers not submit such information when not required. Internal technological controls are also in place to assist in the identification of such risks in filings received and posted to the SEC website.