U.S. Securities and Exchange Commission

Personal Trading Compliance System (PTCS)
PRIVACY IMPACT ASSESSMENT (PIA)

January 22, 2020

Office of the Ethics Counsel

Privacy Impact Assessment

Personal Trading Compliance System (PTCS)

Section 1: System Overview

1.1 Name of Project or System

Personal Trading Compliance System (PTCS)

1.2 Is the system internally or externally hosted?

☒ Internally Hosted (SEC) Office of Information Technology

☐ Externally Hosted (Contractor or other agency/organization)

1.3 Reason for completing PIA

☐ New project or system

☒ This is an existing system undergoing an update

First developed: 2/6/2012

Last updated: 11/16/2016

Description of update: PTCS is being upgraded for the SharePoint 2013 platform and the legacy platform is scheduled to be retired by May 2020

1.4 Does the system or program employ any of the following technologies?

☒ Electronic Data Warehouse (EDW)

☐ Social Media

☐ Mobile Application (or GPS)

☐ Cloud Computing Services

☐ www.sec.gov Web Portal

☐ None of the Above

Section 2: Authority and Purpose of Collection

2.1 Describe the project and its purpose or function in the SEC's IT environment

The Personal Trading Compliance System (PTCS) is an information system owned by the SEC Office of the Ethics Counsel (OEC). Because of the nature of its regulatory mission, SEC employees are required to obtain pre-approval for securities transactions made by or on behalf of themselves, their spouses, their minor children, individuals for whom the employee serves as legal guardian.

The purpose of PTCS is to facilitate the collection and processing of personal securities information in accordance with the SEC's Supplemental Ethics Regulations, 5 CFR Part 4401, and to assure compliance by SEC employees with those regulations; the SEC's Conduct Regulations, 17 CFR Part 200, Subpart M,; and the federal government ethics laws and regulations, including the Ethics in Government Act of 1978 and Office of Government Ethics regulations at 5 CFR Parts 2635 and 2640.

PTCS is used for the submission and processing of Pre-Trade Requests for securities transactions and for the Annual Certification of Holdings for the previous calendar year. Employees submit and process Pre-Trade Requests for securities transactions and OEC reviews all these requests and either approves or rejects them. If approved, the employee has 5 business days to execute the transaction, and then must report the transaction within 5 business days after it is executed. Every year, employees are required to upload year-end brokerage statements containing reportable securities holdings and transactions and certify compliance.

User authentication is currently performed via Active Directory (AD) integration with the SharePoint 2010 infrastructure PTCS is built upon. PTCS will be migrated to SharePoint 2013 by approximately February 2020.

2.2 What specific legal authorities, arrangements, and/or agreements allow the information to be collected?

SEC Supplemental Ethics Regulations, 5 CFR Part 4401; SEC's Conduct Regulations, 17 CFR Part 200, Subpart M; and the federal government ethics laws and regulations, including the Ethics in Government Act of 1978 and Office of Government Ethics regulations at 5 CFR Parts 2635 and 2640.

2.3 Does the project use, collect, or maintain Social Security numbers (SSNs)? *This includes truncated SSNs.*

☒ No
☐ Yes
If yes, provide the purpose of collection:
If yes, provide the legal authority:

2.4 Do you retrieve data in the system by using a personal identifier?

☐ No
☐ Yes, a SORN is in progress
☒ Yes, there is an existing SORN
Ethics Conduct Rules Files (SEC-60), 74 Fed. Reg. 46254 (Sept. 8, 2009).

2.5 Is the information covered by the Paperwork Reduction Act of 1995 (PRA)?

☒ No
☐ Yes

2.6 Considering the purpose of the collection, what privacy risks were identified and how were those risks mitigated?

The purpose of the system is to help SEC employees comply with regulatory requirements regarding reporting and pre-clearing of personal securities holdings and transactions. The primary privacy risk is that employees will submit more personal financial information than is required.

This privacy risk is mitigated by clearly communicating to employees the requirements of the SEC Supplemental Ethics Rule. Employees receive training at new employee orientation and annually on the personal trading rules; receive instructions on preclearance and reporting requirements; have access to frequently asked questions on personal trading at OEC's website; and can contact OEC directly for advice and guidance. Employees also receive reminders of their obligations via ethics communications from the Office of Ethics Counsel, and on SEC's intranet.

Section 3: Data Collection, Minimization, and Retention

3.1 What information is collected, maintained, used, or disseminated about individuals? *Check all that apply.*

☐ The system does not collect, maintain, use, or disseminate information about individuals.

Identifying Numbers

☐ Social Security Number	☐ Alien Registration	☒ Financial Accounts
☐ Taxpayer ID	☐ Driver's License Number	☒ Financial Transactions
☐ Employee ID	☐ Passport Information	☐ Vehicle Identifiers
☐ File/Case ID	☐ Credit Card Number	☐ Employer ID
☐ Other:		

General Personal Data		
☒ Name	☐ Date of Birth	☐ Marriage Records
☐ Maiden Name	☐ Place of Birth	☒ Financial Information
☐ Alias	☒ Home Address	☐ Medical Information
☐ Gender	☐ Telephone Number	☐ Military Service
☐ Age	☐ Email Address	☐ Mother's Maiden Name
☐ Race/Ethnicity	☐ Education Records	☐ Health Plan Numbers
☐ Civil or Criminal History	☒ Zip Code	
☐ Other:		
Work-Related Data		
☐ Occupation	☐ Telephone Number	☐ Salary
☒ Job Title	☒ Email Address	☐ Work History
☐ Work Address	☐ Certificate/License Number	☐ Business Associates
☐ PIV Card Information	☐ Fax Number	
☒ Other: Department/Office		
Distinguishing Features/Biometrics		
☐ Fingerprints	☐ Photographs	☐ Genetic Information
☐ Voice Recording	☐ Video Recordings	☐ Voice Signature
☐ Other:		
System Administration/Audit Data		
☒ User ID	☒ Date/Time of Access	☐ ID Files Accessed
☐ IP Address	☐ Queries Ran	☐ Contents of Files
☐ Other:		

3.2 Why is the PII listed in Question 3.1 collected, used, shared, or maintained by the system or project?

The data being collected is to facilitate the user's certification of holdings and preclearance and confirmation of personal securities transactions, to assist employees in avoiding prohibited holdings, and to assist employees in avoiding conflicts between their official duties and their private financial interests. Employees are instructed on the option to redact personal information, for example home address, from financial statements that employees upload as part of the Annual Certification of Holdings. If submitted, OEC does not use or disseminate any such personal information.

3.3 Whose information may be collected, used, shared, or maintained by the system?

☒ SEC Employees
Purpose: Annual certification of holdings and pre-clearance of securities transactions.

☐ SEC Federal Contractors
Purpose:

☒ Interns
Purpose: Pre-clearance of securities transactions.

☐ Members of the Public
Purpose:

☒ Employee Family Members
Purpose: Annual certification of holdings and pre-clearance of securities transactions.

☒ Former Employees
Purpose: OEC maintains PTCS records after employees depart the SEC, as required by our records retention schedule approved by the Office of Records Management Services (ORMS).

☐ Job Applicants

Purpose:

☐ Vendors
Purpose:

☐ Other:
Purpose:

3.4 Describe the PII minimizing mechanisms and if the PII from the system is being used for testing, training, and/or research efforts.

For application development, training and/or high level research efforts, fictitious data is used. In the case of major bug resolution or system enhancements, additional research and testing with real data is authorized by the CIO with proper justification to ensure successful deployments to the production environment.

3.5 Has a retention schedule been established by the National Archives and Records Administration (NARA)?

☐ No.

☒ Yes.
GRS 2.8 item 010 requires retention of PTCS records for 6 years.

3.6 What are the procedures for identification and disposition at the end of the retention period?

At the end of each retention period, OEC seeks permission from ORMS to destroy applicable records (more than 6 years old). Once permission is granted, OEC properly disposes of those calendar year records.

3.7 Will the system monitor members of the public, employees, and/or contractors?

☒ N/A

☐ Members of the Public
Purpose:

☐ Employees
Purpose:

☐ Contractors
Purpose:

3.8 Considering the type of information collected, what privacy risks were identified and how were those risks mitigated?

The privacy risk associated with the use of PTCS information is misuse of data by authorized users. This risk is mitigated by employing role-based access to PTCS data to only the respective employee and those in OEC who need to have access to the employee's personal information to implement the SEC's compliance program. Also, version history is enabled to record changes. In addition, OEC validates roles as part of the Office of Information Technology's (OIT) bi-annual user access validation process.

Section 4: Openness and Transparency

4.1 What forms of privacy notice were provided to the individuals prior to collection of data? *Check all that apply.*

☐ Privacy Act Statement

☒ System of Records Notice
SEC-60 "Ethics Conduct Rules Files"
☒ Privacy Impact Assessment
Date of Last Update: 2/24/2013
☐ Web Privacy Policy

☒ Other notice:
FAQs for employees, posted on OEC's SharePoint site (FAQs Personal Trading; FAQs, Annual Certification of Holdings
☐ Notice was not provided.

4.2 Considering the method(s) of notice provided, what privacy risks were identified regarding adequate notice and how were those risks mitigated?

The primary privacy risk is inadequate notice. This risk is mitigated by providing training at new employee orientation and annually on the personal trading rules; providing access to frequently asked questions on personal trading at OEC's website; publication of routine uses in SORN SEC-60 "Ethics Conduct Rules Files;" and publication of the PTCS PIA.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

Compliance Administrators review and approve or reject pre-trade requests submitted by employees, and review financial statements submitted for the Annual Certification of Holdings. They may ask questions of and provide ethics advice and guidance to employees about the securities information presented, and Compliance Administrators may correct or advise employees to correct the information as a result. Compliance Administrators, the Chief Compliance Officer (CCO), the Designated Agency Ethics Official (DAEO), and the Alternate DAEO (ADAEO) can add comments to PTCS documenting decisions made.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes
Organizations: PTCS may share and disclose information with SEC organizations that is consistent with the disclosures authorized in Privacy Act 5 USC 552a(b). For example, disclosure to the Office of the Inspector General, Office of Human Resources (OHR), and/or an employee's supervisor concerning a compliance violation, for purposes of consideration of enforcement action taken by those offices.

5.3 Describe the risk to privacy from internal sharing and describe how the risks are mitigated.

The primary privacy risk is inappropriate disclosure of personal information to unauthorized parties. This risk is mitigated by segmenting access to PTCS data in two groups. (1) Employees can see only the data they have submitted themselves; (2) Compliance Administrators, the CCO, the DAEO, and the ADAEO, all in OEC, can see all data submitted by all users. Procedures have been written for the management and monitoring of the SharePoint groups that identify users in one of the three designated roles (Employee, Compliance Administrator (includes CCO), and DAEO/ADAEO (includes CCO)). Unauthorized access risk is further mitigated by OEC participating in OIT's bi-annual user access validation process, initiated by the OIT Cyber Documentation Team.

5.4 Will external organizations have access to the data?

☐ No
☒ Yes

Organizations: PTCS may share and disclose information with organizations external to SEC that is consistent with the disclosures authorized in the routine uses listed in SORN SEC-60. When transmitting information derived from PTCS to organizations external to SEC under the SORN (e.g., to DOJ in connection with a legal proceeding), OEC complies with whatever protocols OIT then has in place, for example, encrypted email transmission. OEC will not share PTCS information with any other external organizations besides those described in the SORN. Data is transmitted or disclosed using the established processes and procedures for making disclosures under SORN SEC-60.

5.5 Describe the risk to privacy from external sharing and describe how the risks are mitigated.

Recipients of this information that are external to SEC, have their own established safeguards in place to protect data, which may contain confidential information from PTCS, once received from OEC. There is a risk that SEC will share PTCS data under inappropriate circumstances, or with individuals without a demonstrated need to know. This risk is mitigated by laws, statutes or other arrangements that generally require the external party accessing or receiving information to employ measures relating to security, privacy, and safeguarding of information that are equivalent or comparable to measures employed by SEC. OEC relies on those controls for protecting the information disclosed to the external organizations.

Section 6: Data Quality and Integrity

6.1 Is the information collected directly from the individual or from another source?

☒ Directly from the individual.
☒ Other source(s): PTCS receives data indirectly from other SEC Divisions/Office and from sources external to the SEC. Compliance Administrators also may enter data as a proxy for an employee.

6.2 What methods will be used to collect the data?

Data in PTCS is entered directly by employees and by OEC Compliance Administrators. PTCS receives a securities data feed from an outside vendor pursuant to an OIT contract. PTCS receives AD information from OIT. Compliance Administrators also may enter data as a proxy for an employee in certain circumstances outlined in OEC procedures (for example, when the employee is out of the office or without internet access), which include a requirement that the CA obtain the data to be entered into PTCS, and permission to do so, directly from the employee. For each Annual Certification of Holdings (COH), OEC receives from OHR a master list of employees onboard as of December 31 of the prior year, and uses that list to launch the COH task for that year.

6.3 How will the data collected from individuals, or derived by the system, be checked for accuracy and completeness?

Data processed in the system (e.g., Pre-Trade Requests; Annual Certification of Holdings) is entered directly by individual employees or at their direction by a Compliance Administrator as the employee's proxy. Employees are required to submit accurate information into PTCS and to certify to the accuracy and completeness of their Annual Certification of Holdings. An employee always has access to the information in PTCS that the employee entered, or that was entered on the employee's behalf by a CA as the employee's proxy, and the employee is obligated to ensure that the employee's data in PTCS is accurate and complete.

OEC does not check data feeds into PTCS or data received from OHR for accuracy and completeness. OEC relies on the data originators to validate their own data before it is sent to PTCS/OEC.

6.4 Does the project or system process, or access, PII in any other SEC system?

☐ No

☒ Yes.

System(s): PTCS consumes active directory (AD) data maintained by OIT and stores it in a master user information list to which it will reference user IDs for permission-based restrictions.

6.5 Consider the sources of the data and methods of collection and discuss the privacy risk for this system related to data quality and integrity? How are these risks mitigated?

There is a risk that PTCS may receive inaccurate brokerage information or collect more data than is necessary. To mitigate this risk, OEC publishes FAQs and training materials for employee reference to ensure they are aware of both their responsibilities as an SEC employee and to distinguish what information is required and what may be redacted prior to submission. PTCS relies on accurate information from AD administered by OIT, which in turn is reliant on accurate employee information originating from OHR.

Section 7: Individual Participation

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

The employee may not decline to provide data, as it is required by law. Reporting of personal securities holdings and transactions is required by SEC and government ethics laws and regulations and is part of the terms of employment for every SEC employee. The use of the information is limited to the purposes for which the information is collected.

7.2 What procedures are in place to allow individuals to access their information?

Employees are permitted to access information they have entered or that has been entered at their direction and on their behalf by a Compliance Administrator, for the past six years.

7.3 Can individuals amend information about themselves in the system? If so, how?

Once Pre-Trade Requests or the Annual Certification of Holdings are complete, employees may view but may not access the information they originally entered, to make a correction. Employees may contact a Compliance Administrator to enable the employee to enter a correction to the Annual Certification of Holdings, or may enter a new Pre-Trade Request and cancel the incorrect one. PTCS keeps copies of all such entries (during the 6-year records retention period) for audit purposes.

Most information entered into the system by an OEC employee is not visible to the employee about whom the records pertains, and may contain deliberative or privileged information. Employees may contact the SEC FOIA/Privacy Act Officer to receive information on how to access, contest, or correct information in the system.

7.4 Discuss the privacy risks related to individual participation and redress? How were these risks mitigated?

There is no risk to individual participation. Data in the system is entered directly by the individual employee, or entered at the employee's direction and on the employee's behalf by a Compliance Administrator. Employees can view their information going back six years and are able to correct inaccurate information by contacting a

Compliance Administrator. Compliance Administrators can either correct erroneous information brought to their attention by employees (unless corrections would undermine the integrity of the information entered), or advise employees on how to submit corrected information. OEC staff interaction with the employee concerning corrections helps to mitigate the risk that the integrity of the information submitted in PTCS and upon which OEC made compliance decisions, would be compromised.

Section 8: Security

8.1 Has the system been authorized to process information?

☒ Yes
Date of Authority to Operate (ATO) Expected or Granted: 4/29/2019
☐ No

8.2 Identify individuals who will have access to the data in the project or system and state their respective roles.

☒ Users
Roles: Every SEC federal employee is granted this role as part of the "onboarding" process. This role gives the user the ability to create forms requesting preapproval of transactions, confirm transactions, and annually certify holdings and transactions and upload financial statements.
☐ Contractors
Roles:
☐ Managers
Roles:
☒ Program Staff
Roles: Compliance Administrators, Chief Compliance Officer, DAEO/Alternate DAEO. Users that have been granted this role have the ability to view forms created by all users, and to enter transactions and upload financial statements as a proxy for another user. They can approve or reject trade requests. They cannot do so for their own requests.
☐ Developers
Roles:
☒ System Administrators
Roles: Application Administrators. Site Collection Administrators are a group responsible for maintenance of systems hardware and software and related infrastructure. Data Administrator is a group responsible for the performance, integrity and security of a database.
☐ Others:
Roles:

8.3 Can the system be accessed outside of a connected SEC network?

☒ No
☐ Yes

If yes, is secured authentication required?	☐	No	☐	Yes	☐	Not Applicable
Is the session encrypted?	☐	No	☐	Yes	☐	Not Applicable

8.4 How will the system be secured?

The application currently resides in a partitioned, secure, encrypted section of the SharePoint 2010 application farm. The application will be moved to SharePoint 2013 in FY 2020. The information in the system is encrypted at rest and in transit. SharePoint security groups delegate varying levels of access for the separate roles. TLS 1.2 is enabled (https) and there is no external access allowed to PTCS, so there is no DMZ or firewall

needed to restrict external users accessing the system without being on the SEC network via go.sec.gov (need user ID, network password, mobile access password and RSA app code). SEC employees can access PTCS provided they are able to access the SEC network. Post submission, employee requests or submissions are automatically restricted to permit compliance staff to review a static version of the data. Based on the determination of compliance staff, the employee may be required to supplement additional information, in which case access is re-opened to the employee. Once the process is complete, the material is deemed a record and access is restricted to a read-only state. There are no special physical controls for PTCS, beyond SEC network access controls. There are no technical controls for PTCS, beyond the SEC network access controls described above. PTCS is subject to and complies with all of the normal OIT administrative controls such as SS&A and bi-annual user access recertification.

8.5 Does the project or system involve an online collection of personal data?

☒ No
☐ Yes
Public
URL:

8.6 Does the site have a posted privacy notice?

☒ No
☐ Yes
☐ N/A

8.7 Does the project or system use web measurement and/or customization technologies?

☒ No
☐ Yes, but they do not collect PII

☐ Yes, and they collect PII

8.8 Describe any privacy risks for this system that relate to the technology and security of the system and how those risks are mitigated.

The primary privacy risk is inappropriate disclosure of personal financial information to unauthorized parties. This risk is mitigated by limiting access to those OEC personnel whose official duties require access. Computerized records are safeguarded through information technology security.

Section 9: Accountability and Auditing

9.1 Describe what privacy training is provided to users, either general or specific to the system or project.

All SEC users complete the Privacy and Information Security Awareness training prior to being granted access to SEC information and information systems. Also, users are trained on SEC Rules of the Road governing their activities related to safeguarding SEC information. Privacy and Information Security Awareness is provided on a continuous basis to keep users alert to the privacy and security requirements and safeguards.

9.2 Does the system generate reports that contain information on individuals?

☐ No
☒ Yes
OEC generates reports internally for its use in managing the program; these reports typically include employee name. OEC also generates an annual report that is sent to the Division of Economic and Risk Analysis (DERA) as part of our compliance testing program; this report contains employee name.

9.3 Do contracts for the system include Federal Acquisition Regulation (FAR) and other applicable clauses ensuring adherence to the privacy provisions and practices?

☐ No
☐ Yes
☒ This is not a contractor operated system

9.4 Does the system employ audit logging or event logging?

☐ No
☒ Yes
Version history is enabled to record changes. The audit logs are integrated with Splunk.

9.5 What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of the data? What mechanisms are in place to identify security breaches?

All PTCS users are authenticated via integration with the SEC's active directory system before gaining access to the PTCS. Users will also have role-based access to information in the system as determined by OEC Staff. Roles will be assigned based on the staffer's function in the Office of Ethics, i.e., Compliance Administrators, the CCO, the DAEO, and the ADAEO, all in OEC, can see all data submitted by all users. PTCS utilizes the SEC network physical controls and technical controls per the General Support System. PTCS is subject to and complies with OIT administrative controls such as SS&A and bi-annual user access recertification. PTCS also is subject to OIT's annual SharePoint Site attestation that mandates audits of all groups accessing the SharePoint site.

9.6 Given the sensitivity of the PII in the system, manner of use, and established safeguards, describe the expected residual risk related to access.

This systems is only accessible to SEC staff. Administrative, technical, and physical security controls, inherited from the SEC general support system (GSS), are in-place to safeguard information collected by and stored in PTCS. Based on these controls there are no additional identified residual risks related to access. .