Privacy Impact Assessment
for the

Coastal Surveillance System (CSS)

DHS/S&T/PIA-033

October 10, 2018

Contact Point
Joe A. Campillo
CSS System Owner
Science and Technology Directorate
(540) 653-0843

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has launched the Coastal Surveillance System (CSS) Pilot program. CSS is a technology demonstration project that establishes a framework (data standards and interfaces) for authorized sharing of data between DHS Components and partners. CSS allows authorized personnel to access information collected by other maritime law enforcement, safety, and security programs. S&T is submitting this Privacy Impact Assessment (PIA) because CSS collects, maintains, and shares personally identifiable information (PII) from other systems.

Overview

The purpose of the Department of Homeland Security (DHS) Science and Technology (S&T) Coastal Surveillance System (CSS) Pilot program is to improve the collection and authorized sharing of maritime law enforcement, safety, and security data. CSS implements a framework for real time information sharing that provides greater visibility across DHS component agencies and their partners of coastal and maritime activities, while enabling data source system owners to control the dissemination of data to protect the privacy of individuals.

CSS is a platform that subscribes to data sources ("feeds") from other partner systems and acts as a bridge, redistributing data to vetted and authorized users in accordance with the sharing policy of the originating system owner. CSS feeds include radar and video sensors; self-reported vessel information via the USCG Automatic Identification System (AIS)[1] and Ship Arrival Notification System (SANS);[2] and law enforcement database information. The type, location, and scope of the data can be customized for each partner agency. This allows maritime law enforcement, safety, and security partners to create a comprehensive, and user defined, operating picture. CSS does not determine the placement of sensors or cameras from source systems, or the data that they collect.

CSS users use their individual operating picture to aid in identifying and dismissing benign vessels and investigating vessels that appear to be engaging in suspicious activity. CSS does this by enabling partners to easily access and compare sensor and other operational data that was once isolated within participating agencies. Vessel data and other PII is not immediately displayed in a

[1] AIS is a cooperative vessel tracking system whereby vessels transmit their position, identification, speed, course, cargo type and other information to other vessels in their area and to shore-based receivers within range of the vessel transmitters. *See* DHS/USCG/PIA-006 Vessel Requirements of Notices of Arrival and Departure (NOAD) and Automatic Identification System, *available at* www.dhs.gov/privacy.

[2] The USCG Ship Arrival Notification System (SANS) provides a centralized repository for Notice of Arrival/Departure (NOA/D) information for maritime vessels entering U.S. ports. *See* DHS/USCG/PIA-005 United States Coast Guard Maritime Awareness Global Network (MAGNET) and DHS/USCG/PIA-006 Vessel Requirements of NOAD and Automatic Identification System, *available at* www.dhs.gov/privacy.

CSS user's operating picture, but it can be pulled from AIS or SANS if necessary to further an investigation or create a fuller picture of the situation.

CSS is a joint effort by S&T, the U.S. Coast Guard (USCG), and the U.S. Customs and Border Protection (CBP) Air and Marine Operations Center (AMOC). Data sources in CSS are currently owned by the USCG, CBP, U.S. Immigration and Customs Enforcement (ICE), the Office of the Director of National Intelligence (ODNI) National Maritime Intelligence-Integration Office (NMIO), and the Maryland Natural Resources Police (MNRP). Data source system owners will henceforth be referred to as System Owners. CSS will continue to integrate with other federal and non-federal systems containing law enforcement, security, sensor, and screening information and analysis capabilities. These systems contain sensor data from radar and imagers (*e.g.*, infrared and visible cameras), and are used to communicate maritime vessel alerts based on data correlation and analysis.

The DHS Office of the Chief Information Officer's (OCIO) Information Sharing and Services Office (IS2O) provides the system access identification and authentication (identity management) through the Homeland Security Information Network (HSIN).[3] CSS will work with OCIO IS2O to implement two-factor authentication and a controlled set of user and data attributes to ensure secure and appropriate authorized access for the federal, state, local, tribal, international, public, and private (FSLTIPP) partners. The originating system owner maintains the role of lifecycle manager of the data. Data within CSS is typically kept for a short duration (30 days or less) to support viewing by authorized users for the purpose of shared situational awareness of maritime activities. All systems that CSS shares data with have a signed Interconnection Security Agreement (ISA) and all information sharing policy implementation within CSS is owned and managed by the source owner.

HSIN is the identity provider and a HSIN account is required to gain access to CSS.[4] CSS users are sponsored into HSIN regional or national Communities of Interest (COI) by federal security, safety, and law enforcement personnel. Data access within CSS is determined by HSIN COI membership, (which is organized by geographic region) and other user attributes (*i.e.*, organization and job duties). Validated encryption and access to the system web server is protected by requiring users to authenticate through an identity management service (HSIN), as well use as a valid user name and password.

CSS follows the National Institute of Standards and Technology's (NIST) Special Publication 800-37 "Risk Management Framework (RMF) to Federal Information Systems a

[3] HSIN is the trusted network for homeland security mission operations to share Sensitive But Unclassified information. Federal, state, local, territorial, tribal, international, and private sector homeland security partners use HSIN to manage operations, analyze data, and send alerts and notices. *See* DHS/ALL/PIA-061-3 Homeland Security Information Network Sensitive But Unclassified *available at* www.dhs.gov/privacy.
[4] *See* Appendix B of DHS/ALL/PIA-061-1 R3 HSIN User Accounts, *available at* https://www.dhs.gov/privacy.

Security Life Cycle Approach," and complies with the DHS Sensitive Systems Policy Directive 4300A information security and privacy requirements.[5]

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?

CSS is governed by Sections 303-313 of Public Law 107-296, "Homeland Security Act of 2002 (The Act)" Title VIII, sub title I, "Homeland Security Information Sharing Act," which states that, "It is the sense of Congress that Federal, state, and local entities should share homeland security information to the maximum extent practicable, with special emphasis on hard-to-reach urban and rural communities." CSS delivers a prototype of this capability. DHS Management Directive (MD) 10100.1, "Organization of the Office of The Under Secretary For Science And Technology", section "H. Division Head, Borders and Maritime Security Division (BMD)." CSS establishes a demonstration prototype system for the purpose of sharing Unclassified For Official Use Only (U//FOUO) data. PII provided to CSS by data owners is in compliance with those organizations legal authorities. All data ingested into CSS is governed by an ISA in which the data owner agrees to manage the sharing of their data using CSS provided security controls, in accordance with their organization's legal authorities, regulations, and policies.

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

The below DHS Component SORNs apply to the source system data in CSS:

- DHS/CBP-019 Air and Marine Operations Surveillance System (AMOSS);[6]
- DHS/USCG-013 Marine Information for Safety and Law Enforcement (MISLE);[7]
- DHS/USCG-029 Notice of Arrival and Departure (NOAD);[8]
- DHS/USCG-061 Maritime Awareness Global Network (MAGNET);[9] and
- DHS/ICE-009 External Investigations.[10]

[5] *See* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.
[6] DHS/CBP-019 Air and Marine Operations Surveillance System (AMOSS) System of Records Notice, 78 FR 57402 (September 18, 2013).
[7] DHS/USCG-013 Marine Information for Safety and Law Enforcement (MISLE), 74 FR 30305 (June 25, 2009).
[8] DHS/USCG-029 Notice of Arrival and Departure System of Records, 82 FR 32715 (July 17, 2017).
[9] DHS/USCG-061 Maritime Awareness Global Network (MAGNET), 73 FR 28143 (May 15, 2008).
[10] DHS/ICE-009 External Investigations 75 FR 404 (January 5, 2010).

The following SORN covers the user information required to gain access to CSS:

- DHS/ALL-037 E-Authentication Records.[11]

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

CSS is operating under a Security Authorization Decision (Authorization To Operate - ATO) signed May 11, 2016. The Security Authorization Package consists of the Security Plan (SP); Security Assessment Report (SAR); and Plan of Action and Milestones (POA&M).

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

CSS follows DHS records retention schedules, as documented in General Records Schedule (GRS) 5.2, Item 20, which covers the operational data on the CSS platform as intermediary records. Under the GRS, the records must be destroyed when no longer needed for business use. S&T also collects data from CSS for testing and evaluation purposes. S&T abides by GRS 3.1, item 11, which cover test files, data, and evaluation. Test and Evaluation files are considered temporary and cut off at the end of the calendar year after completion or cancellation of a project. All records are then destroyed or deleted five years after cutoff or one year after responsible office determines it is no longer needed for legal, audit, administrative, or business purposes. Information Technology (IT) Security files are retained in the DHS Information Assurance Compliance System (IACS). The retention schedule is implemented by the Homeland Security Advanced Research Projects Agency (HSARPA) BMD, which is approved by the NARA. Data owners will follow their agency's previously established records schedules for source system records.

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.

CSS does not meet the requirements of the PRA as it does not collect information directly from the public.

[11] DHS/ALL-037 E-Authentication Records System of Records, 79 FR 46857 (August 11, 2014).

Section 2.0 Characterization of the Information

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

CSS operates as a "pipeline" with a data cache (temporary storage). CSS passes the data from one system to another system, caching it for up to 30 days. CSS is a framework for the distribution of data from other systems in accordance with the data owners' data sharing policies in compliance with U.S. law and regulation. Privacy-sensitive information is collected from existing systems and then distributed within CSS. For a listing of interconnected data source systems by data type refer to Appendix A.

Data from USCG AIS

AIS is a USCG data source that is an automatic tracking system used on ships. AIS data distributed through CSS includes:

- Vessel identification and registration data;
- Nationality of the vessel (where the vessel is registered);
- The vessel's Maritime Mobile Service Identity (MMSI) – a unique nine-digit identification number;
- International Maritime Organization (IMO) ship identification number – a seven-digit number that remains unchanged upon transfer of the ship's registration to another country;
- Radio call sign – international radio call sign, up to seven characters, assigned to the vessel by its country of registry; and
- Vessel Name – 20 characters to represent the name of the vessel.

Video Data

Video data includes information captured by cameras, such as the vessel name/vessel identifying flag and may include PII and/or sensitive personal information on visible personnel. It could also include information on individuals that happen to be present when the video was taken. Video collected shall be image-only videos from safety[12], security, law enforcement,[13] and covert investigative surveillance solutions.

[12] For more information *see* USCG Ports and Waterways Safety System (PAWSS) *available at https://www.navcen.uscg.gov/?pageName=vtsPAWSS*.
[13] For more information *see* http://news.maryland.gov/dnr/2014/05/21/nrp-wins-award-for-state-of-the-art-enforcement-tool/

Radar Data

Radar data collection includes object-detection using radio waves to determine the position, range, angle, or velocity of aircraft and vessel. Radar data alone cannot identify personnel or vessels. Applications include translating data into a usable format for geo-fencing[14] sites designated as critical. CSS aggregates disparate coastal maritime radar sensors to:

- Maintain awareness of vessel activities in U.S. Ports and coastal waters
- Identify, characterize, and verify vessel identification
- Collaboratively share maritime domain awareness
- Determine vessel movement, past history, and current location

User/Account Information

CSS uses the HSIN system as the identity and access management provider. CSS uses the below fields from HSIN to authenticate users:

- First name
- Middle initial;
- Last name; and
- Email address.

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

CSS does not receive information directly from individuals. The information is collected by the source systems listed in Appendix A. Data provided to CSS is essential for overall situational awareness. These systems provide sensor data and law enforcement database information. The information is collected for temporary use (usually not in excess of 30 days) in maintaining situational awareness and law enforcement and security operations support.

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

The system provides links to publicly available websites for reference (such as vessel data from www.marinetraffic.com and www.shipspotting.com), but the content of the website is not processed or stored by the system. If a user clicked on the link, another browser window opens.

[14] Geo-fencing is placing a virtual perimeter around a geographic location, usually through the use of the global positioning system.

These sites include open source vessel statistics, voyage information, position, call sign, MMSI number, IMO number, and pictures.

2.4 Discuss how accuracy of the data is ensured.

CSS relies upon the source systems' data owners to ensure the accuracy of the data it collects. CSS does not allow CSS users to change the source data. CSS users can update or correct data within the CSS system, but the source data remains unaltered. CSS subscribes to source data, including updates. The data owners are responsible for data integrity. Operational security, safety, and law enforcement personnel using CSS follow their agencies established procedures governing the use of the data.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: CSS may contain inaccurate information presented to users for overall situational awareness in support of law enforcement, security, and safety operations.

Mitigation: The risk is not fully mitigated. The types of data available in the demonstration system are generated by sensors or self-reported via AIS. CSS does not modify source data, but CSS users can update or correct data within the CSS system. CSS is an information broker only. CSS is developing concepts and technologies to enable data quality enhancement through publishing changes and corrections to the data sources' systems.

Privacy Risk: CSS may collect data that is not relevant to law enforcement, security, and safety operations missions.

Mitigation: Information is collected under the law enforcement authorities of the data owners for temporary use. Data Owners determine and provide data that only is directly relevant and necessary in maintaining situational awareness in support of law enforcement, security, and safety operations. Data is only retained for up to 30 days.

Section 3.0 Uses of the Information.

3.1 Describe how and why the project uses the information.

CSS enables DHS and partner law enforcement, security, and safety organizations to share and access maritime vessel information (*e.g.*, itinerary, position, and imagery) to enhance situational awareness for security, safety, and law enforcement purposes.

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.

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

CSS's mission is to enable inter and intra-Departmental sharing of information. Assigned roles and responsibilities include Users, COI Manager, Feed Administrators, Entitlement Administrators, and Node Administrators.

Users include Law Enforcement, Safety, and Security personnel across the FSLTIPP spectrum. They are able to view data provided by partner systems in accordance with Data Owner policy.

COI Managers control access to Communities of Interest based upon Geographic or Administrative Boundaries. DHS Components can have this role. COI membership is managed by HSIN, which provides Identification and Authentication, and attribute management for CSS Authorization decisions.

Data Owners providing data to CSS are assigned the **Feed Administrator** role. They implement data sharing controls for their data. All data sharing controls are governed by ISA and/or Approval To Test (ATT) documents.

Entitlement Administrator and **Node (System) Administrator** roles are performed by the DHS S&T CSS Program Management Office (PMO). Entitlement Administrators provide Subject Matter Expertise to data owners to support correct configuration of sharing policies. Node Administrators ensure users and user attributes are set up per the approved user form.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: CSS users may gain access to information for which they are not authorized. This may happen as a result of improper policy implementation, improper user attribute vetting, or improper escalation of privileges or similar type of vulnerability.

Mitigation: CSS mitigates this risks through several factors: Attribute Based Access Control (ABAC) and associated sharing policies, referred hereafter as CSS entitlement, restrict access to data based on the source Data Owners' policies. Policies enforce Geographic distribution, intended uses, and authorized users of the data. CSS protects PII (in all forms) through entitlements, using ABAC to implement associated system owner sharing policies that maximize

information sharing while controlling or eliminating risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. The default CSS policy is to deny sharing; a system owner must explicitly share data to users possessing a specific attribute or set of attributes.

System Owners are currently trained in building and implementing policies in accordance with industry and system best practices by program Subject Matter Experts in the role of Entitlement Administrators. Audit functions identify and track data use, allowing information security staff to identify and minimize improper access to data.

CSS COI Managers and Node Administrators are responsible for ensuring User Attributes are properly assigned and vetted. The assigned attributes are reviewed on a yearly basis along with every user account. As more attributes are moved to and managed in HSIN, the ability to manage attributes will lie with the appropriate authority (COI Manager, System Owner (for system specific attributes), employer (organization, position), etc.).

CSS software source code is reviewed for vulnerabilities prior to installation, following industry best practice and Government requirements. Any issues are remediated prior to installation or update.

Privacy Risk: CSS users may use information beyond the purpose of its original collection.

Mitigation: CSS users and administrators are held accountable for the protection of PII. All CSS users receive training for their system user role and the acceptable use of the rights/privileges associated with their user role. All users complete, sign, and agree to the General User Agreement Request (GUAR) form and General User Rules of Behavior (ROB). Privileged Users complete, sign, and agree to the Privileged Account Request (PAR) form and Privileged Account ROB. All DHS personnel are required to complete privacy training. This includes CSS users, data owners, and systems administrators. CSS audits access to PII in compliance with privacy principles and all applicable privacy protection requirements.

All CSS users undergo a DHS Background Investigation and receive an Enter On Duty (EOD) and Favorable Suitability Decision as condition for access to CSS.

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.

CSS does not collect information directly from individuals, and therefore cannot provide individuals notice. CSS ingests and aggregates data from the source systems listed in Appendix A.

CSS is reliant upon the source systems' owners to provide notice to individuals prior to collection of information.

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

CSS ingests and aggregates data from other source systems. Individuals consent to uses, decline to provide information, or opt out based upon the privacy policy of the systems providing source data to CSS.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: An individual may be unaware of CSS collection, use, and dissemination of his or her information.

Mitigation: This risk is partially mitigated. The majority of data transmitted by CSS is provided by other systems. Individuals consent to uses, decline to provide information, or opt out during the initial information collection, if applicable, by the source systems providing data to CSS. There are some instances in which an individual would not be able to opt out, such as during a law enforcement action or if an individual or his or her PII is inadvertently captured as part of a video that is uploaded in the system. When CSS is the federal ingestion source for non-DHS PII, S&T provides notice via the CSS PIA regarding its collection, use, dissemination, and maintenance of PII. Collection and uses of PII from other DHS Component sources are described in their respective data feed owners' privacy notices, PIAs, and SORNs.

For data from other system owners, DHS establishes ISAs with each data owner that defines collection and security incident notification requirements.

Section 5.0 Data Retention by the project

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

CSS retains information within the CSS platform per the data owner's data retention policy. Data is not kept for more than 30 days. The CSS Program Manager and the Executive Steering Committee (ESC) may determine in rare circumstances a requirement to keep data beyond 30 days for Operational Testing and Evaluation (OT&E) by an Independent Verification and Validation team. Data is destroyed five years after conclusion of OT&E testing and submission of the report or earlier if no longer needed for legal, business, or audit purposes.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: CSS may retain information beyond the period allowed by applicable statute, policy, instruction, or guidance.

Mitigation: CSS is bound by Memoranda of Understanding (MOU), Memoranda of Agreement (MOA), or ISA to retain information per the data owner's data retention policy. Maximum limits of data retention is governed by DHS policy. Generally, data is not kept for more than 30 days.

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.

Per the roles and responsibilities stated above, COI are created and managed by DHS Components to enable sharing with Law Enforcement, Security, and Safety partners across the FSLTIPP. Data owners across the FSLTIPP can participate as Feed Owners and share their data with their FSLTIPP partners. Communities of Interest and Identity are managed in HSIN and policies are implemented via CSS's ABAC.

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

Data owners listed in Section 1.2 are responsible for ensuring their data sharing policies are compatible with their SORNs.

- DHS/CBP-019 AMOSS SORN
    - Routine use H allows for the sharing of information to federal and foreign government intelligence agencies or components when DHS becomes aware of an indication of threat to national or international security, or to assist in ant-terrorism efforts;
    - Routine use J allows for the sharing of information to any third party in the course of safety, security, and a law enforcement operations to the extent necessary to obtain information pertinent to the investigation; and
    - Routine use L allows for the sharing of information to appropriate federal, state, local, tribal, or foreign governmental organizations when CBP is aware of a need to use relevant data for purposes of testing new technology and systems designed to enhance border security or identify other violations of law.[15]

[15] DHS/CBP-019 Air and Marine Operations Surveillance System (AMOSS) System of Records Notice, 78 FR 57402 (September 18, 2013).

- DHS/USCG-013 MISLE
    - Routine use O allows for the sharing of information to Federal, State, or local agencies with which the USCG has a MOU, MOA, or Inspection and Certification Agreement (ICA) pertaining to maritime security, maritime intelligence, or maritime law.[16]
- DHS/USCG-029 NOAD
    - Routine use H allows for the sharing of information to federal and foreign government intelligence and counterintelligence agencies and components if USCG becomes aware of an indication of a threat or potential threat to national or international security, or if such use is to assist in anti-terrorism efforts; and
    - Routine use M allows for the sharing of information to appropriate federal, state, local, tribal, territorial, or foreign governmental organizations or multilateral government organizations if DHS is aware of a need to use relevant data for purposes of testing new technology and systems designed to enhance border security or identify other violations of law.[17]
- DHS/USCG-061 MAGNET
    - Routine use B allows for the sharing of information to Federal, State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other national security directive;
    - Routine use E allows for the sharing of information to Federal, State, or local agencies with which the USCG has a MOU, MOA, or Inspection and Certification Agreement (ICA) pertaining to maritime security, maritime intelligence, or maritime law; and
    - Routine use I allows for the sharing of information to appropriate 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.[18]

[16] DHS/USCG-013 Marine Information for Safety and Law Enforcement (MISLE), 74 FR 30305 (June 25, 2009).
[17] DHS/USCG-029 Notice of Arrival and Departure System of Records, 82 FR 32715 (July 17, 2017).
[18] DHS/USCG-061 Maritime Awareness Global Network (MAGNET), 73 FR 28143 (May 15, 2008).

- DHS/ICE-009 External Investigations
    - Routine use K allows for the sharing of information to an appropriate Federal law enforcement and/or regulatory agency, technical or subject matter expert, or any other entity involved in or assisting with law enforcement efforts pertaining to suspected or confirmed export violations in accordance with Federal export laws, including the Arms Export control Act, 22 U.S.C. 2778 and the Export Administration Act, 50 U.S.C. 2410;
    - Routine use L allows for the sharing of information to Federal or foreign government intelligence or counterterrorism agencies or components where DHS becomes aware of a threat or potential threat to national or international security, or where such use is to assist in anti-terrorism efforts; and
    - Routine use Q allows for the sharing of information to Federal, State, Tribal, local or foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence information, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.[19]
- DHS/ALL-037 E-Authentication Records
    - Routine use K allows the sharing of information to a trusted third-party identity service provider under contract with DHS or certified by the Federal Identity Management Credential and Access Management initiative for the purpose of authenticating an individual seeking a credential with DHS.[20]

6.3 Does the project place limitations on re-dissemination?

Limitations on re-dissemination of data from CSS are dictated by established MOA/MOUs and ISAs. Re-dissemination is controlled by the Data Owners' data sharing policies through CSS's ABAC.

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

As an S&T program, CSS is developing detailed system audit logging to address privacy and security requirements. The enhanced audit logging will record all user login/logout, all policy activation/deactivation, and all policy snapshots. This enhanced audit trail will enumerate

[19] DHS/ICE-009 External Investigations 75 FR 404 (January 5, 2010).
[20] DHS/ALL-037 E-Authentication Records System of Records, 79 FR 46857 (August 11, 2014).

data shared to individual users. S&T expects to launch this capability the end of 2018.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Information may be shared for purposes not compatible with the stated purpose and use of the original collection.

Mitigation: Data Owners providing data to CSS control sharing of their data outside of DHS. The CSS default policy is to deny sharing; a system owner only shares data with users possessing a specific attribute or set of attributes. Per the roles and responsibilities stated above, COIs are created and managed by DHS Components to enable sharing with Law Enforcement, security, and safety partners across the FSLTIPP. Data Owners across the FSLTIPP can participate as Feed Owners and share their data with their FSLTIPP partners. Identity is managed in HSIN and policies are implemented via CSS's ABAC. Source systems and applicable data are listed in Section 2.1 and Appendix A.

CSS protects PII (in all forms) through entitlements, using ABAC to implement associated system owner sharing policies to maximize information sharing, while controlling or eliminating risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. System Owners are currently trained in building and implementing policies in accordance with industry and system best practices by program Subject Matter Experts in the role of Entitlement Administrators.

CSS COI Managers and Node Administrators are responsible for ensuring User Attributes are properly assigned and vetted. The assigned attributes are reviewed on a yearly basis along with every user account. As more attributes are moved to and managed in HSIN, the ability to manage attributes will lie with the appropriate authority (COI Manager, System Owner, etc.).

CSS implements a framework for information sharing that provides greater visibility across DHS component agencies and their partners, while enabling system owners to control the dissemination of data as required to protect the civil liberties and civil rights of individuals.

Section 7.0 Redress

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

CSS does not maintain any mechanisms to allow individuals to access their information in the system. Access by individuals to their information is governed by the respective data owner's FOIA/Privacy Act request policy.

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

Individuals desiring to correct inaccurate or erroneous information can seek the support of the originating system's public records or Component FOIA/Privacy Act Officer.

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

The respective owners of the data feeds used by CSS have established procedures for correcting information. CSS does not modify any of the original data from the data owners.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Incorrect information in CSS cannot be corrected or flagged as incorrect at the request of an individual.

Mitigation: The PII contained within CSS is provided by law enforcement databases or Sensor systems. Sensor systems provide a one-way feed that prevents alteration of the data. Therefore, redress of inaccurate or erroneous sensor information can be addressed with the source data provider. Redress of inaccurate or erroneous law enforcement database information is obtained through the originating data owner of the data. Refer to Appendix A for a list of systems and data owners providing data to CSS.

CSS does not collect information directly from the individual. CSS does leverage self-published information collected by other DHS systems (*i.e.*, AIS and SANS). Sensor information is collected from federal and state systems operating in public spaces and collecting information for law enforcement, security, and safety purposes. Individuals can contact the data owner(s) to seek redress.

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?

CSS audit logs record and track access to the CSS system by users and System Administrators. CSS has a POA&M to add audit logging of addition, modification, and deletion of entitlement policies. CSS users are required to follow the CSS Rules of Behavior and their respective agency's information use policies.

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

All DHS personnel are required to complete privacy training. This includes CSS users, data owners, and systems administrators. Systems owners sharing PII data are responsible for ensuring users receive system specific role-based privacy training from their organization. Law enforcement, safety, and security personnel using the system are expected to receive specific role-based privacy training from their organization. The data sharing MOUs that participating agencies sign requires that the agencies provide to the CSS System Owner a memorandum for record on a quarterly basis listing and validating that users have received Privacy Training. The CSS System Owner ensures that its CSS PMO, Cybersecurity, Development, and Operations personnel receive privacy training.

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 CSS users undergo a DHS Background Investigation and receive an EOD and Favorable Suitability Decision as condition for access to CSS. Per the CSS SP, all CSS users' accounts that are inactive for 30 days are automatically disabled. The CSS ISSO reviews the CSS account list at least annually, or as needed (out processing of departing personnel), in coordination with the CSS Information System Owner (ISO) and validates that all CSS users maintain a "need to know for access" to CSS information. Per the roles and responsibilities defined above, COIs are created and managed by DHS Components to enable sharing with Law Enforcement, Security, and Safety partners across the FSLTIPP. Data Owners across the FSLTIPP can participate as Feed Owners and share their data with their FSLTIPP partners. Identity is managed in HSIN and policies are implemented via CSS's ABAC. Source systems and applicable data are listed in Section 2.1 and Appendix A.

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?

Memoranda of Agreement/Understanding are reviewed, approved, and signed at the DHS S&T HSARPA executive level. The CSS ISO, the Information System Security Manager (ISSM), the ISSO, and the DHS S&T Privacy Office will review and advise the Authorizing Official on all Information Sharing Agreements, MOUs, Interconnection Security Agreements, new uses of the information, and new access to the system by organizations within DHS and outside DHS. All Interconnection Security Agreements are reviewed, approved, and signed by the respective

Authorizing Officials. Users are sponsored by COI Managers as recommended by Component partners.

Responsible Officials

Joe A. Campillo
Science & Technology Directorate
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

Appendix A: Interconnected Data Sources by Data Type

The following CSS data source systems may provide AIS data:

- USCG Nationwide Automatic Identification System (NAIS);[21]
- USCG Sensor Management System (SMS);[22]
- USCG Port and Waterways Safety System (PAWSS) Ship Arrival and Notification System (SANS);[23]
- CBP Northern Border - Remote Video Surveillance System's (NB-RVSS) Maritime Detection Project (MDP);[24]
- Maryland Natural Resource Police's Maritime Law Enforcement Information Network (MLEIN);[25] and
- Office Director of National Intelligence (ODNI) National Maritime Intelligence-Integration Office (NMIO) Canada United States (CANUS) Information Sharing System - Puget Sound (CANUSISS-PS).[26]

The following CSS data source systems may provide video data:

- USCG Sensor Management System (SMS)
- U.S. Immigrations and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Video Evidence Collections & Distribution System (VECADS);[27] and
- Maryland Natural Resource Police's Maritime Law Enforcement Information Network (MLEIN).

[21] DHS/USCG/PIA-006 Vessel Requirements for Notices of Arrival and Departure (NOAD) and Automatic Identification System (AIS) *available at* www.dhs.gov/privacy.
[22] The Sensor Management System access is provided to the USCG by the U.S. Navy located in designated sectors of shared areas of responsibility. "Sensors" being provided to USCG and maintained by Navy for the USCG include: cameras, radars, Command and control equipment, and a network to distribute the sensor feeds.
[23] PAWSS does not collect PII. For more information *see* https://www.navcen.uscg.gov/?pageName=vtsPAWSS
[24] *See* DHS/CBP/PIA-022 Border Surveillance Systems (BSS) *available at* www.dhs.gov/privacy
[25] For more information *see* http://news.maryland.gov/dnr/2014/05/21/nrp-wins-award-for-state-of-the-art-enforcement-tool/
[26] More information about ODNI's privacy policies can be found *at* https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-resources/privacy-civil-rights-civil-liberties
[27] *See* DHS/ICE/PIA-045 ICE Investigative Case Management *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf.

The following CSS data source systems may provide radar data:

- USCG Sensor Management System (SMS);
- CBP Northern Border - Remote Video Surveillance System's (NB-RVSS) Maritime Detection Project (MDP);
- Maryland Natural Resource Police's Maritime Law Enforcement Information Network (MLEIN); and
- Office Director of National Intelligence (ODNI) National Maritime Intelligence-Integration Office (NMIO) Canada United States (CANUS) Information Sharing System - Puget Sound (CANUSISS-PS).

Appendix B: Federal, State, Local, Tribal, International, Public or Private (FSLTIPP) User Communities

CSS is available to communities of users based on DHS Regional Coordinating Mechanisms (ReCoM), which are defined by DHS USCG Sector (Geographic) Boundaries:

1. Sector Puget Sound
2. Sector Los Angeles/Long Beach
3. Sector San Diego
4. Sector Maryland (Baltimore)
5. Sector Detroit
6. Sector Buffalo