Privacy Impact Assessment
for the

Seized Assets and Case Tracking System (SEACATS)

DHS/CBP/PIA-040

April 10, 2017

Contact Point
Dennis McKenzie
SEACATS Business Owner
U.S. Customs and Border Protection
(202) 344-2476

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) Seized Assets and Case Tracking System (SEACATS) is the information system of record for the full lifecycle of all enforcement incidents related to CBP and U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) operations. The system tracks the physical inventory and records disposition of all seized assets, as well as the administrative and criminal cases associated with those seizures, and functions as the case management system capturing the relevant information and adjudication of the legal outcomes of all fines, penalties, and liquidated damages. The system also serves as the financial system of record for all collections related to these enforcement actions. This PIA is being conducted because SEACATS collects and maintains personally identifiable information (PII) about members of the public associated with CBP arrests and seizures during law enforcement operations.

Overview

SEACATS provides CBP with a single repository for enforcement actions related to the Treasury Forfeiture Fund (TFF),[1] as well as seized property inventory and case processing information related to arrests, seized and forfeited property, fines, penalties, and liquidated damages. SEACATS is managed and operated by CBP's Office of Field Operations (OFO) for use by the OFO Fines, Penalties, and Forfeitures (FP&F) and the U.S. Border Patrol's Asset Forfeiture (AF) divisions, including use by other departments and agencies with similar law enforcement responsibilities to: (1) provide accurate and timely management information; (2) measure seizure performance; (3) track seized and forfeited property; (4) provide a single, accurate repository for case and incident information; (5) document individuals and businesses who violated, or are alleged to have violated, customs, immigration, agriculture, or other laws and regulations enforced or administered by CBP; (6) collect and maintain records on fines, penalties, and forfeitures; and (7) collect and maintain records of individuals who have provided assistance with respect to identifying or locating individuals who have or are alleged to have violated customs, immigration, agriculture, or other laws and regulations enforced or administered by CBP and its partners.

Process

The process begins when an enforcement action results in an arrest, or when property is seized by CBP or ICE, and includes supporting information, such as: the violation, property description, quantities, and violator. Once an arrest or seizure case is initiated, the initiating officer must submit the incident report in SEACATS to his or her supervisor within 24 hours of the arrest

[1] The Treasury Forfeiture Fund (TFF) is the receipt account for the deposit of non-tax forfeitures made pursuant to laws enforced or administered by bureaus participating in the TFF. The principal revenue-producing member bureaus include the Internal Revenue Service's Criminal Investigation (IRS-CI), U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and U.S. Secret Service (USSS).

or seizure. The incident report may include supporting information about the violation, the property description, quantities of items seized, and information related to the violator. At this stage, cases are assigned a SEACATS tracking number associated with the incident report. The incident report is then forwarded to the appropriate supervisor who has 24 hours to review and decide whether to approve it. Once approved by the supervisor, the case is referred to FP&F or AF within five business days for processing. Questions or concerns from the violator regarding a case are referred to the FP&F or AF office with jurisdiction over the port of entry or station where the property was seized. All inquiries into a SEACATS case must be associated with the assigned tracking number, which is used to identify the specific case when contacting FP&F or AF.

SEACATS Documentation

The current SEACATS Legacy System provides documentation for CBP enforcement activities related to arrests and seizures. This includes:

- Arrests of fugitives or violators of CBP-related law enforcement activities.
- Issuance of penalties and liquidated damages.
- CBP enforcement activities from case initiation to final disposition and closure.
- Collection of fines and penalties related to enforcing laws.
- Administrative forfeiture of seized property.
- Fugitives identified by National Crime Information Center (NCIC) records.
- Auditable financial year end statements for the Department of Treasury to document the financials of CBP Forfeiture Programs. Reported financial information includes all information that is entered into SEACATS, including any information ICE HSI stored in the SEACATS system.

Transition from the Legacy System to the Modernization System[2]

The legacy SEACATS platform does not meet CBP's mission needs and will be decommissioned with the implementation of a modernized SEACATS. CBP requires a system capable of supporting system-to-system data sharing, such as the sharing of information between SEACATS and the Automated Targeting System (ATS),[3] which has the ability to generate targeting and intelligence information to meet the requirements of CBP and its mission partners.

[2] Modernized SEACATS will be placed into operation in September 2017.
[3] *See* DHS/CBP/PIA-006(e) Automated Targeting System (ATS) (January 13, 2017), *available at* https://www.dhs.gov/publication/automated-targeting-system-ats-update.

In order to meet these needs, CBP is updating legacy SEACATS to a modern, scalable system to enhance information sharing between disparate enforcement systems and geographical locations.

The modernized SEACATS system improves upon the legacy SEACATS system by providing increased support for updates and bug fixes, improved security posture, and server virtualization for improved hardware consistency. When transitioning the legacy SEACATS database and its functions to the modernized SEACATS system, CBP uses adaptive type software, which leverages agile development methodologies.[4] The modernized SEACATS system creates necessary interfaces between CBP and ICE enforcement systems to increase the efficiency of its operations and maintenance (see Section 3.3 of this PIA). The modernized SEACATS system also enhances access to the enforcement systems necessary to meet CBP's present and future mission needs.

With the transition from legacy SEACATS to modernized SEACATS, SEACATS moves from an outdated mainframe platform[5] technology to a more modern, cloud computing technology. The modernized SEACATS system uses the CBP Cloud Computing Environment (C3E), a virtualized environment[6] that improves security, provides better support, reduces build-out time, and increases environmental consistency. The C3E operating system uses a modern, unified, technically supported operating system that allows updates as newer versions of operating systems are released, which allows the system to be more secure against cyber threats.

Improved System-to-System Data Sharing within CBP

SEACATS relies on data sharing via direct connections with a variety of CBP systems, including: TECS,[7] Automated Commercial Environment (ACE),[8] Tasking, Operations, and

[4] Agile software development is a set of principles for software development in which requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development, early delivery, and continuous improvement, and it encourages rapid and flexible response to change. Agile itself has never defined any specific methods to achieve this, but many systems have grown as a result and are recognized as being "Agile."

[5] Mainframe computers refer to the large cabinets called "mainframes" that house the central processing unit and main memory of early computers. The mainframe platforms no longer receive technical support, which leaves SEACATS difficult to update and vulnerable to cyber-attacks, viruses, malware, hackers, and compatibility issues.

[6] Virtualized environments emulate a particular computer system. A virtual environment is comprised of virtual machines that operate based on the computer architecture and functions of a real or hypothetical computer.

[7] *See* DHS/CBP/PIA-021 TECS System: Platform (August 12, 2016), *available at* https://www.dhs.gov/publication/dhscbppia-021-tecs-system-platform.

[8] *See* DHS/CBP/PIA-003 Automated Commercial Environment (ACE) (July 31, 2015), *available at* https://www.dhs.gov/publication/filing-data-acsace.

Management Information System (TOMIS),[9] CBP Portal (E3),[10] Systems, Applications, and Products in Data Processing (SAP),[11] Firearms and Credentials Tracking System (FACTS),[12] and ATS. Each of these connections contributes to a more complete and accurate law enforcement information. Legacy SEACATS maintains a direct interface with TECS; TECS is critical to SEACATS because the legacy TECS database serves as the repository for SEACATS information. Completed SEACATS reports are sent to TECS to document activity and store records. Modernized SEACATS will continue to maintain this connection to TECS, but will now reside on its own dedicated platform as a stand-alone system with the ability to interact with systems such as TECS. In return, TECS requires access to SEACATS to monitor law enforcement activity, primarily for subject entry and queries.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

CBP's law enforcement jurisdiction is highly complex and derives authority from a wide spectrum of federal statutes. The following are legal authorities related to the operations and maintenance of SEACATS:

- 5 U.S.C. § 301;
- The Federal Records Act, 44 U.S.C. § 3101;
- Immigration laws, including 8 U.S.C. §§ 1221 and 1321-1328, and 8 CFR parts 270, 274, 280;
- Customs laws, including but not limited to: 18 U.S.C. §§ 542 and 545, and 19 U.S.C. §§ 66, 1436, 1497, 1509, 1592, 1593a, 1594, 1595a, 1618, 1619, 1624, and 1703, and 19 CFR parts 162, 162.31(a), 162.31(b), 171, and 172;
- Agriculture laws, including 7 U.S.C. §§ 8303, 8304, and 8307; and
- Executive Order 9397, *Numbering System for Federal Accounts Relating to Individual Persons*, as amended by Executive Order 13478, *Amendments to Executive Order 9397*

[9] TOMIS is a mainframe reporting management information system that only collects PII from DHS personnel. TOMIS is covered under DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012).

[10] *See* DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT (July 25, 2012), *available at* https://www.dhs.gov/publication/cbp-portal-e3-enforceident.

[11] SAP is a multi-module financial system that maintains PII of CBP personnel and members of the public. SAP is described in DHS/ALL/PIA-053 DHS Financial Management Systems (July 30, 2015), *available at* https://www.dhs.gov/publication/dhsallpia-053-dhs-financial-management-systems.

[12] FACTS is an asset management system that tracks and records purchase, seizure, and distribution of assets for redistribution or for final disposition. FACTS is covered under DHS/ALL-010 DHS Security Asset Management Records System of Records, 73 FR 63181 (October 23, 2008).

Relating to Federal Agency Use of Social Security Numbers.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The Seized Assets and Case Tracking System System of Records Notice[13] (SORN) governs maintenance, use, and dissemination of SEACATS information.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

The SEACATS system has a current security plan and Authority to Operate (ATO) that was completed on April 4, 2014. The security plan for SEACATS is updated annually or as necessary. A new ATO will be completed in April 2017 and will include both the legacy and modernized portions of the SEACATS information system. Modernized SEACATS will be placed into operation in September 2017.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

CBP retains SEACATS records consistent with the SEACATS SORN. Specifically, records that are related to a law enforcement action; are linked to an alleged violation of law or regulation; or match or are suspected of matching to enforcement activities, investigations, or cases (i.e., administrative penalty actions or criminal prosecutions) will remain accessible until the conclusion of the law enforcement matter and any other related enforcement matters or associated investigative, administrative, or judicial action, plus five years. Records associated with a law enforcement matter, when all applicable statutes of limitation have expired prior to the conclusion of the matter, will be retained for two years following the expiration of the applicable statute of limitations.

[13] *See* DHS/CBP-013 Seized Assets and Case Tracking System, 73 FR 77764 (December 19, 2008).

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

CBP uses legacy U.S. Customs Forms (CF) [14] that are in the process of being converted for use by Modernized SEACATS. Many of these forms are "For-Official-Use-Only" (FOUO), and are accessed through a restricted webpage requiring username and password. These forms now go through the privacy compliance and Paperwork Reduction Act (PRA) processes; however, they do not currently have OMB Control numbers. Once automated, and OMB Control numbers are received, these forms will allow SEACATS to reduce the amount of paperwork required.

The following forms are included or referenced in internal procedures and documents:

- Seized Asset Management and Enforcement Procedures Handbook Issued by OFO, FP&F Division, HB 4400-01B (07/2011);
- DHS Form 4605: Currency/Monetary Instrument Seizure Inventory (corresponds with CF 6051S);
- CF 6051S: Custody Receipt for Seized Property and Evidence (11/2001);
- CF Form 6051A: Continuation Sheet Custody Receipt for Detained or Seized Property (11/2001);
- DHS Form 4613: Order to Destroy and Record of Destruction of Forfeited, Abandoned, or Unclaimed Merchandise (10/1999);
- CF 58: Vehicle/Vessel/Aircraft Inventory and Receipt (03/2004);
- CF 4607: Notice of Abandonment and Assent to Forfeiture of Prohibited or Seized Merchandise; 19 CFR part 162 (06/2011); and
- CF 6051-I: Shelf Weight Recordation Log (04/2009).

Per DHS policy, and through coordination with the PRA Office, the CBP Privacy Office reviews all applicable SEACATS forms to ensure privacy oversight is provided for all PII collected. The CBP Privacy Office is in the process of completing an inventory of all SEACATS forms.

[14] Legacy U.S. Customs Forms (CF) and DHS forms used during seizures and for control of seized assets/goods are for internal use and marked "For-Official-Use Only." They are not publicly available, and are only provided to the violator, or those with official responsibilities in carrying out seizures or taking control of seized assets/goods in violation of an applicable import law or regulation.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

In general, individuals whose information is included in this system include current, former, alleged, or suspected violators of customs, immigration, agriculture, or other laws and regulations administered or enforced by CBP. In addition, this system maintains information related to parties involved in, affected by, or queried concerning the violation of customs, immigration, agriculture, or other laws enforced or administered by CBP.

Individuals whose information may be retained in this system include:

- Individuals believed to be involved in possible violation of customs, immigration, agriculture, or other laws administered or enforced by CBP.
- Individuals believed to be involved in smuggling merchandise or contraband, including narcotics and other illegal drugs, into the Unites States.
- Individuals and businesses fined, penalized, or forced to forfeit merchandise because of violations of customs, immigration, agriculture, or other laws administered or enforced by CBP.
- Individuals and businesses who have filed false invoices, documents, or statements that result in a violation of customs, immigration, agriculture, or other laws and regulations administered or enforced by CBP.
- Individuals and businesses who have filed supplemental petitions for relief from fines, penalties, and forfeitures assessed for violations of the laws and regulations administered or enforced by CBP.
- Owners, claimants, and other interested parties to seized property.
- Purchasers of forfeited property.
- Individuals to whom prohibited merchandise is addressed.
- Individuals who assist in the enforcement of customs, immigration, agriculture, or other laws administered or enforced by CBP.

In addition, SEACATS contains information linked to vessels, aircraft, and other conveyances used in or found in violation of customs, immigration, agriculture, or other laws and regulations enforced or administered by CBP.

Specific data elements retained in this system may include:

- Name (Last name, first name, and middle name or initial)
- Aliases

- Business name
- Social Security number
- Physical description of individual
- Date of birth
- Business, home, and work addresses
- Telephone number
- Citizenship (country of document issuance)
- Gender
- Criminal history
- Violator's prior history
- Occupation
- Driver's License Information
- Document type, number, and related details (e.g., passport, visa, Alien Registration Number)
- Country of residence
- U.S. address while in the United States (number and street, city, state, zip code)
- U.S. Border Crossing event history, when applicable
- Entry documentation
- Personal identifying number, such as informant number
- Case number or seizure number
- Description of merchandise
- Location of merchandise
- Financial value of merchandise
- Import/export information
- Immigration status
- Case disposition information
- Fines and penalties data

- Vessel name, including registration number
- Aircraft name and tail number
- License plate number
- Type of violation/suspected violation
- Description of violation or alleged violation, including circumstances surrounding the violation or alleged violation, and the section of law violated or alleged to have been violated
- Date and place of violation or alleged violation
- On-site disposition actions, such as whether a seizure was made, an item was detained, or inspection occurred
- Sender of the seized or detained goods
- Intended recipient of the seized or detained goods
- Parties entitled to legal notice or who are legally liable
- Bond information
- Notices (such as a notice of seizure, arrival violation, etc.)
- Investigative reports and disposition of fines, penalties, and forfeitures
- Case-related memoranda
- Petitions and supplemental petitions
- Recommendations pertaining to litigation
- Referrals to the Department of Justice
- Notes from officers related to a CBP action
- Case information pertaining to violation
- Actions taken by CBP
- Documents relating to the internal review and consideration of the request for relief (including return of property) and decision thereon
- Property description
- CBP Port code
- Delivery to seizure clerk who maintains custody of seized property

- Applicants for awards of compensation and determination of such applications
- External DHS agencies initiating a case: Department of Treasury and Internal Revenue Service (IRS)

2.2 What are the sources of the information and how is the information collected for the project?

SEACATS collects information from the following sources:

Systems

Several CBP systems provide SEACATS with information.

- SEACATS and ACE exchange information when revenue is collected, adjusted, refunded, or negated, keeping the two systems synchronized. This information is used to create IRS tax forms.
- TOMIS initiates the SEACATS incident entry process (seizure or arrest). Using the TOMIS interface, users can create a corresponding incident in SEACATS.
- SEACATS supports the import of certain E3 event data into a SEACATS incident to facilitate the initial creation of SEACATS records. E3 is Border Patrol's enforcement action monitoring system.

Forms

- Forms completed by the individual, including: CBP Declaration forms,[15] petitions for relief of fines, penalties, and forfeitures, and appeals forms.
- Forms completed and information supplied by importers, brokers, and other agents pursuant to the entry and processing of merchandise or in the clearing of individuals or baggage through CBP.

Documents

- Information gathered during CBP investigations of suspected or actual violations of customs, immigration, agriculture, or other laws enforced or administered by CBP, regulations, recommendations, and information supplied by other agencies.
- Information related to mail or express consignment shipments, including shipper, consignee, and shipping manifest listing.
- Passports, licenses, and other government-issued identification.
- Shipping manifests.

[15] U.S. Customs and Border Protection Customs Declaration Form, *available at* https://www.cbp.gov/sites/default/files/assets/documents/2016-Jun/CBP%20Form%206059B%20%280316%29%20-%20Fillable_ENGLISH_0.pdf.

Individuals

- CBP Port Directors and Border Patrol Sector Chiefs with jurisdiction over fines, penalties, and forfeitures.
- Passports, licenses, and other government-issued identification.
- Officers and agents of other federal agencies, such as: U.S. Secret Service, ICE, and IRS.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. This system does not collect or use commercial or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Data collected by officers or agents initiating a case is entered into SEACATS and assigned a tracking number prior to being submitted to the incident supervisor and then FP&F and AF officers, who review for accuracy, legal sufficiency, and approval in SEACATS.[16] All property dispositions notices are reviewed by an FP&F or AF officer before issuance. Data is collected directly from the violator, individual, or interested party associated with the property, or from his or her documents, forms, and petitions, whenever possible. Collected data is routinely compared to existing records to determine the accuracy of information and then, an additional review is conducted by an FP&F officer or AF officer.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that some PII collected is not directly relevant or necessary for SEACATS to accomplish its mission.

Mitigation: Case records undergo a two-tier review process. First, supervisors review entries for relevancy and accuracy. Then, an FP&F or AF officer reviews the case for legal sufficiency. CBP only collects information from sources that are necessary to complete and process the cases once legal sufficiency has been established. Substantiating documentation includes: individuals' statements, forms, and petitions completed by entities associated with the property, or through investigation by trained officers.

Privacy Risk: There is a privacy risk that the data is inaccurate because it is provided by a violator, who may believe he or she has a personal benefit to provide false information.

[16] The FP&F procedures are documented in the FP&F handbook. For more information, *see* https://help.cbp.gov/app/answers/detail/a_id/256/kw/FP%26F%20Officer.

Mitigation: The documents related to a seizure case, and submitted to CBP, are considered legal and official statements. Several layers of review for the information provided exist, and such statements are routinely compared to existing records or information provided by the initiating officer and undergo supervisory and FP&F or AF review. If the violator provides false information, or information implicating someone other than him or herself, and a redress action is initiated, any personal information belonging to someone other than the violator would be retained; however, such information is annotated as to not implicate those not connected to the violation.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The information contained in SEACATS is used to: 1) track and record the arrest, seizure, penalty, or liquidated damages of persons or goods entering the United States or enforcement actions abroad, as well as individuals associated with the violation; 2) target potential violatons by understanding trends of violators; 3) identify trends in enforcement actions; and 4) for other law enforcement purposes.

SEACATS shares information with several CBP systems.

- Modernized SEACATS will continue to provide TECS with seizure information through a direct automated interface. SEACATS has always been the repository for information and will continue to be. SEACATS and TECS will continue to have and share the same information, but there will be two separate systems with two separate interfaces. Modernized SEACATS is now a more robust, standalone system than it once was as part of TECS.
- SEACATS provides SAP, the financial system of record for CBP, with nightly financial information updates to keep the two systems synchronized. These updates consist of:
    - General Ledger voucher information – SEACATS tracks the value of seized or forfeited property from time of seizure to the time property leave CBP custody. Any change in property value is sent to SAP in a General Ledger voucher, which also contains property type codes (cash, other monetary instrument, or non-monetary property) and fund codes (seized or forfeited) describing the property.
    - General Order (GO) payment information – GO property is property that is abandoned and of little monetary value. When any GO property is sold, the money realized from the sale is reported to SAP as a GO payment. SAP will in turn distribute the proceeds to parties with claims on the property, for example, to the warehouse vendor storing the property.

  - Vendor account updates – The TFF employs contractors that, in turn, may subcontract out to multiple vendors that operate seized property warehouses. When these vendors change, or vendor information changes (e.g., address, point of contact, bank account number, Tax Identification Number (TIN)), the updates are sent to SAP so that vendors are correctly reimbursed for claims on GO property proceeds.

- SEACATS provides ATS with seizure, arrest, and FP&F information.
- SEACATS provides FACTS with information in the event that a weapon has been forfeited and is to be transferred to the National Firearms Program Staff (NFPS). Once the weapon is ready for transfer from CBP to NFPS, a disposition record is entered in SEACATS and sent to FACTS. FACTS then tracks the disposition record and updates SEACATS once the disposition has been completed.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. SEACATS does not conduct searches, queries, or analyses for predictive purposes.

3.3 Are there other components with assigned roles and responsibilities within the system?

Yes. Based on a need-to-know, CBP may share data from SEACATS with other DHS components. Currently, ICE is granted access to SEACATS records for law enforcement purposes. For example, ICE may have an investigation that is related to an arrest, seizure, or forfeiture in SEACATS. The ICE case number would be added to a SEACATS case as a reference in order to associate the two cases. ICE also leads task forces that may include the participation of agents from other DHS components including U.S. Citizenship and Immigration Services, U.S. Coast Guard, and the Transportation Security Administration. To access SEACATS, these personnel are granted ICE privileges.

The U.S. Secret Service (USSS) is granted limited access to IRS property records in SEACATS to request queries for the CBP property. However, USSS personnel cannot access other CBP records nor store their information in SEACATS.

Access to SEACATS is role-based, which depends on: 1) the mission of the component; 2) the user's official need-to-know; and 3) the home port that houses the required records. For security purposes, SEACATS user profiles can be set to limit access to SEACATS records, so that

a user cannot access records outside the scope of that user's need-to-know, or to which he or she is not involved.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that the information in SEACATS may be used inappropriately.

Mitigation: This risk is mitigated in several ways: 1) records entered into SEACATS require supervisory approval as well as a legal case sufficiency review by an FP&F or AF officer; 2) all users are required to complete annual privacy training that addresses the appropriate use of PII; 3) access controls are in place at every work station to prevent the creation of records in other geographic locations outside the scope of that user's need-to-know, or to which he or she is not involved; and 4) audit logs track access to records and are periodically reviewed by managers, System Control Officers, the Management Inspection Division, and the Office of Professional Responsibility. The combination of supervisory approval, access controls, and audit logs helps to prevent the misuse of information.

Privacy Risk: There is a risk that the information in SEACATS may be accessed by unauthorized persons.

Mitigation: This risk is mitigated because access to SEACATS is limited to those with an official need-to-know. When user access is requested, the request must be approved by the user's first line supervisor and the SEACATS System Control Officer. SEACATS follows and documents the security controls as identified by NIST security guidance.

With the modernization of SEACATS, two-factor authentication will be implemented for additional access control security. The legacy SEACATS system currently only requires users to input a user name and password. Modernized SEACATS requires users to have a Personal Identity Verification (PIV) card in addition to a password to be able to access the system. Currently, the underlying identity management system that supports modernized SEACATS only supports use of CBP or ICE PIV cards. Task force personnel are issued ICE PIV cards and when technically feasible, other agency PIV cards may be supported.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Once property is seized by CBP, an individual is informed of the seizure through the Custody Receipt for Seized Property and Evidence, CF 6051S form.[17] In addition, the website www.forfeiture.gov[18] is used as the primary method to notify the public that property was seized and is subject to forfeiture. The site posts seized property for thirty (30) days from the date of publication. This PIA and associated SORN also provide notice to the public regarding the collection of this information.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

When assets are seized, specific information is required at the time of seizure and may be obtained from entry documents, the individual, or through investigation. Once property is seized by CBP, an individual is informed of the seizure through the Custody Receipt for Seized Property and Evidence, CF 6051S form, which contains instructions on how to file a protest through the fines, penalties, and forfeitures process. Individuals do not have the right to opt out of the use of their information once their property has been seized. SEACATS information is collected for law enforcement purposes, and the ability to opt out would affect a lawful investigation and potential criminal prosecution.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not be aware that CBP is collecting information on their activity once a seizure is made.

Mitigation: This risk is partially mitigated. Individuals are made aware of the property seizure through the Custody Receipt for Seized Property and Evidence, CF 6051S form, and the website www.forfeiture.gov provides notice to the public that property was seized and is subject to forfeiture.

However, individuals may not be made aware of additional law enforcement activities related to the seizure. The DHS Secretary has exempted the SEACATS ststem of record from several portions of the Privacy Act including subsection (e)(8), Notice to Individuals. Given that

[17] SEACATS digital forms required to process violators and violations are only available to authorized SEACATS users with a need-to-know and a CBP-issued credential or user name and password.
[18] www.forfeiture.gov is managed by the Department of Justice's Asset Forfeiture Management Staff, and contains a comprehensive list of pending forfeiture notices for federal agencies, including CBP.

SEACATS is a law enforcement system, providing notice to an individual associated with a law enforcement activity could interfere with the legal process, pose an impossible administrative burden on DHS and other agencies, and alert the subject(s) to an investigation of which they were previously unaware, thus potentially interfering with the outcome of the investigation and possible prosecution. CBP partially mitigates this risk by providing broad public notice in this PIA of its retention of seizure and incident records in SEACATS.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

The proposed Retention and Disposal Schedules have been published in the SEACATS SORN. Records related to a law enforcement action, that are linked to an alleged violation of law or regulation, or are matches or suspected matches to enforcement activities, investigations or cases (i.e., administrative penalty actions or criminal prosecutions), will remain accessible until the conclusion of the law enforcement matter. Related investigative, administrative, or judicial action to which the action becomes associated, will remain accessible until the conclusion of the law enforcement matter, and any other enforcement matters or related investigative, administrative, or judicial action to which it becomes associated, plus five years. Records associated with a law enforcement matter, and simultaneously entered in TECS,[19] when all applicable statutes of limitation have expired prior to the conclusion of the matter, will be retained for two years following the expiration of the applicable statute of limitations.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: This is a risk that SEACATS will retain information longer than necessary.

Mitigation: The information in SEACATS must be retained long enough to meet operational needs and reach a final disposition regarding seized property. Law enforcement needs require data to be retained beyond final disposition to show a history of violations in order to determine any future fines, penalties, and forfeiture actions. In addition, data must be retained beyond final disposition of the property to identify violation trends. When information is no longer relevant, CBP purges the data in conformance with the retention period listed in the SEACATS SORN. Once a Retention and Disposal Schedule has been approved, CBP will develop a capability (programming script) to automatically purge the records.

[19] SEACATS records with a connection to a law enforcement matter are entered into both SEACATS and TECS. Records entered into TECS follow the TECS records retention schedule applicable to that system. For more information on TECS and its retention schedule, please *see* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

CBP shares legacy SEACATS information with outside entities via system-to-system interfaces and provisioning personnel from outside entities as SEACATS users. For legacy SEACATS, a Memorandum of Understanding (MOU) is signed between the outside entity and CBP Commissioner. CBP also requires an Interconnection Security Agreement that is specific to each interface implemented with the outside entity. The MOU specifies the general terms and conditions that govern the use of the data, including use limitations, and the specific information to which the agency is being granted access, depending upon its mission needs. The Interconnection Security Agreement specifies the data elements, format, and interface type based on operational considerations. Via the MOU, recipients of SEACATS data are required to employ the same or similar precautions as CBP in the safeguarding of shared information. CBP requires all non-CBP SEACATS users to receive the same training as CBP users regarding the safeguarding, security, and privacy concerns relating to information stored in SEACATS. This training is available online for users who have met the background requirements for access to the mainframe platform on which SEACATS previously resided. The training module must be completed prior to a user accessing the mainframe platform environment. Additionally, all users must complete annual privacy recertification courses to maintain access to SEACATS.

CBP also contracts with billing vendors to print and mail CBP's fines, penalties, and liquidated damages billing directly to violators on behalf of CBP. The SEACATS bill data sent via a system-to-system interface is for violations of CBP laws (penalty) or bonds (liquidated damage). The data sent includes PII (importer name, address, and money owed, and depending on the circumstance, Social Security number).

SEACATS has a system-to-system interface with the Forfeiture System operated by the Department of Justice (DOJ) Asset Forfeiture Management Staff (AFMS). SEACATS provides content weekly to AFMS in order to advertise the SEACATS administrative seizures on the DOJ's official Forfeiture.gov website. No PII is contained in the content provided to DOJ.

In addition, the DOJ's Drug Enforcement Administration receives a monthly compilation of drug type and weight seizure data, but does not have access to the system. Contractors for CBP that store seized property have access to the Property Management module, permitting them to see inventory and property tracking data, as well as any disposition orders directing them where to send the property.

As participating bureaus in TFF, legacy SEACATS user access is granted to IRS-CI and Department of Treasury Executive Office for Asset Forfeiture members. Multiple agencies within DOJ and Department of Treasury have been granted user access based on participation in law enforcement task forces.

In lieu of an MOU or other prior written agreement, information that is shared with other federal, state, local, tribal, or foreign agencies, requires a written request by the agency identifying the type of information sought and the purpose for which the information will be used. Requests are made as needed for law enforcement needs. Authorization to share information in this request scenario is subject to approval by the CBP Privacy Officer, to ensure the request and use are consistent with Privacy Act or the published routine uses and/or exemptions in the SEACATS SORN, and the receiving agency acknowledges restrictions on the re-dissemination of the shared information. All three requirements - use consistent with purpose for collection, sharing consistent with a statutory or published routine use, and acceptance of the restriction barring unauthorized dissemination outside the receiving agency - and the legal responsibility clause for wrongful dissemination contained in the Paperwork Reduction Act (44 U.S.C. § 3510) are stated as conditions pertaining to the receiving agencies acceptance and use of the shared information. These conditions are stated in the written authorization provided to the receiving agency and represent the constraints around the use and disclosure of the information at the time of the disclosure.

All external users are subject to the access controls and audit logs described in Section 3.4 of this PIA. With the requirement of two-factor authentication in modernized SEACATS, and current limitations when PIV cards of outside entities are not supported, outside agency user access is being reviewed. CBP PIV cards and equipment may be issued when required. Legacy MOUs and Interconnection Security Agreements are being reviewed and updated as appropriate based on the changes in user access requirments for modernized SEACATS.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

CBP shares data from SEACATS with entities external to DHS in accordance with the Privacy Act exemptions and routine uses identified in the SORN for the applicable SEACATS systems listed in Section 1.2.

6.3 Does the project place limitations on re-dissemination?

Yes. Prior to each sharing of information, CBP identifies limitations on the use and re-dissemination in signed MOUs and other written arrangements. CBP's external sharing of SEACATS data is required to comply with statutory requirements for national security and law enforcement systems. Additionally, MOUs and other written arrangements, which define roles and

responsibilities, have been executed between CBP and each agency that regularly accesses SEACATS. These legacy SEACATS MOUs are being reviewed and updated as required for modernized SEACATS.

In addition, agencies agree that information not owned by that agency cannot be disclosed by that agency without specific approval from CBP.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Authorization for non-DHS agencies to access SEACATS requires approval by the CBP Commissioner and is authorized via a MOU between CBP and the outside entity and an Interconnection Security Agreement specific to each interface implemented with that entity. The MOU specifies the general terms and conditions that govern the use of SEACATS and the data, including privacy-related limits on use, as well as the types of information in SEACATS to which the agency is being granted access, depending upon its mission needs. The Interconnection Security Agreement specifies the data elements, format, and interface type based on operational considerations. All legacy SEACATS MOUs and Interconnection Security Agreements are being reviewed and updated as required for modernized SEACATS.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the increased number of individuals with access to SEACATS will also increase the risk of misuse of the information.

Mitigation: This risk is mitigated and managed by employing user profiles that define rights and responsibilities concerning a user's access to data contained in the system. The principal method for determining what access rights and system responsibilities a user will have is the user's need-to-know. Need-to-know determinations are prescribed by internal CBP policies and procedures that associate a user's mission or operational responsibilities to the specific sub-set of data contained within SEACATS. SEACATS retains audit logs for all user access. These logs are reviewed to ensure that user access is limited to the information the user needs to perform his or her duties. Users are subject to periodic renewal of their access and annual required privacy training to ensure they safeguard data and are aware of the appropriate use or sharing of SEACATS information. Further, employees receive yearly recertification training on procedures for the release of information when there is a need-to-know and an operational requirement.

Privacy Risk: There is a risk that information may be shared under inappropriate circumstances.

Mitigation: CBP mitigates this risk by granting access to SEACATS using need-to-know criteria that requires a mission-related purpose before access is granted. Users are also required to comply with all privacy and security requirements, including annual IT Security and Privacy

Awareness training, in order continue access to SEACATS. In addition, SEACATS users may only share information following CBP disclosure procedures, which require disclosure requests to be submitted to the CBP Privacy Office for determination as to whether the sharing is appropriate. Once information is approved to be shared, all disclosures are documented using the DHS Form 191, Privacy Act Disclosure Record, and are retained by the program for five years.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

In general, CBP does not grant requests from individuals to access their SEACATS records because the system is primarily used for law enforcement purposes. However, if an item is detained or seized, a chain of custody form is issued to the individual. This form provides an individual with the point of contact for the case. During the fines, penalties, and forfeitures process, an individual may be given access to some information, including the reason for the action taken by CBP, to contest the determination.

The DHS Secretary has exempted this system from notification, access, and amendment because of the law enforcement nature of the information. However, CBP will review requests on a case-by-case basis and release or amend information as appropriate. Individuals seeking access to any record contained in this system of may submit a Freedom of Information Act (FOIA) or Privacy Act request in writing to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, DC 20002

Any individual, regardless of citizenship, may file a FOIA request. FOIA requests must be in writing, including a daytime phone number, email address, and as much information as possible on the subject matter to expedite the search process. Specific FOIA contact information can be found at http://www.dhs.gov/foia under "Contact Information."

When seeking records about one's self from this system of records or any other CBP system of records, the request must conform to the Privacy Act regulations set forth in 6 CFR part 5. One must first verify his or her identity, meaning that he or she must provide full name, current address, and date and place of birth. The request must be signed, and the signature must either be notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, one may obtain forms for this purpose from the Director, Disclosure and FOIA, http://www.dhs.gov or (866) 431-0486. In addition, the following information should be provided:

- An explanation of why they believe the Department would have information on them;
- Specify when they believe the records would have been created; and
- If the request is seeking records pertaining to another living individual, it must include a statement from that individual certifying his or her agreement for access to his or her records.

Without this information, CBP may not be able to conduct an effective search, and the request may be denied due to lack of specificity or lack of compliance with applicable regulations.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

There are currently no procedures for an individual to correct information in SEACATS because it is a closed law enforcement system. Notification, access, and amendment exceptions under the Privacy Act apply to SEACATS, and the proper Final Rule for Privacy Act Exemptions[20] has been made in the Federal Register. Individuals, regardless of citizenship, may seek redress through the fines, penalties, and forfeitures process if they feel their items have been improperly seized. Information an individual provides may be stored in SEACATS and used to correct improper actions.

For FP&F information, individuals can contact the address of the local FP&F Office or port of entry processing and handling the case where the violation occurred. The individual will need to provide an FP&F case number, which identifes the port handling the case. Without a case number, FP&F will not be able to assist the individual with his or her inquiry.

7.3 How does the project notify individuals about the procedures for correcting their information?

SEACATS does not provide procedures to correct information because SEACATS contains investigatory material compiled for law enforcement purposes and is exempt from the amendment provisions of the Privacy Act. Notifying an individual that he or she is or has been the subject of a law enforcement investigation would undermine the performance of the law enforcement mission of CBP. However, when an individual seeks to correct records, requests for redress should be directed to CBP's Customer Service Center below. When an individual contests an action taken by CBP with regard to a seizure, the fines, penalties, and forfeitures process will serve as the individual's method for redress.

Records are not generally available to or amendable by the public. However, individuals, regardless of citizenship, may contest a CBP action through the fines, penalties, and forfeitures

[20] Final Rule for Privacy Act Exemptions, 74 FR 45074 (August 31, 2009).

adjudication process if the action pertains to a seizure. Otherwise, travelers who have questions about CBP's travel regulations or screening process, or who wish to register a complaint about how they were treated by a CBP Officer, should contact the Customer Service Center via:

- Phone: Within the United States call: (877) 227-5511. International callers: (703) 526-4200. Phones are answered between 8:30 a.m.-5:00 p.m. EST. Telecommunications device for hearing impaired: (866) 880-6582. (Outside the United States call: 202-325-8000);
- Online: Go to http://www.cbp.gov and click on the "Have A Question?" section.
- Mail-Mail questions/concerns to:

  U.S. Customs and Border Protection (CBP)
  Office of Public Affairs
  Customer Service Center
  1300 Pennsylvania Avenue NW
  Washington, DC 20229

If the individual is uncertain what agency is responsible for maintaining the information, redress requests may be sent to DHS's Traveler Redress Inquiry Program (TRIP) online at www.dhs.gov/trip. Individuals making inquiries should provide as much identifying information as possible regarding themselves, to identify the record(s) at issue.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not get the level of redress required by law, DHS or CBP policy, or requested by the individual making the request.

Mitigation: This risk is partially mitigated. Redress for seizures is available through the fines, penalties, and forfeitures adjudication process. However, SEACATS is exempt from certain provisions of the Privacy Act. Permitting access to the records contained in SEACATS could inform violators of CBP's law enforcement techniques or activities. Access to these records could also permit the violator to impede CBP's investigation, to tamper with witnesses or evidence, and to avoid detection, seizure, or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on law enforcement agencies. The existing redress procedures are adequate to address the individual's right to access and correct his or her records and comply with all legal and policy requirements.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

SEACATS secures information by complying with the requirements of the DHS Information Technology Security Program Policy.[21] This handbook establishes a comprehensive program, consistent with federal law and policy, to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, and application rules. In order to gain access to SEACATS information, a user must not only have a need-to-know, but must also have successfully undergone a single-scope background investigation and complete annual privacy training. A supervisor submits the request to the CBP Office of Information and Technology (OIT) indicating the individual has a need-to-know for official purposes depending on the user's role within the system. CBP OIT verifies that the necessary background check and privacy training have been completed prior to issuing a new internal user account. Internal user accounts are reviewed annually to ensure that these standards are maintained. These rules also require a periodic assessment of technical, administrative, and managerial controls to enhance data integrity and accountability. System users must sign statements acknowledging that they have been trained and understand the security aspects of their systems. Further, SEACATS has audit logs to track the use of the system and as well as permitting periodic reviews for abuse.

The MOUs and Interconnection Security Agreements with other agencies specify security and access privileges. The agreements reflect the scope of protection and use of SEACATS data by third parties (including other agencies) to follow the same privacy protection guidance as DHS personnel. Legacy SEACATS MOUs and Interconnection Security Agreements are being reviewed and updated as necessary in preparation for modernized SEACATS.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

Privacy-related training "Privacy at DHS: Protecting Personal Information" is delivered to all employees that access SEACATS data, including information in any systems that contain data on individuals. This training references the Privacy Act of 1974, and provides guidelines as to the applicability of the law within CBP. In addition, SEACATS users complete annual privacy recertification courses and reference material on privacy-related considerations that relate to their use of the system. If an individual does not complete the required courses, he or she will lose access to all CBP systems covered under the Privacy Act, including SEACATS.

[21] *See* DHS 4300A Sensitive Systems Policy, *available at* https://www.dhs.gov/publication/4300a-sensitive-systems-policy.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

All individuals are given access to SEACATS only after: 1) passing a single-scope background investigation, 2) completing annual privacy recertification courses, 3) being assigned a user profile for the home port area in which they are stationed, and 4) being assigned duties that give them an official need to access the system. All background investigation and training records associated with users who have access to SEACATS are kept in Cornerstone,[22] and routine audits are performed to ensure individuals are not accessing the information without a need-to-know, which is established when access is granted by requiring supervisor approval.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Information sharing agreements and SEACATS MOUs are developed by the SEACATS project team and CBP Privacy Office at the direction of the SEACATS business owner, with input and review by the business owner, impacted SEACATS stakeholders within CBP, and the CBP Office of Chief Counsel. MOUs are signed by the CBP Commissioner and the head of the outside entity. Any new access to the system or new uses of the information requiring SEACATS system changes must be approved by the SEACATS business owner; and assigned as a project for the modernized SEACATS development team. In order to gain user access to the SEACATS information, a user must not only have a need-to-know, but must also have an appropriate background check and completed annual privacy training. A supervisor submits the request to CBP OIT indicating the individual has a need-to-know for official purposes. CBP OIT verifies that the necessary background check and privacy training has been completed prior to issuing a new internal user account. Internal user accounts are reviewed annually to ensure that these standards are maintained. These rules also require a periodic assessment of technical, administrative, and managerial controls to enhance data integrity and accountability. System users must sign statements acknowledging that they have been trained and understand the security aspects of their systems. Further, SEACATS has audit logs to track the use of the system and as well as permitting periodic reviews for abuse.

The legacy SEACATS MOUs and Interconnection Security Agreements with other agencies specify security and access privileges. The agreements reflect the scope of protection and use of SEACATS data by third parties (including other agencies) to follow the same privacy

[22] *See* DHS/CBP/PIA-038 Cornerstone (February 27, 2017), *available at* https://www.dhs.gov/publication/dhscbppia-038-cornerstone.

protection guidance as DHS personnel. Procedures for the sharing of information are detailed in the system security plan (SP) and in the Interconnection Security Agreement as defined in DHS 4300A. The Interconnection Security Agreement and SP are documented and maintained by the system Information System Security Officer (ISSO). Interconnection Security Agreements and SPs are approved by the Deputy Assistant Commissioner for CBP. No PII data is transferred to agencies outside of DHS without proper approval or except as agreed upon in an information sharing arrangement.

Responsible Officials

Dennis McKenzie
SEACATS Business Owner
U.S. Customs and Border Protection
Department of Homeland Security

Debra L. Danisek
CBP Privacy Officer
U.S. Customs and Border Protection
Department of Homeland Security

Approval Signature

Original, signed version on file at the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security