Privacy Impact Assessment
for the

# Regulatory Management Information System (RAMIS)

## DHS/CBP/PIA-028

## March 14, 2016


**Contact Point**
**Mark Ziner**
**Director**
**Office of International Trade**
**U.S. Customs and Border Protection**
**(202) 863-6106**

**Reviewing Official**
**Karen L. Neuman**
**Chief Privacy Officer**
**Department of Homeland Security**
**(202) 343-1717**

# Abstract

The Department of Homeland Security, U.S. Customs and Border Protection (CBP), Office of International Trade uses the Regulatory Management Information System (RAMIS) to conduct post-entry regulatory audits of importers, brokers, and other parties involved in international trade activities. Its associated repository, the Regulatory Audit Archive System (RAAS) stores completed audit documentation and reports compiled by RAMIS. These audits enable revenue collection, facilitate legitimate trade, provide a compliance framework to the trade community, and deter future trade violations. CBP is conducting this PIA because this system collects personally identifiable information about members of the public.

# Overview

CBP safeguards the United States and its borders by fostering economic security through lawful international trade and travel. RAMIS collects and maintains audit plans and records, which may include personally identifiable information (PII) on importers, brokers, and others subject to regulatory audits related to merchandise entry and revenue management. Pursuant to its authorities for Examining Books and Witnesses[1] and regulating Customs Brokers,[2] CBP conducts oversight activities, including audits on importers, brokers, airlines, carriers, freight forwarders, bonded warehouses, foreign trade zones, duty free establishments, and other entities engaged in international trade. CBP responds operationally to referrals from U.S. Immigration & Customs Enforcement (ICE) regarding fraud investigations and assists the Department of Justice (DOJ) in prosecuting cases involving the False Claims Act.[3]

***The Regulatory Audit Framework:***

CBP uses its National Annual Audit Plan (NAAP) to conduct assessments on importers, custom brokers, or others engaged in international trade. NAAP uses statistical principles from the Quantitative Risk Assessment Method (QRAM)[4] to determine risks[5] associated with entities engaged in international trade in order to minimize non-compliance that results in loss or harm to the U.S. Government, domestic industries, or the public. CBP uses these risk determinations, additional audit criteria, and referrals to select audit candidates for a particular year. The audit criteria and types of referrals that may determine an audit candidate may include:

[1] *See* 19 U.S.C. § 1509.
[2] *See* 19 U.S.C. § 1641.
[3] *See* 31 U.S.C. § 3729.
[4] Quantified Risk Assessment Methodology, or "QRAM," identifies audit candidates by ranking companies based on multiple risk factors uncovered over the past five years of auditing major importers.
[5] Risks may include product safety, merchandise value discrepancies, or other trade-related concerns.

- Importers with an entered value of over $10 million;
- Importers not subjected to an audit in the previous five years;
- Importers not conducting Importer Self-Assessments;
- Audits conducted in association with criminal, civil, or intelligence investigations;
- Referrals by CBP's Office of Field Operations pertaining but not limited to fraud, agricultural issues, and import safety;
- Referrals of Textile Transshipments;[6]
- Referrals by the Transportation Security Administration (TSA) for user fee concerns; and
- Referrals by ICE pertaining to fraud, money laundering, and immigration cases.

CBP may audit records pertaining to a single year or multiple years based on the circumstances surrounding the audit. Companies do not have the option to opt out of an audit, but maintain the right to dispute the results and formally address the audit's recommendations. QRAM contains CBP historical importer information extracted from the Automated Commercial Environment system (ACE).[7]

***RAMIS and its Supporting Systems:***

RAMIS generates the preliminary audit plan that leads to the final, published NAAP. CBP compares audit accomplishments against the final NAAP. RAMIS generates a variety of reports during the audit life cycle, including importer information, audit status, report status, findings, recommendations, and CBP staff hours expended. RAMIS also provides strategic analysis on audit results.

RAMIS stores completed audit documentation and reports and allows CBP employees and contractors to query completed audit assignments and associated documentation.

ACE serves as the primary data source for RAMIS. ACE provides limited importer information, contact information, and limited trade-related PII. The PII includes employee identification numbers (EIN), also known as Federal Taxpayer Identifying Numbers (*See* Section 2.3). In certain instances, importers that do not have an EIN may submit Social Security numbers (SSN)[8] pursuant to federal regulations requiring importer filing identification numbers.[9] Although

[6] Transshipment is the movement of goods through a second country en-route to the United States.
[7] DHS/CBP/PIA-003(a), Automated Commercial Environment (ACE), available at: http://www.dhs.gov/sites/default/files/publications/privacy-piaupdate-cbp-ace-july2015.pdf.
[8] *See* E.O. 13478.
[9] See 19 CFR § 24.5.

RAMIS contains EINs or SSNs submitted to ACE during the merchandise entry process, the reports generated in both systems do not contain EINs or SSNs.

## 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 and regulations pursuant to:

- Trade and Customs Revenue Functions of the Department of Homeland Security;[10]
- Tariff Act of 1930, *as amended*;[11]
- Penalties for Fraud, Gross Negligence, and Negligence;[12]
- False Claims Act;[13]
- Ascertainment, Collection, and Recovery of Duties;[14]
- Licensing of Customs Brokers;[15]
- Identifying Numbers;[16]
- Customs Financial and Accounting Procedures;[17]
- Importer Security Filing Data Elements;[18] and
- Office of Management and Budget (OMB) Circular A-50 Revised (Audit Follow-up) of September 29, 1982.[19]

[10] *See* 6 U.S.C. §§ 115(a)(1) and 212(b)(2).
[11] *See* 19 U.S.C. Chapter 4.
[12] *See* 19 U.S.C. § 1592.
[13] *See* 31 U.S.C. § 3729.
[14] *See* 19 U.S.C. §§ 1481 – 1529.
[15] See 19 U.S.C. § 1641.
[16] *See* 31 U.S.C. § 7701(c).
[17] *See* 19 CFR Part 24.
[18] *See* 19 CFR Part 149.3
[19] OMB Circular A-50 Revised. Available at: https://www.whitehouse.gov/omb/circulars_a050/.

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

Information maintained within RAMIS is covered by the following SORNs:

- DHS/CBP-014 Regulatory Audit Archive System (RAAS) System of Records and corresponding Final Rule for Privacy Act Exemptions, Regulatory Audit Archive System (RAAS).[20]

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

Yes. RAMIS received an extended Authority to Operate (ATO) on June 19, 2015, and receives a full ATO upon publication of this PIA.

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

Yes. CBP maintains regulatory audit records in accordance with N1-36-86-1 approved by NARA on November 9, 1989. CBP maintains regulatory reports and company findings on-site for one year and then transfers the records to the Federal Records Center (FRC), which destroys the records after ten (10) years. CBP maintains regulatory audit subject records on-site for one year and transfers the files to the FRC, which destroys the records after three years.

### 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.

Not applicable. RAMIS does not collect information directly from individuals or place additional administrative burdens on members of the public.

## Section 2.0 Characterization of the Information

[20] DHS/CBP-014 Regulatory Audit Archive System (RAAS) System of Records, 73 FR 77807 (December 19, 2008). Available at: http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29846.htm. An update of this SORN will be published contemporaneously with the posting of this PIA. Implementation of Exemptions; DHS-CBP-014 RAAS SORN NPRM, 74 FR 45076 (August 31, 2009). Available at: http://www.gpo.gov/fdsys/pkg/FR-2009-08-31/html/E9-20751.htm. An update of this rule will be published contemporaneously with the posting of this PIA.

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

RAMIS obtains information from the following individuals:

Audit Subjects (obtained from ACE):

- Company or individual names, including names of officers of customs broker firms or other business entities engaged in international trade or associated with the scope of the audit;
- Contact information (business address, home address for individuals, phone number, and email address);
- EINs and SSNs (Taxpayer Identifying Numbers);
- Importer of Record (IR) Number;
- License and permit numbers, dates issued, and district or port covered; and
- Dun and Bradstreet, Inc. Data Universal Numbering System (DUNS) numbers.[21]

CBP Employee and Contractor Information:

- User name/ID;
- Password information;
- Email address; and
- Phone number.

Information Obtained and Maintained By the Office of Trade Audit Team:

- Audit reports of subject accounts and records;
- Business records associated with the audit;
- Correspondence with the subject of the audits;
- Congressional inquiries concerning customs brokers or other audit subjects and disposition made of such inquiries;
- Internal audit life-cycle data and CBP personnel work-hours expended information for a particular audit;

[21] *See* http://fedgov.dnb.com/webform/pages/dunsnumber.jsp.

- Records (including the results) related to investigatory referrals to ICE that are not part of a Grand Jury; and
- Ongoing and final audit reports (which may contain PII).

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

The ACE/RAMIS interface allows RAMIS users to query current information (listed above under "Audit Subjects") associated with a forthcoming audit. RAMIS also obtains data during the regulatory audit process from in-person interviews with importers, brokers, airlines, carriers, freight forwarders, bonded warehouses, foreign trade zones, duty free establishments, and other entities engaged in international trade.

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

RAMIS may receive publicly available data once ACE obtains corporate information and DUNS numbers from Dun & Bradstreet, Inc. CBP uses this information to verify the legitimacy of businesses associated with merchandise entry or international trade.

## 2.4 Discuss how accuracy of the data is ensured.

RAMIS inherits the information listed above under "Audit Subjects" from ACE. In addition to procedures and safeguards to address data accuracy within the ACE population, CBP may obtain information directly from the audit subject through in-person interviews or collaborate with ACE data managers to correct the original dataset.

Although RAMIS cannot verify data accuracy within the ACE dataset, it uses strict access rules and procedures to restrict access to audit data contained in the system.

## 2.5 Privacy Impact Analysis: Related to Characterization of the Information

**Privacy Risk:** There is a risk that regulatory audits may contain inaccurate information.

**Mitigation:** CBP mitigates this risk by obtaining data directly from entities subjected to the audit or from ACE, the transaction system that collected the trade data from the audit subject. Prior to the data arriving in RAMIS, CBP collects information directly from applicants through Trade Portal Accounts. All importers, or individuals acting on their behalf, must complete training and a CBP certification before they transmit information into ACE. ACE contains parameters that alert the submitter about inaccurate or otherwise inadequate data. Individuals may enter the

information themselves and have the ability to amend all of their submissions. All brokers or other authorized third-party submitters must obtain an ACE certification and receive written authorization from the importer.

# Section 3.0 Uses of the Information

## 3.1 Describe how and why the project uses the information.

***Primary Uses:***

CBP uses the information obtained from audit subjects and ACE to perform post-entry audit planning, tracking, analysis, and reporting. CBP uses RAMIS to select audit candidates using the agency's QRAM risk assessment process to obtain CBP historical shipment entry data from ACE. RAMIS provides tools to manage an audit during its life cycle. In addition to planning and tracking audits, the system generates a variety of reports during each stage of the audit process for risk assessment and research purposes. The reports may include importer information, audit status, report status, revenue collection information, findings, recommendations, and CBP staff hours expended. RAMIS allows authorized CBP personnel to conduct strategic analysis on audit results.

In addition to data obtained from ACE, RAAS stores completed audit documentation and reports. It also serves as a system of records for RAMIS. RAAS allows CBP employees and contractors to query completed audit assignments and associated documentation.

***Residual Uses:***

RAMIS provides year-end data to implement the NAAP-related portion of CBP's Performance and Accountability Report (PAR). The PAR combines CBP's Annual Performance Report with its audited financial statements, assurances on internal control, accountability reporting, and agency assessments. CBP's PAR enables Congress and the public to assess the performance of the agency

RAMIS allows CBP to comply with OMB Circular A-50 (Audit Follow-up) dated September 29, 1982. This compliance capability strengthens CBP's ability to identify and resolve findings, and implement corrective action recommended in audit reports.

### 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.

Yes. RAMIS uses the QRAM risk assessment process to determine risks associated with entities engaged in international trade in order to minimize non-compliance that results in loss or harm to the U. S. Government, domestic industries, or the public. CBP uses these risk determinations to select audit candidates for a particular year. This assessment tool helps identify risks or anomalies that, in many cases, have no nexus to terrorism or criminal activity.

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

No. RAMIS receives entry-related information from ACE and does not share information with other DHS programs or systems. The ACE PIA reflects roles and responsibilities assigned to other DHS Components.

### 3.4 Privacy Impact Analysis: Related to the Uses of Information

**Privacy Risk**: There is a risk that information could be used in a manner inconsistent with the purpose of collection.

**Mitigation**: CBP mitigates this risk with administrative, technical, and physical security controls that place limitations on PII collection and protect PII against unauthorized disclosure, use, modification, or destruction. One mitigation mechanism includes assigning user rights based on the individual's role within the regulatory audit process. For example, RAMIS program managers assign master administrators to control access to the system. Master administrators restrict access to individuals who have assigned regulatory audit projects. Users do not have administrative rights over their assigned projects. Master administrators provide similar restrictions on audit executive users. These users receive restricted, read-only access in order to monitor audit progress, compliance, and risk levels. Additionally, all system users receive annual privacy training. ACE users receive system specific training.

**Privacy Risk**: There is a risk that the automated QRAM risk assessment process may lead to audits conducted on entities that may not warrant such an assessment.

**Mitigation**: CBP mitigates this risk by conducting thorough post-selection staff reviews of the NAAP and submitting the annual plan to CBP Executive Management for review and final approval prior to NAAP implementation. No actions are taken based solely on automated risk assessments.

# 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.

CBP provides notice through a Federal Register general notice[22] and a webpage page related to Importer Self-Assessments. This PIA's publication serves as notice by providing awareness of how CBP uses, disseminates, and retains RAMIS information. The RAAS SORN as amended and published in the Federal Register serves as additional notice.

The ACE PIA and SORN provide notice by describing the scope of information collected by CBP during trade processing activities.

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

Since RAMIS data originates primarily from ACE, there are no opportunities for individuals to consent to uses, decline to provide information, or opt out of the collection. Regarding the data contained in ACE, U.S. law requires importers to provide CBP information that contains PII in conjunction with submitted commercial entry documents needed to import commodities or merchandise in to or transit through the United States. Importer identity, manufacturer or supplier, and other parties involved in the import transaction and supply chain are necessary for commercial entry acceptance. Failure to provide required information results in rejection of the commercial entry and CBP issuing an order to remove the commodity from the territory of the United States. When importers submit the required information to ACE, they fulfill their legal requirements and provide consent to how CBP uses the data.

## 4.3 Privacy Impact Analysis: Related to Notice

**Privacy Risk:** There is a risk that importers or their representatives may not know that CBP uses ACE data to facilitate the regulatory audit process.

**Mitigation:** CBP mitigates this risk to the extent possible through its Federal Register general notice and Internet page related to Importer Self-Assessments and the Regulatory Audit website.[23] It further mitigates this risk by publishing this PIA to inform audit subjects about the

[22] CBP Importer-Self-Assessment Program General Notice and Website. Available at: https://www.federalregister.gov/articles/2002/06/17/02-15308/importer-self-assessment-program *and* http://www.cbp.gov/trade/programs-administration/importer-self-assessment.
[23] CBP Audits/Regulatory Audits Website. Available at: http://www.cbp.gov/trade/programs-administration/audits.

data's origin. It also mitigates this risk by providing notice through an update to the RAAS SORN's Category of Records in the System that now includes additional corporate information, EIN/Taxpayer Identification Number, and SSNs collected from ACE.

# Section 5.0 Data Retention by the project

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

CBP maintains regulatory reports and company findings on-site for one year and then transfers the records to the FRC, which destroys the records after ten (10) years. CBP maintains regulatory audit subject records on-site for one year and transfers the files to the FRC, which destroys the records after three years. The agency destroys records pertaining to company formation and organization, by laws, identity of officers, minutes of board of directors meetings, and other records after they are no longer needed for administrative purposes.

CBP manages ACE data in accordance with NARA-approved records retention schedules associated with that system.

## 5.2 Privacy Impact Analysis: Related to Retention

**Privacy Risk:** There is a risk that RAMIS managers may retain data longer than the approved RAMIS retention schedule to accommodate ACE-specific records schedules.

**Mitigation:** CBP mitigates this risk by directing RAMIS managers to follow NARA-approved records retention schedules specific to regulatory audit processing, which are shorter in duration than those assigned to ACE. This risk is inherent in federal records retention when different parts of an agency may have differing needs for the information. Regulatory audit data retention schedules are aligned with the purpose and mission of the agency, and permit RAMIS to manually delete information after ten years, protecting PII by reducing the proliferation of the data.

# 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.

Although CBP responds to requests for referrals of information from the Department of Justice (DOJ) to aid in prosecuting cases involving the False Claims Act, RAMIS is a self-contained internal system that normally does not share information with other DHS or non-DHS

programs or systems. RAMIS may share information with external agencies in accordance with the Privacy Act, 5 USC 552(a), pursuant to the routine uses set forth in DHS/CBP-014, Regulatory Audit Archive System of Records (RAAS).[24]

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

As noted above, PII is typically not disclosed outside of CBP since the agency conducts its own regulatory audit activities. However, CBP is permitted to disclose information to external entities consistent with its regulatory audit mission and pursuant to the following Routine Uses:

Routine Use D of DHS/CBP-014 RAAS SORN allows DHS to disclose information with an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

Routine Use G of DHS/CBP-014 RAAS SORN allows DHS to disclose information with federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where DHS determines that the information would assist in the enforcement of civil or criminal laws.

### 6.3 Does the project place limitations on re-dissemination?

Yes. As a condition of sharing information pursuant to a routine use in the RAAS SORN, CBP requires anyone that receives non-public RAMIS data to obtain written permission from CBP before re-disseminating the information.

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

To obtain RAMIS information, the requesting party must submit a written request for specific information and state how it plans to use the information in relation to regulatory audits or an investigatory matter. CBP retains a copy of this request and submits it to the CBP Privacy Office for review. Once the CBP Privacy Office reviews the request, based on the circumstances of each case, a CBP Privacy official drafts an authorization memorandum specific to each case.

[24] DHS/CBP-014 - Regulatory Audit Archive System (RAAS) System of Records, 73 FR 77807 (December 19, 2008). Available at: http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29846.htm. An update of this SORN will be published contemporaneously with the posting of this PIA.

CBP retains a copy of the memorandum. If the disclosure is approved, CBP also maintains a record of the disclosure using DHS Form 191.

### 6.5 Privacy Impact Analysis: Related to Information Sharing

**Privacy Risk:** There is a risk that information will be shared with external entities for purposes that are beyond the regulatory audit process.

**Mitigation:** CBP has procedures to ensure that all external sharing follows CBP policies and procedures. All requesting parties must submit a written request for specific information from RAMIS and state how they plan to use the information in relation to regulatory audits or an investigatory matter. CBP retains a copy of this request and submits it to the CBP Privacy Office for review. Once the CBP Privacy Office reviews the request, based on the circumstances of each case, a CBP Privacy official drafts an authorization memorandum specific to each case. CBP retains a copy of the memorandum. If the disclosure is approved, CBP also maintains a record of the disclosure using DHS Form 191.

## Section 7.0 Redress

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

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, DHS/CBP will consider individual requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the DHS Chief Freedom of Information Act (FOIA) Officer or CBP's FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contacts." Individuals may also submit a request via FOIA-Online.[25] If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0655, Washington, D.C. 20528.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 6 C.F.R. Part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your

[25] *See*: https://foiaonline.regulations.gov/foia/action/public/home.

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 your inquiry requires no specific form, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, you should:

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

Procedures for accessing data contained in ACE can be found it the ACE PIA and its associated SORN.

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

Data contained in RAMIS originate primarily from ACE. Individuals that file information electronically may amend, correct, or cancel their active data in ACE. ACE performs nightly updates, but RAMIS retrieves the data on a weekly basis. Individuals may also follow the procedures in section 7.1 above or contact the ACE Client Representative Division below to request CBP correct erroneous ACE information:

Director, Client Rep Division
ACE Business Office, Office of International Trade
U.S. Customs and Border Protection
8444 Terminal Road
Beauregard A-312-5
Lorton, Virginia 22079

Individuals may also notify CBP or their Account Managers regarding incorrect or inaccurate information in ACE, and may send correction requests to:

U.S. Customs and Border Protection
CBP Information Center
Office of Public Affairs
1300 Pennsylvania Avenue
Washington, D.C. 20229

Although requests to amend information should be made in writing, individuals may contact the CBP INFO Center by phone at (877) 227-5511 or (703) 526-4200. Following the links on https://help.cbp.gov/app/home/search/1, individuals may submit complaints online.

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

Individuals may contact the CBP INFO Center[26] to obtain guidance for requesting correction of their information. This PIA, the ACE PIA and SORN, www.cbp.gov, and the Regulatory Audit Field Office website[27] provides contact information for making those requests. Within ACE, individuals who submit information electronically are notified of the procedures for correcting their information in the electronic user guides and during the training process.

## 7.4 Privacy Impact Analysis: Related to Redress

**Privacy Risk:** There is a privacy risk that RAMIS is unable to correct information since it relies on underlying ACE system information.

**Mitigation:** CBP mitigates this risk by providing individuals the opportunity to correct their information either directly by accessing the source ACE system or through the measures stated throughout this PIA, associated SORNs, and associated websites. CBP further mitigates this risk by limiting the amount of information used within the regulatory audit program from ACE, therefore alleviating the need to correct data directly in RAMIS or RAAS. Furthermore, when the electronic system encounters a possible error with the transmitted data, it issues a response message alerting the individual that he or she may need to correct the information. Otherwise, individuals may submit a Privacy Act request as described in section 7.1.

[26] CBP INFO Center Website. Available at: https://help.cbp.gov/.
[27] Regulatory Audit Field Office Website. Available at: http://www.cbp.gov/trade/audits/field-offices.

# 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?

RAMIS master administrators create and manage all accounts, conduct technical modifications, and employ audit trails that maintain a record of system and individual user activity. They create individual accounts at the request of Regulatory Audit program managers. The system employs role-based access controls that limit the access of information by different users and administrators based on the need to know the information for the performance of their official duties. CBP also employs processes to enforce separation of duties, to prevent unauthorized disclosure, or to prevent modification of information. No unauthorized users are permitted access to system resources. RAMIS system access control procedures adhere strictly to the DHS Sensitive Systems Policy Directive 4300A[28] and CBP's internal information system security policies.

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

RAMIS users are required to take annual privacy, information security, and safeguarding national security information training prior to gaining and/or retaining access to the systems. ACE users take system-specific training prior to gaining access. RAMIS, RAAS, and ACE program managers maintain a master list of all users and whether they have completed privacy and security training. If a user fails to complete the training by the annual deadline, then he or she loses access to the systems.

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

CBP Regulatory Audit program managers employ master administrators that control access to the RAMIS systems. A potential user's supervisor submits a request to regulatory audit program managers, and upon approval, transmit that request to a master administrator. Both the potential user's supervisor and the program manager determine whether the individual has a "need to know" basis for access to RAMIS. After approval from the program manager, the master administrator only grants access to users once they receive an assigned audit project through the NAAP.

Additional access controls restrict audit executives to read-only access, which allows them to monitor progress, compliance, and risk levels within a particular audit. Regulatory audit

[28] DHS 4300A. Available at: http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf.

program managers further restrict access to the systems by establishing specific roles and responsibilities, such as: Headquarters Manager, Field Director, Assistant Field Director, Program Manager, Time Keeper, and Auditor. CBP conducts audits in accordance with DHS Information Security guidelines.

### 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?

All information sharing and MOUs concerning PII sharing, including those related to RAMIS, are created by the operational owner of the system and are sent to the CBP Privacy Officer and Office of Chief Counsel for review and to the DHS Privacy Office for final concurrence before approval and signing.

## Responsible Officials

Mark Ziner
Director, Office of International Trade
U.S. Customs and Border Protection
Department of Homeland Security

John Connors
CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection
Department of Homeland Security

## Approval Signature

Original signed copy on file with DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security