Federal Trade Commission
Privacy Impact Assessment

Financial Disclosure Online (FDonline)

December 2018

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission (FTC) is committed to preserving the public's trust by adhering to the various laws and ethics regulations that guide the performance of each FTC employee's official duties. The Ethics Team within the FTC Office of General Counsel (OGC) is responsible for helping agency employees maintain these high standards of ethical behavior. They are responsible for ensuring that FTC staff receive the appropriate ethics training and disclose any potential conflicts of interest to their supervisors and to the Ethics Team. Ensuring that FTC employees perform their duties while adhering to the agency's strong guidelines and principles is an important part of the FTC's mission of protecting consumers. Failure to do so may result in costly ethics violation fines, loss of public trust, and irreparable damage to the agency's reputation.

The Ethics Team utilizes the Financial Disclosure Online (FDonline) system so that FTC employees (including new hires before they are officially employed, if required by the Ethics Team) can file and FTC designated reviewing officials and the Ethics Team can review their confidential disclosure reports electronically, as well as for the Ethics Team to track and manage the annual financial disclosure process. Previously, the Ethics Team manually processed hardcopy reports, a cumbersome and time-consuming process. Converting to a centralized, e-tracking system not only improves efficiencies and decreases inaccuracies but also permits the Ethics Team's limited resources to be redirected to other duties, including conflicts review, educational outreach, etc. FDonline's automation function also helps the Ethics Team respond in a timely manner (as required by law) to personnel actions that trigger federal ethics requirements.

FDonline is owned and operated by HRworx, a commercial third party entity which the FTC has contracted with for use of the FDonline system. FDonline is hosted on the Amazon Web Services (AWS) GovCloud.[1]

FDonline's primary function is to automate the confidential financial disclosure process:

- **FDonline facilitates the electronic filing, review, and certification of the confidential financial disclosure report (OGE Form 450)**. The OGE Form 450 is an OGE-owned document used throughout the Executive Branch. All FTC employees at the GS-14 and GS-15 levels are required to complete the OGE Form 450. In certain cases, with consultation from the Ethics Team, managers may designate employees at lower grade levels to file the OGE Form 450 based on the nature of their official duties. FDonline saves the information provided in the form each year so employees are only required to update information as appropriate. Only the certified, final version of the report is retained by FDonline. FDonline automatically notifies employees of the filing deadline and issues reminders via email as the target date approaches. These automatic notifications include a link to a

[1] AWS GovCloud (US) is designed to allow U.S. government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements.

program that walks employees through the entire filing process, ensuring both the accuracy and timely submission of reports. (The notifications do not contain any sensitive PII in case they are misdirected or forwarded.)

- **FDonline automates the management of certified OGE Form 450 reports.** For example, FDonline helps the Ethics Team maintain an accurate record of when and which employees have submitted their reports, as well as whether the reports have been reviewed and certified in a timely manner by reviewing officials. FDonline also ensures the reports are securely stored in a central repository. Specifically, access is limited to the filer, the reviewing officials (i.e., FTC supervisors), and the Ethics Team. The Ethics Team may also disclose OGE Form 450 reports to other authorized FTC employees as appropriate (e.g., in connection with FTC personnel or Inspector General matters). The U.S. Office of Government Ethics (OGE) periodically inspects/audits the ethics programs of federal agencies, including the FTC's ethics program. Accordingly, the FTC may share information contained in FDonline with OGE.

The secondary purpose of FDonline is to automate other aspects of the FTC's federal ethics program:

- **FDonline automates the tracking of ethics training.** All new FTC employees must receive initial ethics orientation. FTC employees at the GS-14 and GS-15 levels must receive one hour of live federal ethics training every three years and one hour of paper/electronic training during the interim years. FTC managers have designated certain FTC employees at lower GS levels to meet the same annual ethics training requirements as GS-14 and GS-15 employees. Senior staff, including political appointees and career members of the Senior Executive Service, must receive one hour of live federal ethics training every year. FDonline automates the process of tracking this information by individual employee (*e.g.*, by sending training notifications and reminders to employees, logging employee attendance, etc.).

- **FDonline automates other employee requests for ethics guidance and approval.** The system may be used to submit, approve, and log requests for outside employment, free attendance to widely-attended gatherings, and non-federal source travel reimbursement. For example, the FDonline may also be used to log and store the FTC's Ethics K-9 Korner Consent and Release Form (used when employees submit photos of their pets for use in the agency's ethics educational campaigns). FDonline also may be used to store final guidance provided to employees on a variety of ethics subjects (regardless of whether the final guidance is captured in an email or formal legal memorandum).

In order for FTC employees to use FDonline, the Ethics Team must first create an account for the employee by setting up a filing (with a set of designated forms to be completed). The employee can log in using a username and password along with a one-time code (second authentication factor) sent to the user's e-mail address. The employee then proceeds to fill out the designated forms through a series of question and answer prompts and certifies that

the information provided is accurate. Once the employee has made this certification, they are not able to make any further updates or changes to their forms unless the Ethics administrator reopens the filing and allows them to edit the information provided. The filing may be reviewed by the employee's supervisor, as necessary, then approved and recertified by the Ethics administrator.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

Ethics in Government Act of 1978, 5 U.S.C. app.; Ethics Reform Act of 1989, Pub. L. 101-194; 5 CFR parts 735 & 2634, and other applicable ethics-related laws, rules, and Executive Orders.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[2] may be collected or maintained in the system/project. Check all that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.

☒ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☐ Date of Birth	☐ Audio Recordings	☐ Internet Cookie Containing PII
☐ Home Address	☐ Photographic Identifiers (e.g., image, x-ray, video)	☒ Employment Status, History, or Information
☒ Phone Number(s)	☐ Certificates (e.g., birth, death, marriage, etc.)	☐ Employee Identification Number (EIN)
☐ Place of Birth	☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☒ Salary
☐ Age	☐ Vehicle Identifiers (e.g., license plates)	☐ Military Status/Records/ ID Number
☐ Race/ethnicity	☒ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☐ IP/MAC Address
☐ Alias	☐ Geolocation Information	☐ Investigation Report or Database
☐ Sex	☐ Passport Number	☐ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address (FTC)		☒ Other *(Please Specify)*: information pertaining to employee's spouse and dependent children
☒ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

FDonline maintains the following types of PII collected via the OGE Form 450: the filing employee's name (last, first, and middle initial); FTC email address; FTC position/title; GS-level; agency name; business address; and work phone number. Financial information

[2] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

maintained in FDonline includes only a listing of assets (e.g., names of securities or mutual funds held) and financial reports. Specific account numbers, account values, PINs, or credit reports are not included.

Additional PII maintained in the system by the FTC Ethics Team includes: employee name, employee office/organization code, GS-level, and potentially the name of an employee's pet (for FTC's K-9 Korner photo consent form). The signatures of the filing employee and the initial reviewer and/or the final reviewing official are also included in FDonline.

FDonline maintains system security log information which includes the user name and the action performed. Session dates and times are not currently logged.

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

The information collected by FDonline with respect to the OGE Form 450 report includes: the date the report was submitted; the date the report was certified by the initial reviewer and/or the final reviewing official (reviewing officials include FTC supervisors and/or Ethics Team members); reportable assets or sources of income for the filing employee, his/her spouse, and dependent children; reportable liabilities (debts) for the filing employee, his/her spouse, and dependent children; reportable outside employment positions for the filing employee; reportable agreements or arrangements for the filing employee (*e.g.*, continued participation in a retirement plan with a former employer); and, reportable gifts or travel reimbursements for the employee, his/her spouse, and dependent children.

The information collected by FDonline with respect to other aspects of the FTC's ethics program includes: date of employee request; date of approval/response by the Ethics Team; a description of the outside employment activity (including identity of employer and compensation information); a description of the widely attended gathering (including, identification of the sponsor and the individual who extended the offer of free attendance); a description of non-federal source travel information (including, identification of the sponsor and monetary details about what has been offered to the FTC employee); facts conveyed to the Ethics Team by the employee in order to obtain legal guidance; and legal guidance issued by Ethics Team to the employee.

2.3 What is the purpose for collection of the information listed above?

The OGE Form 450 is owned by OGE and certain federal employees are required by law to provide the information collected therein. Information from the form is maintained in FDonline and used for review by the FTC Ethics Team to determine compliance with applicable government conflict of interest laws and regulations. Using records identifiable by employee is necessary to provide guidance on an individual basis and to ensure consistency with guidance issued by the Ethics Team.

2.4 What are the sources of the information in the system/project? How is the information collected?

Source of Data	*Type of Data Provided & How It Is Collected*
FTC Employees (OGE Form 450 filers)	FTC employees required to complete the OGE Form 450 will access FDonline through a web application and enter their information into the system. They are required to proceed through a question and answer form that, when completed, renders the completed Form 450.
FTC Employees (Managers/Supervisors)	FTC employees who serve as reviewing officials of OGE Form 450 reports will also access FDonline via the web application and enter information into the system as necessary (such review is required to certify the reports).
FTC Employees (Ethics Team)	The FTC's Ethics Team also accesses FDonline (concerning the OGE Form 450 and otherwise as discussed above) to review and certify completed forms. This may include providing additional information about the employee or correcting inaccurate information provided by the filing employee.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
FTC Employees	GS-14 and GS-15 level employees have access to FDonline to draft and submit their OGE Form 450 reports. Reviewing officials (i.e., designated supervisors and the FTC's Ethics Team) have access to the reports in order to ensure they are timely submitted, complete, and to address potential conflicts of interest. FTC supervisors will only have access to the OGE Forms they are required to review and certify; supervisors have the ability to see all information entered by their employees. This is important because supervisors familiar with the specific work/projects assigned to their subordinates are key to spotting potential conflicts and ensuring they do not lead to actual conflicts. The FTC's Ethics Team will have access to all information in FDonline, which includes reports generated by the system that includes employee PII. Other FTC employees may access FDonline to complete other forms (*e.g.*, OGE Form 450-A) as appropriate.
U.S. Office of Government Ethics (OGE)	OGE staff cannot directly access FDonline to review FTC information, nor does the FTC directly share forms in FDonline with OGE. However, OGE periodically audits/inspects federal agencies, including the FTC, and OGE staff may request to review the information contained in FDonline for auditing purposes. The FTC Ethics Team may produce reports to provide to OGE as part of its compliance activities.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
HRworx	HRworx manages and supports FDonline. HRworx uses a role-based approach for FDonline management activities; only those authorized to access the information and have valid credentials can review FTC data in the system. Access to FDonline and the PII fields contained within is limited to HRworx personnel with an Application, Infrastructure, or Security Administrator role supporting the FDonline system. Application administrators have access to the system to perform support and technical support functions. Infrastructure administrators have access to the data in order to perform maintenance to the system. Security administrators have access to the system to monitor and investigate any security related issues.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

HRworx manages and supports FDonline. HRworx uses a role-based approach for FDonline management activities. HRworx employees are required to undergo security awareness training at the time of hire and annually after that. This is further supplemented with role-based and targeted training covering such topics as privacy and phishing. System security logs capture all actions.

HRworx does not currently have any subcontractors supporting FDonline. If, in the future, HRworx opts to allow subcontractors access to data in FDonline, they will be subject to the same training requirements as all HRworx employees. The FDonline system does not provide PII to any third-party organizations.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

HRworx's incident response plan is communicated to employees as part of its training curriculum. All employees are responsible for recognizing and reporting suspicious events and circumstances (particularly those involving government PII) to the security team. As part of its analysis, HRworx must determine the type and severity of the incident and communicate any potential risks to the customer (FTC) security/privacy officials as necessary.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

☒ Notice is provided via (*check all that apply*):

☒ Privacy Act Statement (☒ Written ☐ Oral)

☐ FTC Website Privacy Policy

☐ Privacy Notice (e.g., on Social Media platforms)

☒ Login banner

☒ Other (*explain*): A Privacy Act Statement is included on the OGE Form 450 as it appears within the FDonline system. Additionally, an explanation of the requirement to file the OGE Form 450 report is provided in writing by the FTC Human Capital Management Office (HCMO) during the hiring process. OGE Form 450 and FTC Form 474 (outside employment approval) filing requirements are also discussed orally during ethics orientation (mandatory for all new hires) and during annual ethics training (required for a subset of FTC employees). All standardized forms used by the FTC's Ethics Team contain a written Privacy Act Statement. Specifically, written Privacy Act Statements are found on: OGE Form 450 report; FTC Form 474; the Initial Ethics Orientation web-based confirmation portal (each new hire must personally confirm he/she attended ethics orientation), and the Ethics K-9 Korner Consent and Release Form (used when employees submit photos of their pets for future use in ethics educational campaigns).

☒ Notice is not provided (explain): Additional information entered into FDonline by the Ethics Team may be derived from informal email exchanges between FTC employees and the FTC's Ethics Team (those internal messages do not contain Privacy Act Statements).

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

FTC employees at the GS-14 and GS-15 levels are legally mandated to complete the OGE Form 450. Likewise, employees who engage in certain outside activities[3], are legally required to obtain approval from their supervisors and the FTC's Ethics Team. As such, FTC employees must provide their information for use in FDonline to meet financial disclosure requirements. An employee who willfully falsifies the information on his or her report, willfully omits information, or willfully fails to file may be subject to civil penalties and/or criminal prosecution. FTC disciplinary actions may also be imposed if the employee does not fully respond or cooperate with the Ethics Team in attempting to certify the employee's filing.

All new hires must attend ethics orientation and a subset of employees have been designated (by law and/or FTC policy) for annual ethics training. This is mandatory and a condition of their employment with the FTC. Employees are legally required to obtain advance approval of non-federal-source reimbursement and free attendance to widely attended gatherings from

[3] All FTC employees are required to obtain approval from their supervisor and the FTC Ethics Team prior to engaging in certain non-FTC related activities. This includes any compensated activity outside of the FTC; any service as officer/director/trustee (regardless of compensation); any personal service to a for-profit entity; and any provision of a professional service (operating in the same field of work that the employee engages in at the FTC). All these outside activities are subject to FTC approval.

the FTC's Ethics Team. In contrast, employees normally otherwise have the option to contact the Ethics Team for legal guidance (such contact is encouraged by the Ethics Team to avoid inadvertent violations).

Employees do have the option to decline to provide their information for use by the Ethics Team in certain FTC ethics educational awareness initiatives involving voluntary employee participation. For example, employees may choose whether or not to submit photos of their pets for use in FTC's K-9 Korner activities; this is strictly voluntary and at the discretion of the FTC employee.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

FTC employees will access the FDOnline system to file and view their own OGE Form 450 reports. FTC employees may also contact the FTC's Ethics Team to access or update other information about themselves.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

Employees who submit the OGE Form 450 are required to update their report on an annual basis. Once the filing has been digitally signed or "certified," the filing employee can no longer make additional changes or updates to their form. Individual filers can contact the FTC Ethics Team to request access to their records and reopen a filing if anything needs to be updated. After a filing has been reopened, the employee can log in with his/her credentials and make any corrections/updates. With respect to other employee information in the system, FTC employees may contact an FTC Ethics Team member and request that his/her information be updated/corrected. The FTC Ethics Team will update the information.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

Filers of the OGE Form 450 report are responsible for entering accurate information into FDonline. The FTC's Ethics Team conducts an in-depth review of the contents of a subset of OGE Form 450 reports each year. All OGE Form 450 reports are reviewed by a supervisor or an FTC Ethics Team member for accuracy and completion. All requests for outside employment approval (FTC Form 474) are reviewed by supervisors and an FTC ethics attorney. All other information in FDonline is entered into the system by the FTC's Ethics Team. There are various safeguards in place to ensure accuracy. For instance, only final legal guidance/documents that have undergone the appropriate review within the Ethics Team are entered into the system. Likewise, attendance data for annual ethics training and

ethics orientation for new hires is cross-checked with lists generated by FTC Human Capital Management Office (HCMO).

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

Only authorized FTC Ethics Team administrators have access to all the information in FDonline. FTC system administrators and employees will login to the system using their user name, password, and one-time code (second authentication factor) sent to the user's e-mail address. FDonline automatically locks the user out of his/her account after three failed password attempts. They will then be instructed to reset their password via a link sent to their email. The system also logs user activity and notes when an authorized made changes to a specific filing. Filing employees only have access to their own accounts and forms. Supervisors reviewing an employee's filing have access to only their designated employee's information. Once reports are finalized, they may not be altered or changed.

Access to FDonline and the PII fields contained within the system are limited to HRworx personnel with an Application, Infrastructure, or Security Administrator role supporting the FDonline system. Individuals are only granted access to functionality necessary to accomplish assigned tasks and responsibilities, such as application support and system administration. Access and authorization requests are documented, authorized and approved by the individual's manager and the HRworx Security Officer prior to account creation.

HRworx individuals are provided access to the FDonline system in accordance with established account provisioning and management processes. These individuals login to the system using a two-factor authentication process. Additionally, HRworx provides security awareness training to all employees and displays a warning banner each time an individual logs onto the system, describing that unauthorized or improper use may result in disciplinary action and civil and criminal penalties.

The HRworx Security Officer also maintains the role of Privacy Officer and is responsible for assuring safeguards for the PII within FDonline. The Security Officer has the responsibility of performing a security impact analysis for significant changes to the system and also provides guidance to other FDonline support personnel on the proper protection of sensitive information, through established policies and procedures. FDonline stores all data in an encrypted MySQL database and allows access to the database via the application (which has its own authentication) or an Intelliworx/HRworx infrastructure administrator. System users access the system via an HTTPS connection.

FDonline operates within and leverages the AWS GovCloud Infrastructure as a Services (IaaS) environment. HRworx uitilizes the AWS GovCloud IaaS multiple availability zone functionality as the alternate processing site for the FDonline system. Both primary and secondary availability zones are within the FDonline system FedRAMP authorization boundary where the same controls are implemented and assessed.

5.3 Has the system/project undergone the appropriate security risk assessment and received authority to operate?

Yes, FDonline has undergone a security risk assessment and received an authority to operate. The system is categorized as a moderate system using Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

5.4 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

☒ Not Applicable

No live PII or production data are used for testing or any other purposes.

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

The information contained in FDonline will be disposed of in accordance with NARA GRS 2.8 (Employee Ethics Records).

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

Authorized FTC employees access FDonline via a web application that uses temporary session cookies. Use of the temporary session cookie is necessary to move the user continuously through the system without requiring them to reenter their credentials at each step.

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Risk	*Mitigation Strategy*
Information contained in system/project may be inaccurate or incomplete.	The FTC's Ethics Team is able to review data in FDonline and correct errors. The FTC's Ethics Team will perform quality monitoring periodically and can identify, review, correct, and log inaccuracies to prevent recurrence (*e.g.*, although all OGE Form 450 reports are tracked, logged, and reviewed by a supervisor, a subset of OGE Form 450 reports are also carefully reviewed by the FTC's Ethics Team each year for accuracy).
Individuals who have access to PII could exceed their authority and use the data for unofficial/unauthorized purposes.	The FTC's Ethics Team strictly manages access control and limits the use and access of all data to purposes for which it was collected. Designated reviewing officials (*i.e.*, FTC supervisors) only have access to the OGE Form 450 reports for which they are officially responsible. The Ethics Team shall be responsible for managing and immediately updating system accounts for reviewing officials to revoke access to filings for any employee they no longer supervise or, if the reviewing official leaves FTC service, cancelling his or her system account and login credentials to prevent continued system access. Only the FTC's Ethics Team has full access to the system. A system log is maintained that reflects who accessed the data at any given time, and whether the data was tampered with or edited. Specifically, all login activities to the FDonline system are logged. Additionally, logs related to privileged functions, administrator activity, and data changes and deletions are automatically input into the Splunk Security Information and Event Management (SIEM) tool for automated monitoring and analysis to detect suspicious activity and indicators of inappropriate or unusual activity.
An individual may enter a financial account number or other sensitive PII in a free text field.	The FTC's Ethics Team has the ability to access individual records and delete information as necessary, including financial account numbers. This and other forms of sensitive PII are not required by the system. If employees opt to provide such information, the FTC's Ethics Team will instruct the employee to remove it or the FTC's Ethics Team will delete it (advising the employee that such information should not be submitted in the future).

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

When a user logs into the system using user name, password and second authentication factor (one-time code) sent to the user's e-mail address, FDonline automatically locks the user out of his/her account after three failed password attempts. They will then be instructed to reset their password via a link sent to their e-mail address. The system also logs user activity and notes when an authorized made changes to a specific filing.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

The SORN for the FTC's Ethics Program, FTC-II-7, expressly covers paper and electronic records maintained by the Ethics Program. Further, this system corresponds to the systems described and covered by the Government-wide SORNs issued by OGE for agency ethics program records. *See* OGE/GOVT-1 (Executive Branch Personnel Public Financial disclosure Reports and Other Name-Retrieved Ethics Program Records); OGE/GOVT-2 (Executive Branch Confidential Financial Disclosure Reports). *See also* VII-3 -- Computer Systems User Identification and Access Records – FTC (i.e., for user name, IP address, e-mail address).

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

Data in FDonline is encrypted both at rest and in transit with FIPS 140-2 validated encryption.

The FTC will maintain PII and other information within FDonline in accordance with FTC regulations, policies, and procedures. Only authorized employees will have access to the system, and the system automatically logs user interaction for each filing. All FTC employees are required to undergo annual privacy and security training and periodic ethics training.