U.S. Securities and Exchange Commission

Easy Lobby
PRIVACY IMPACT ASSESSMENT (PIA)

September 30, 2013

Privacy Impact Assessment
Easy Lobby v. 10.0.8

General Information

1. Name of Project or System.
   Easy Lobby v10.0.8 Upgrade: Administrator and SVM applications

2. Describe the project and its purpose or function in the SEC's IT environment.
   EasyLobby is an OSO / Physical Security Operations Branch managed visitor tracking system used to track and monitor visitor's to SEC facilities. This system will collect, manage and store employee and visitor PII data. This upgrade is being implemented to bring the Administrator and SVM applications to the current version.

3. Requested Operational Date? This system is currently operational. The last PIA completed on this system was 11/14/2011. This PIA documents the privacy risks and vulnerabilities of the data collected.

4. System of Records Notice (SORN) number? SEC-52, Visitor badge and Employee Day Pass System

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? 5 U.S.C. 301, Executive Order 13231, and Homeland Security Presidentail Directive-12(HSPD-12)

Specific Questions

SECTION I - Data in the System

1. What data about individuals could be collected, generated, or retained?
   The visitor's name and employment information is collected so that the security guard can verify the visitor's identity. The visitor's photo is taken and printed on the visitor badge which must be displayed at all times while on SEC property. The visitor's signature is collected as legal proof the visitor understands his/her precise behavioral obligations while on SEC property. For employees and contractors at the SEC, a limited set of data is collected to allow users to pre-register visitors. The data collected includes: First Name, Last Name, Active Directory User ID, Title, Phone Number, Department, Category (Contractor or Staff) and Email Address.

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.
3. What are the sources of the data?
   The sources of the visitor data will be government approved identification, business cards or personal statements and the visual verification by the security guards. The original source of the employee and contractor data in EasyLobby was an extract of data from Active Directory. Any new employees or contractors are added manually upon request, with the data

being looked up in the Global Address List (GAL). The GAL is the address book in Outlook that comes from Active Directory.

4. Why is the data being collected?
   The visitor's name and employment information is collected so that the security guard can verify the visitor's identity. The visitor's photo is taken and printed on the visitor badge which must be displayed at all times while on SEC property. The visitor's signature is collected as legal proof the visitor understand his/her precise behavioral obligations while on SEC property. Employee and contractor data is being collected in order to validate that the user is permitted to pre-register visitors.

5. What technologies will be used to collect the data?
   EasyLobby software and hardware peripherals and database will be used to capture and maintain this data.

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

1. Describe the uses of the data.
   The visitor's name and photo will be used for identification and verification of the visitor. The visitor's employment information will be used to verify the individual's reason for access. The visitor's signature will be used as legal acknowledgment of the visitor's rights within the SEC facility. Employee and Contractor data is used to validate that the user is permitted to pre-register visitors.

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: The visitor's name and photo will be used for identification and verification of the visitor. The visitor's employment information will be used to verify the individual's reason for access. The visitor's signature will be used as a legal acknowledgment of the visitor's rights within the SEC facility.

3. How will the data collected from individuals or derived by the system be checked for accuracy?
   At the point of badge issuance, the security guard will verify all information and correct inaccuracies.

SECTION III - Sharing Practices

1. Will the data be shared with any internal organizations?
   ☐ No ☒ Yes If yes, please list organization(s): Data will be shared only under the routine uses in OSO as described in the SORN. The data collected will be stored in the Easy Lobby database and will be retrievable only at each of the designated Easy Lobby workstations and the database server. Users in OIT management and the Physical Security Team in OSO, as well as the OSO Security Guard Staff.
2. Will the data be shared with any external organizations?
   ☒ No ☐ Yes If yes, please list organizations(s): How is the data transmitted or disclosed to external organization(s)?

3. How is the shared data secured by external recipients?

NA

4. Does the project/system process or access PII in any other SEC system?
   ☐ No
   ☒ Yes. If yes, list system(s).
   The systems shares information with Active Directory. Employee and contractor data is manually entered based on information in the Global Address List, which can be viewed in AD.

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: Visitors to SEC facilities voluntarily provide information. Visitors who chose not to provide information may be denied access to the facilities. Information is solely collected for purposes compatible with the purposes in the SORN. .

3. Do individuals have the right to consent to particular uses of the data?
   ☐ Yes ☒ No ☐ N/A
   Please explain: See number 2 above

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: These records will be maintained for a period of 2 years, at which time they will be retired or destroyed in accordance with records schedules of the United States Securities and Exchange Commission as approved by the National Archives and Records Administration.

2. Describe the privacy training provided to users, either generally or specifically relevant to the program or system?
   Each SEC Security Guard with access to EasyLobby will have completed the required SEC Privacy Awareness Training. Additionally the standard security guard training includes a module on protection of individual privacy in the performance of all security guard duties. Each SEC employee and contractor with access to EasyLobby (eAdvance) will have completed the required SEC Privacy Awareness Training.
3. Has a system security plan been completed for the information system(s) supporting the project?
   ☒ Yes If yes, please provide date C&A was completed: 07/22/2011
   ☐ No If the project does not trigger the C&A requirement, state that along with an explanation

4. 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

5. Are there regular (ie. periodic, recurring, etc.) PII data extractions from the system?
   ☐ No
   ☒ Yes If yes, please explain: Badges are printed for visitors to access SEC facilities.

6. Which user group(s) will have access to the system?
   The Secured Visitor Management (SVM) application will be used by the SEC Guard Staff. Approximately 60 guards will be assigned the Operator role. The Operator role allows the user to check-in and check-out visitors. Guards access the system using a "locked down" workstation with limited functionality and no access to the SEC production network or the Internet. These guard workstations operate on a Virtual Local Area Network (VLAN) segregated via the EasyLobby server from the SEC Intranet and the Internet.

   The Administrator application has specific users within OIT management and the Physical Security team. Approximately 10 users will be assigned the Enterprise Administrator role. The Enterprise Administrator role allows the user complete access to the application. The centralized database and network access also allows OAS Security Branch to analyze and report on visitor data.

   The eAdvance application can be used by all SEC staff and authorized contractors to pre-register guests and receive an email notification when the visitor checks in with the guard staff.

7. How is access to the data by a user determined? OSO determines the users access. The end users with 'Admin' privileges can add/delete and alter user accounts as needed.
   Are procedures documented? ☐ Yes ☒ No

8. How are the actual assignments of roles and rules verified.
   End users and their roles are reviewed for accuracy on a yearly basis by both the customer(physical security) and the OIT Security team.

9. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data? Easy Lobby provides audit logging, to include the check-in and check-out data of all visitors. The system does not audit the veiwing and/or changing of a visitor record. Only SVM and Administrators have access to this information and no one else.

SECTION VI - Privacy Analysis

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

Due to the content and nature of the information being processed, unauthorized disclosure of certain personal identity information or unauthorized access to the badge issuance capability has the potential to result in a serious effect on agency operations. The following controls mitigate the identified risks:

a. Authorized users are limited to the security guard staff located at Station Place and the Operations Center. All users who have access to the data have had background checks, signed non-disclosure agreements and will have attended Privacy Awareness Training prior to using EasyLobby 10.0.4.
b. The SVM application is installed only on security guards' workstations therefore access of data is minimized to authorized personnel.
c. The Administrator application is only installed on 8 user's workstations therefore access of data is minimized to authorized personnel.
d. The server hosting the database is physically secured within SEC facilities.
e. From a network standpoint, the server is behind SEC firewalls and is not configured to be accessed from outside the SEC network.
f. Database access is restricted using standard SEC security policies and is limited to database administrators.