U.S. CUSTOMS AND BORDER PROTECTION

DIRECTIVE NUMBER:
2120-010A

DIRECTIVE TITLE:
Privacy Policy, Compliance, and Implementation

EFFECTIVE DATE:
June 29, 2022

U.S. Customs and Border Protection

CBP Publication No. 1724-0422

What are Freedom of Information Act (FOIA) "Exemptions"?

Not all information within records is required to be released under the FOIA. Congress established nine exemptions from disclosure for certain categories of information to protect against certain harms, such as an invasion of personal privacy, or harm to law enforcement investigations. The FOIA authorizes agencies to withhold information falling under these categories when an agency reasonably foresees that disclosure would harm an interest protected by one of the nine exemptions are described below.

Exemption 1

Classified Information: Information specifically authorized under criteria established by an executive order to be kept secret in the interest of national defense or foreign policy and are in fact properly classified pursuant to such executive order.

Exemption 2

Personnel Rules and Practices: Information related solely to the internal personnel rules/practices of an agency.

Exemption 3

Information Exempted by Statute: Information specifically exempted from disclosure by statute if that statute requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue; or establishes particular criteria for withholding or refers to particular types of matters to be withheld; and if enacted after the date of enactment of the OPEN FOIA Act of 2009, specifically cites to 5 U.S.C. § 552(b)(3).

Exemption 4

Trade Secrets and Confidential Commercial Information: Trade secrets and commercial or financial information obtained from a person and privileged or confidential.

Exemption 5

Privileged Information: Inter-agency or intra-Agency memorandums or letters that would not be available by law to a party other than an agency in litigation with the agency, provided the deliberative process privilege shall not apply to records created 25 years or more before the date on which the records were requested.

Exemption 6

Personal Information: Personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Exemption 7

Certain Law Enforcement Information: Records or information compiled for law enforcement purposes (but only to the extent that the production of such law enforcement records/information) that:

7(A) Could reasonably be expected to interfere with enforcement proceedings.

7(B) Would deprive a person of a right to a fair trial/impartial adjudication.

7(C) Could reasonably be expected to constitute an unwarranted invasion of personal privacy.

7(D) Could reasonably be expected to disclose the identity of a confidential source, including a state, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a law enforcement authority in the course of a criminal investigation execution of a lawful national security intelligence investigation, information furnished by a confidential source.

7(E) Would disclose techniques and procedures for law enforcement investigations/prosecutions or would disclose guidelines for law enforcement investigations/prosecutions if such disclosure reasonably risked circumvention of the law.

7(F) Could reasonably be expected to endanger the life or physical safety of any individual.

Exemption 8

Information About Financial Institutions: Information contained in or related to examination, operating or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions.

Exemption 9

Information About Wells: Geological or geophysical information and data, including maps, concerning wells.

Additional descriptions and examples of each FOIA Exemption Category above can be found at:
https://www.dhs.gov/foia-exemptions

U.S. CUSTOMS AND BORDER PROTECTION DIRECTIVE

CBP DIRECTIVE NO. 2120-010A **DATE: June 29, 2022**

ORIGINATING OFFICE: OC-PDO

REVIEW DATE: June 29, 2025

SUBJECT: PRIVACY POLICY, COMPLIANCE, AND IMPLEMENTATION

1. PURPOSE

This Directive is designed to provide U.S. Customs and Border Protection (CBP) personnel with procedures and practices for safeguarding the collection, maintenance, use, and dissemination of personally identifiable information (PII); or when engaged in activities that otherwise impact the privacy of individuals.

2. SCOPE

This Directive applies to all personnel as defined in Section 5, particularly those individuals who have access to, and work with, PII in the conduct of their job-related duties.

3. POLICY

3.1 This Directive applies to all CBP personnel.

3.2 This Directive applies to all CBP forms, Information Technology (IT) systems, tools, platforms, programs, and mobile applications.

3.3 This Directive provides procedures to ensure that the collection, maintenance, use, and dissemination of PII complies with all applicable laws, regulations, and policies.

3.4 The procedures set forth in this Directive must be followed before CBP begins the collection of PII on or from individuals, including CBP personnel; or prior to a change in CBP practices pertaining to the collection, maintenance, use, or dissemination of PII, regardless of whether the source of the change is operational, technological, or regulatory.

3.5 The procedures set forth in this Directive shall be followed before any records owned by CBP that contain PII are shared with another party external to CBP, including any onward sharing of CBP data by other Department of Homeland Security (DHS) Components; and the terms of any new information sharing access agreement or contract services should be consistent with the procedures set forth in this Directive.

3.6 The procedures set forth in this Directive shall be followed when there is an unauthorized access, sharing, or use of PII collected and maintained by CBP.

3.7 This Directive, which follows and implements DHS Directive 047-01, Instruction 047-01-001, and Instruction 047-01-005, at CBP, supersedes any previous conflicting CBP Directives, policy statements, and manual supplements regarding CBP's privacy policy.[1]

4. AUTHORITIES/REFERENCES

4.1 "E-Government Act of 2002," as amended, Public Law 107-347 Section 208 [Title 44, United States Code (U.S.C.), § 3501 note]

4.2 The Privacy Act of 1974, as amended [5 U.S.C. § 552a]

4.3 Tariff Act of 1930, as amended

4.4 "Privacy Officer" 6 U.S.C § 142

4.5 The Federal Information Security Management Act of 2002, as amended (FISMA) [44 U.S.C., Chapter 35, Subchapter II, "Information Security"]

4.6 "Disclosure of records and information" [Title 6, Code of Federal Regulations (CFR), Chapter 1, Part 5]

4.7 "Availability of Information" [19 CFR Chapter 1, Part 103]

4.8 DHS Directive 047-01 "Privacy Policy and Compliance" (July 7, 2011)

4.9 DHS Instruction 047-01-001 "Privacy Policy and Compliance" (July 25, 2011)

4.10 DHS Instruction 047-01-003 "Privacy Policy for DHS Mobile Applications" (December 14, 2018)

4.11 DHS Instruction 047-01-005 "Component Privacy Officer" (February 6, 2017)

4.12 DHS Instruction 047-01-006 "Privacy Incident Responsibilities and Breach Response Team" (December 4, 2017)

4.13 DHS Instruction 047-01-007 "Handbook for Safeguarding Sensitive PII" (December 4, 2017)

[1] In the event a conflict between an existing information sharing agreement and this Directive arises, the terms of the existing agreement will continue to govern the exchange of information until such time as the agreement has been amended to conform to the terms of this Directive.

4.14 DHS Instruction 047-01-008 "Privacy Incident Handling Guidance" (April 28, 2020)

4.15 DHS Instruction 047-01-010 "Social Security Number Collection And Use Reduction" (June 18, 2019)

4.16 DHS Privacy Policy 262-16 "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information"

4.17 DHS Privacy Policy Instruction 262-16-001 "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information"

4.18 CBP Memorandum "Privacy Compliance and U.S. Customs and Border Protection" (February 10, 2012)

4.19 CBP Directive 4320-025A "Disclosure of Official Information to Foreign Authorities" (April 14, 2014)

4.20 CBP Directive 4320-033 "Sharing of CBP Information for Law Enforcement and Security Purposes" (May 24, 2021)

4.21 CBP Directive 2110-040 "Records and Information Management Directive" (June 3, 2019)

4.22 DHS Information Sharing and Safeguarding Governance Board Charter

4.23 Privacy and Civil Liberties Guidance Memorandum 2009-01, "The Department of Homeland Security's Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy" (June 5, 2009)

4.24 Information Sharing and Access Agreements Guidebook and Templates (October 2010)

4.25 Secretary Michael Chertoff memorandum to all DHS components regarding DHS Policy for Internal Information Exchange and Sharing (hereafter ''One-DHS Memorandum") (February 1, 2007)

4.26 Memorandum from Soraya Correa, DHS Chief Procurement Officer, entitled *Class Deviation 15-01 from the Homeland Security Acquisition Regulation: Safeguarding of Sensitive Information* (March 9, 2015)

4.27 NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*

4.28 Office of Management and Budget (OMB) Memorandum M-17-12, "Preparing for and responding to a Breach of Personally Identifiable Information." (Jan. 3, 2017)

5. DEFINITIONS

5.1 **Authority to Operate (ATO):** a formal declaration by a Designated Approving Authority (DAA) that authorizes operation of an Information Technology System and explicitly accepts the risk of operating that system to agency operations. The ATO is signed after the system has met and passed all requirements to become operational. No Authority to Operate (ATO) shall be issued without the DHS Chief Privacy Officer's approval signifying that the system is in compliance with the requirements outlined in NIST SP 800-53 Appendix J, "Privacy Control Catalogue."

5.2 **Authority to Test (ATT):** An interim authorization to operate that allows personnel to begin testing systems under development or in the prototype phase. ATTs are typically granted for the testing of systems using production data.

5.3 **Bulk Sharing:** The dissemination of large quantities of information, in a single disclosure or multiple disclosures, to external partners, including other DHS components, federal Departments/Agencies, or foreign partners.[2]

5.4 **Business Owner:** The CBP personnel responsible for the planning and execution of a CBP project, operation, or program, including pilots and demonstrations, mobile applications, CBP Forms, regulations, and rulemakings.

5.5 **CBP Privacy Office:** The CBP Privacy Office is a division within the CBP Privacy and Diversity Office, under the Office of the Commissioner. The CBP Privacy Office is tasked with developing and fostering a culture of privacy at CBP by promoting transparency and data integrity in all border security, immigration, and law enforcement activities; as well as assuring that the use of technologies sustain and do not erode privacy protections relating to the use, collection, and disclosure of personal information.

[2] For the purpose of this Directive, the definition of Bulk Sharing differs slightly from the standard DHS DARC definition, which describes "bulk data transfer" as collection or dissemination of large quantities of intelligence or information, a significant portion of which is not reasonably likely to have any ultimate intelligence or operational value to the recipient, but which is provided to the data recipient for the recipient to identify information of intelligence or operational value within it. Bulk data transfer does not include the transfer of records responsive to individual identifiers (e.g., name, date of birth, social security number, etc.), but it does include the transfer of records identified through the application of selectors where the transfer would include a significant number of records that, while responsive to the applied selectors, is not reasonably likely to have any ultimate intelligence or operational value to the recipient (e.g., records responsive to demographic profiles such as age, citizenship, gender, etc.).

5.6 **CBP Privacy Officer:** The senior official within CBP with primary responsibility for privacy compliance and policy, including, but not limited to: monitoring CBP compliance with all federal privacy laws and regulations; implementing corrective, remedial, and preventative actions; assisting in drafting and reviewing all forms of privacy compliance documentation; serving as the point of contact to handle privacy incident response responsibilities; implementing and monitoring privacy training for CBP personnel; contributing CBP information responsive to the public reporting requirements of the DHS Privacy Office; and communicating CBP privacy initiatives, both internally and externally.

5.7 **Chief Privacy Officer:** As set forth in Section 222 of the Homeland Security Act of 2002, as amended, 6 U.S.C. § 142, the senior official in DHS who reports directly to the DHS Secretary, with the primary responsibility for privacy compliance and policy within DHS.

5.8 **Data Access Review Council (DARC):** The coordinated oversight and compliance mechanism for the review of departmental initiatives and activities involving the internal or external transfer of personally identifiable information (PII) through bulk data transfers[3] that are domestic in nature and are in support of the Department's national and homeland security mission.

5.9 **Data Access Request Process (DARP) Questionnaire:** The form that may be used to initiate any domestic information sharing project that may require an Information Sharing Access Agreement (ISAA). In filling out a DARP Questionnaire, both parties to the ISAA must identify all relevant stakeholders, the information subject to the exchange, the authorities permitting the exchange, intended uses of the information, and any policy implications of the information exchange.

5.10 **Fair Information Practice Principles (FIPPs):** The policy framework adopted by DHS in Directive 047-01, "Privacy Policy and Compliance," regarding the collection, use, maintenance, disclosure, deletion, or destruction of PII.

5.11 **Homeland Security Acquisition Regulation:** The Department of Homeland Security Acquisition Regulation (HSAR) establishes uniform acquisition policies and procedures, which implement and supplement the Federal Acquisition Regulation (FAR) and help to ensure privacy protections are in place for technologies and services acquired by the Department and its components.

[3] Coordination with the DARC is only required when the bulk data transfer involves the collection or dissemination of large quantities of intelligence or information, a significant portion of which is not reasonably likely to have any ultimate intelligence or operational value to the recipient, but which is provided to the data recipient for the recipient to identify information of intelligence or operational value within it. See Footnote 2.

5.12 Individual: Any natural person. As a matter of law, the Privacy Act of 1974 (Privacy Act), as amended, provides statutory privacy rights only to U.S. citizens and Lawful Permanent Residents. As a matter of policy, DHS affords administrative Privacy Act protections to all persons, regardless of immigration status, consistent with the Fair Information Practice Principles and applicable law. Additionally, the Judicial Redress Act (JRA) provides certain statutory rights related to access, amendment, and disclosure of covered records related to covered persons as defined by the JRA.[4]

5.13 Information Sharing Access Agreement (ISAA): Any Memorandum of Understanding or Agreement (MOU/A) or other document, such as a Letter of Intent or Release Authorization, intending to represent an agreement or arrangement that defines the terms and conditions of information/data exchanges between CBP and one or more non-DHS parties.

5.14 Information Sharing Action Officer (ISAO): Member of the Privacy and Diversity Office (PDO) identified to represent CBP privacy equities on the DHS Information Sharing Coordination Council (ISCC) and the DHS Data Access Review Council (DARC). The ISAO supports the coordination, drafting, review, and clearance of all ISAAs involving CBP data (including PII).

5.15 Information Sharing and Safeguarding Governance Board (ISSGB): The senior level DHS body that governs the implementation and execution of ISAAs. The ISSGB will reconcile information sharing issues referred to it by the Information Sharing Coordination Council (ISCC) and raise unresolved issues to senior leadership.

5.16 Information Sharing Coordination Council (ISCC): The working body for the ISSGB. The ISCC provides a forum for DHS Components to raise information sharing issues. The ISCC is responsible for reviewing all Component requests for an exemption to the One DHS policy for an ISAA. The ISCC will work collaboratively to mitigate these issues. If the ISCC cannot resolve an issue, it will refer the issue to the ISSGB.

5.17 Information Technology Acquisition Review (ITAR): The DHS process to ensure that all information technology investments are aligned with DHS mission objectives and privacy-protective practices, and to effectively manage contract and procurement risks.

5.18 Letter of Release Authorization: A written approval for the provision of copies of CBP records in response to a request for information that conveys the terms and conditions for the use, retention, onward sharing, and disposition of said information.

[4] *See*: Judicial Redress Act of 2015, Pub. L. 114-126 (JRA)

5.19 Ongoing Authorization (OA): The ongoing assessment of security and privacy controls in support of the continual authorization of DHS/CBP Information Technology systems.

5.20 Personnel: All permanent and temporary CBP employees, non-CBP personnel serving with CBP, and contracted personnel; including those personnel representing CBP while assigned to multi-agency task forces or other joint governmental efforts.

5.21 Personally Identifiable Information (PII): Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a United States citizen, lawful permanent resident, or a visitor to the United States.[5]

5.22 Privacy Analyst: CBP personnel designated by the CBP Privacy Officer to serve as a point of contact for the operational components (Office of Field Operations, United States Border Patrol, Air and Marine Operations) and support offices (Office of Information and Technology, Office of Professional Responsibility, Human Resources Management, etc.) regarding privacy issues associated with the collection, maintenance, use, or sharing of PII by that office.

5.23 Privacy Compliance Documentation: Any document required by statute, policy, or by the DHS Chief Privacy Officer that supports compliance with DHS privacy policy, procedures, or requirements, including, but not limited to, Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs),[6] System of Records Notices (SORNs), Notices of Proposed Rulemaking (NPRM) for exemption from certain aspects of the Privacy Act, or Final Rules for exemption from certain aspects of the Privacy Act.[7]

5.24 Privacy Impact Assessment (PIA): The DHS Privacy Office process to be followed and the document required whenever a CBP information technology (IT) system, technology, rulemaking, program, pilot project, demonstration, or other activity

---

[5] For example, when linked or linkable to an individual, such information includes a name, Alien Registration Number, Social Security number, date and place of birth, mother's maiden name, account number, license number, vehicle identifier number, license plate number, device identifier or serial number, internet protocol address, biometric identifier (e.g., photograph, fingerprint, iris scan, voice print), educational information, financial information, medical information, criminal or employment information, and information created specifically to identify or authenticate an individual (e.g., a random generated number).

[6] Section 208 of the E-Government Act of 2002 [44 U.S.C. § 3501) requires the completion of a Privacy Impact Assessment whenever the government develops or procures information technology that collects, maintains, or disseminates PII about members of the public.

[7] The Privacy Act of 1974, as amended (5 U.S.C. § 552a) establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

involves the planned use of PII, or otherwise impacts the privacy of individuals as determined by the Chief Privacy Officer.[8]

5.25 Privacy Incident: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users have access or potential access to PII in usable form, whether physical or electronic, or where authorized users access PII for an unauthorized purpose. Privacy Incidents include both suspected and confirmed incidents involving PII that raise a reasonable risk of harm. The determination of what constitutes a Privacy Incident will be made by the CBP Privacy Office. The term "Privacy Incident" will be used synonymously with the term "breach."

5.26 Privacy Liaison: Employee responsible for serving as a field-level point of contact and initial identifier of privacy issues and programmatic considerations on behalf of the CBP office. This employee is designated by the Director of Field Operations (DFO) for each Field Office within the Office of Field Operations (OFO), the Chief Patrol Agent for each Sector within Border Patrol (BP), the Director of each Branch within the Office of Air and Marine Operations (AMO), the Executive Assistant Commissioner for the Office of Trade, and the Assistant Commissioners for each of the offices within Operations Support and Enterprise Services. Each Field Office, Sector, Branch, and support office shall designate one or more employees, at the GS-14 level or higher in their operational and/or program compliance units as the Privacy Liaison(s).

5.27 Privacy Threshold Analysis (PTA): The DHS Privacy Office process to be followed and the document used to identify the privacy implications of information technology (IT) systems, technologies, rulemakings, programs, pilot projects, or information sharing and access agreements. The DHS Privacy Office, working in conjunction with the CBP Privacy Officer, uses the PTA to determine if an activity may involve PII or otherwise impact the privacy of individuals and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the IT system, technology, rulemaking, program, pilot project, or other Department activity and describes what PII (if any) is collected (and from whom) and how that information is used or retained. The Privacy Office will determine which PTA template (IT system, Mobile Application, information sharing, form, disposition, etc.) is appropriate based on the activity being reviewed.

[8] A PIA describes what information DHS is collecting; why the information is being collected; how the information will be used, stored, and shared; how the information may be accessed; how the information will be protected from unauthorized use or disclosure; and how long it will be retained. A PIA also provides an analysis of the privacy considerations posed and the steps DHS has taken to mitigate any impact on privacy. As a general rule, PIAs are public documents. The Chief Privacy Officer may modify or waive publication for security reasons or to protect classified, sensitive, or private information included in a PIA.

5.28 Project Manager (PM): CBP employee responsible for acquiring, building, technically maintaining, and/or operating a system, tool, program, or project with privacy implications.

5.29 Sensitive Personally Identifiable Information: Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

5.30 System of Records Notice (SORN): The official public notice of a DHS system of records as required by the Privacy Act of 1974 (as amended). SORNs identify the purpose for the system of records, the individuals covered by information in the system of records, the categories of records maintained about individuals, and the ways in which the information is generally shared by the agency, and provide notice of the mechanisms available for individuals to exercise their Privacy Act rights to access and correct the PII that CBP maintains about them.[9]

5.31 Representative of the press: Any person or entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience. A freelance journalist may qualify if the journalist can demonstrate a solid basis for expecting publication, such as a publication contract or extensive history of regular publication.

6. RESPONSIBILITIES

6.1 All CBP personnel, and others who have access to or use of CBP systems and data will:

6.1.1 Comply with this CBP Directive and with privacy policies and procedures issued by the DHS Chief Privacy Officer or by CBP's Privacy Officer;

6.1.2 Alert their Privacy Liaison, designated Privacy Analyst, or the CBP Privacy and Diversity Office about any systems, technologies, regulations, rulemakings, programs, pilot projects, demonstrations,[10] information sharing, contracts, and other activities that involve PII or otherwise impact the privacy of individuals (e.g., the development or use of facial recognition and other biometric technologies; efforts involving the collection, use, or sharing of cellular phone and location data; access to and use of social media information; the collection or disclosure of medical information; the

[9] *See:* 5 U.S.C. § 552a(e)(4).
[10] Demonstrations of third-party developed software, systems, or tools, including those in which CBP engages in using free/no cost accounts, in order to test a product, must be coordinated with the CBP Privacy Office before any use, testing, or deployment occurs.

development or application of artificial intelligence or machine learning; surveillance or body-worn cameras; etc.);

6.1.3 Protect PII from unauthorized collection, maintenance, use, disclosure, or public dissemination and display, whether in physical/hard copy, electronic, or verbal form;

6.1.4 Report any suspected or actual Privacy Incidents, as required by Section 9 of this Directive and the DHS Privacy Incident Handling Guidance;

6.1.5 Ensure any disclosure of PII from a System of Records to a party outside of CBP is consistent with DHS and CBP policy, specifically the parameters outlined in Section 8 of this Directive;

6.1.6 Ensure that any disclosures of PII from a System of Records to a party outside of DHS are properly accounted for through either a system generated or electronically filed DHS-191 Form, other Privacy Act Disclosure Record, or other form or process specifically authorized by the Chief Privacy Officer, and comply with any other reporting requirements which may be applicable to specific data (e.g., Passenger Name Record (PNR) data);

6.1.7 Ensure that any dissemination of PII and SPII to parties outside of DHS is conducted in accordance with DHS Privacy Policy Directive 047-01-007, and is:

6.1.7.1 Sent via password-protected or encrypted attachment to an email, with the password or key sent in a separate message;

6.1.7.2 Transferred via approved system connections or on approved, encrypted removable media device pursuant to the requirements outlined in the DHS Sensitive Systems Policy Directive 4300A; or

6.1.7.3 Transferred in a sealed, opaque envelope or container mailed using First Class Mail, Priority Mail, or a traceable, receipted commercial delivery service;[11]

6.1.8 Safeguard Social Security numbers (SSNs) so that they are protected from public dissemination and display, and only used or accessed consistent with relevant statutes, rules, or directives:

[11] *See*: DHS Management Directive (MD) 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, for the transportation or mailing of data.

6.1.8.1 Where possible, the collection, use, maintenance, and dissemination of SSNs should be avoided, and in their place, separate unique identifiers should be used; and

6.1.8.2 Where the use of SSNs cannot be eliminated, a privacy-enhancing measure, including but not limited to truncation should be implemented where possible;

6.1.9 Safeguard PII and Sensitive PII so that they are protected from public unauthorized dissemination and display, and only used or accessed consistent with relevant statutes, rules, or directives;

6.1.10 Complete mandatory annual privacy training, as well as any program, IT system, or activity-specific privacy training as described in Section 10 of this Directive; and

6.1.11 Contact the Office of Chief Counsel for assistance with any requested or proposed disclosure of CBP information when CBP is under an apparent legal obligation to disclose information in the course of, or in conjunction with, a judicial proceeding (e.g., due to a subpoena or discovery request, in response to a court order, or in response to litigation against the Government), or as required by any other CBP policy regarding the disclosure of CBP information requiring review by the Office of Chief Counsel.

6.2 The CBP Privacy Officer will:

6.2.1 Oversee the completion of required Privacy Compliance Documentation for all proposed CBP IT systems, technologies, rulemakings, programs, pilot projects, information sharing, contracts, or other activities that involve PII or otherwise may impact the privacy of individuals;

6.2.2 Oversee the completion of required Privacy Compliance Documentation for the continuation of, or changes to, operational IT systems, technologies, rulemakings, programs, pilot projects, information sharing, contracts, or other activities that involve PII or otherwise may impact the privacy of individuals;

6.2.3 Review and develop CBP policies and Directives to ensure compliance with DHS and CBP privacy policy, privacy laws, and federal government-wide privacy policies;

6.2.4 Oversee CBP privacy training and the provision of educational materials, consistent with mandatory and supplementary training developed by the DHS Chief Privacy Officer;

6.2.5 Provide privacy training to all Privacy Liaisons in order to assist them in identifying CBP IT systems, technologies, rulemakings, programs, pilot projects, demonstrations, information sharing, contracts, and other activities with privacy implications;

6.2.6 Maintain an ongoing review of all CBP IT systems, technologies, rulemakings, programs, pilot projects, information sharing, contracts, and other activities to identify collections and uses of PII and to identify any other attendant privacy impacts;

6.2.7 Oversee CBP implementation of DHS privacy policy, including any guidance, Directive, memorandum, or related document issued by the DHS Chief Privacy Officer;

6.2.8 Provide the DHS Chief Privacy Officer all CBP information necessary to meet the Department's responsibilities to report to Congress and the Office of Management and Budget (OMB) on DHS activities that involve PII or otherwise impact the meeting of privacy statutory requirements, including issues of policy and process;

6.2.9 Oversee CBP's implementation of CBP procedures, and guidance issued by the DHS Chief Privacy Officer, for handling suspected and confirmed Privacy Incidents, including making a determination of whether an issue constitutes an Incident; determining a Privacy Incident's level of severity; notifying the DHS Chief Privacy Officer and other Department offices of such Incidents as DHS and CBP procedures dictate; ensuring that Privacy Incidents have been properly mitigated and remediated; and making recommendations to the DHS Chief Privacy Officer for closure of Privacy Incidents;

6.2.10 Where PII is being collected or used through an automated system or pursuant to a project, operation, or regulatory change before the proper Privacy Compliance Documentation is completed, make a determination in coordination with the DHS Privacy Office on how to address the situation, including whether to shut down the collection or to take any other corrective actions according to DHS Directive 262-16 and Instruction 262-16-001;

6.2.11 Process privacy complaints and amendment requests from organizations, DHS employees, and other individuals, whether received directly or by referral from the DHS Privacy Office or any other office;

6.2.12 Document and implement procedures for identifying, processing, tracking, and reporting requests for amendments to records made under the Privacy Act;

6.2.13 Maintain an ongoing review of all CBP data collections, whether in electronic or paper-based form, to ensure compliance with the Privacy Act Statements and all implementing regulations and guidelines;

6.2.14 Review CBP record retention schedules for paper or electronic records that contain PII to ensure privacy interests are considered in the establishment of CBP record disposition policies;

6.2.15 In consultation with the DHS Chief Privacy Officer, advise CBP on information sharing activities that involve the disclosure or receipt of PII, and participate in the review of ISAAs. All requests for ISAAs must comply with procedures established by the DHS ISSGB and follow the process established by the ISCC when seeking an exception to the One DHS Rule;[12]

6.2.16 Advise CBP personnel on activities involving bulk sharing initiatives or activities involving the transfer of bulk data to domestic partner agencies for national security purposes brought before the Data Access Review Council (DARC), and participate in the review of such bulk data transfer and bulk sharing initiatives or activities. All bulk data transfer agreements being used for national security purposes must comply with the procedures and processes established by the DARC;[13]

6.2.17 Oversee the issuance of Letters of Release Authorization to permit the ad hoc sharing of records containing PII, when an ISAA or other policy-based mechanism authorizing or supporting the sharing is not in place (ex. Delegation of Authority), under the authority and routine uses of a System of Records Notice, other statutory authority, or through CBP procedure as discussed in Section 8 of this Directive; and

6.2.18 Review technology and service-related procurement documentation, including: Solicitations, Contracts, Statements of Work (SOW), Performance Work Statements (PWS), and Statements of Objectives (SOO) provided in

[12] Pursuant to Secretary Michael Chertoff's memorandum to all DHS components regarding DHS Policy for Internal Information Exchange and Sharing (hereafter "One-DHS Memo)" (February 1, 2007), internal information sharing and safeguarding purposes, including for purposes of Title 5, United States Code, Section 552a, "Privacy Act of 1974," the Department is one agency, and no Component is a separate agency from another Component.

[13] Coordination with the DARC is only required when the bulk data transfer involves the collection or dissemination of large quantities of intelligence or information, a significant portion of which is not reasonably likely to have any ultimate intelligence or operational value to the recipient, but which is provided to the data recipient for the recipient to identify information of intelligence or operational value within it. See Footnote 2.

support of the acquisition review process (HSAR and ITAR), to ensure that required privacy-protective clauses are present.[14]

6.3 All Executive Assistant Commissioners, Assistant Commissioners, Chief of Border Patrol, and Independent Office Directors (Business Owners) will:

6.3.1 Coordinate with CBP's Privacy Officer to ensure that privacy is appropriately addressed when proposing, developing, implementing, or changing any IT system, technology, regulation, rulemaking, program, proposed ISAA, or other activity, including pilot activities, before any PII is collected, used, or disclosed (e.g., the development or use of facial recognition and other biometric technologies; efforts involving the collection, use, or sharing of cellular phone and location data; access to and use of social media information; the collection or disclosure of medical information; the development or application of artificial intelligence or machine learning; surveillance or body-worn cameras; etc.); and

6.3.2 In consultation with CBP's Privacy Officer, develop and implement privacy procedures and job-related privacy training to safeguard PII in program and system operations.

6.4 The Assistant Commissioner for the Office of Information and Technology will:

6.4.1 Ensure no submission of a new system is made to OMB under the "OMB 300" review process prior to the CBP Privacy Office's clearance and the DHS Privacy Office's adjudication of a PTA for the CBP IT system; and

6.4.2 Ensure no "Authority to Operate" (ATO), "Authority to Test" (ATT), or "Ongoing Authorization" (OA) is granted to systems that lack proper Privacy Compliance Documentation and DHS Chief Privacy Officer approval, as required by OMB 14-04.

6.4.2.1 No Authority to Operate (ATO) shall be issued without the DHS Chief Privacy Officer's approval signifying that the system is in compliance with the requirements outlined in NIST SP 800-53 Appendix J, "Privacy Control Catalogue."

[14] Privacy-protective clauses related to the Safeguarding of Sensitive Information (HSAR Class Deviation 15-01), Information Technology Security and Privacy Training (HSAR Class Deviation 15-01), and Contractor Employee Access (HSAR 3052.204-71) shall be incorporated into new and existing contracts where the service provider will have access to sensitive information, or contractor IT systems are used to input, store, process, output, and/or transmit sensitive information.

6.5 The CBP Chief Records Officer (CRO) will Ensure Privacy Compliance Documentation cites accurate and appropriate NARA-approved records retention schedules or unauthorized disposal language.

6.6 The Executive Assistant Commissioner for the Office of Trade and the Assistant Commissioners for each of the offices within Operations Support and Enterprise Services will designate one or more employees, at the GS-14 level or higher, in their offices and/or directorates as a Privacy Liaison(s).

6.7 The Director of Field Operations (DFO) for each OFO Field Office, the Chief Patrol Agent for each Border Patrol Sector, and the Director of each AMO Branch will designate one or more employees, at the GS-14 level or higher, or individuals serving in a supervisory capacity in their operational and/or program compliance units, as a Privacy Liaison(s).

6.8 Privacy Liaisons will:

6.8.1 Serve as Field and support office-level point of contact for the Privacy Office personnel;

6.8.2 Serve as the local privacy point of contact for field and support office-level personnel seeking guidance on privacy-related issues or assistance resolving privacy-related matters, and refer concerns to the CBP Privacy Office as necessary;

6.8.3 Identify IT systems, technologies, rulemakings, programs, pilot projects, demonstrations, information sharing, contracts, and other activities or initiatives with possible privacy issues within their area of responsibility and alert their designated CBP Privacy Analysts (formally or informally) about them;

6.8.4 Coordinate between the Business Owner and the Privacy Analyst during the development of the IT systems, technologies, rulemakings, programs, pilot projects, demonstrations, information sharing, contracts, and other activities with potential or actual privacy issues within their area of responsibility;

6.8.5 Assist in the drafting and submission of PTAs to the CBP Privacy and Diversity Office for IT systems, technologies, rulemakings, programs, pilot projects, demonstrations, information sharing, contracts, and other activities involving PII within their area of responsibility;

6.8.6 Report to and coordinate with the Privacy Analyst during the response to, and remediation of, Privacy Incidents, including facilitating the provision of remedial training to field and support office-level personnel within their area of responsibility; and

6.8.7 Complete required privacy training as described in Section 10 of this Directive.

6.9 Privacy Analysts will:

6.9.1 Serve as points of contact for CBP personnel regarding privacy issues;

6.9.2 Assist in the drafting and review of privacy compliance documentation submitted by Program Managers, Business Owners, Privacy Liaisons, and others;

6.9.3 Provide guidance to Business Owners and Project Managers regarding privacy issues;

6.9.4 Review ISAAs, other information sharing proposals, and documentation related to privacy compliance and the safeguarding of PII;

6.9.5 Draft Letters of Release Authorization to the extent required to permit ad hoc disclosures of CBP information with agencies external to DHS, when an ISAA or other policy-based mechanism authorizing or supporting the sharing is not in place (ex. Delegation of Authority), in accordance with the conditions of disclosure under the Privacy Act; and

6.9.6 Provide privacy training to CBP personnel.

6.10 Business Owners and Project Managers will:

6.10.1 Coordinate with their Privacy Liaison, Privacy Analyst, and CBP's Privacy Officer to ensure that privacy is appropriately addressed when proposing, developing, implementing, or changing any IT systems, technologies, rulemakings, programs, pilot projects, demonstrations, information sharing, contracts, and other activities;

6.10.2 Coordinate with their Privacy Liaison, Privacy Analyst, and CBP's Privacy Officer to ensure that privacy is appropriately addressed for systems prior to the issuance of an "Authority to Operate" (ATO), "Authority to Test" (ATT), or "Ongoing Authorization" (OA);

6.10.3 Coordinate with their Privacy Liaison, CBP's Privacy Officer, the Records and Information Management Office, and the Office of Chief Counsel in the preparation of drafts of all Privacy Compliance Documentation as required when proposing, developing, implementing, or changing any IT systems, technologies, rulemakings, programs, pilot projects, demonstrations, information sharing, contracts, and other activities;

6.10.4 Monitor the design, deployment, operation, and retirement of the IT systems, technologies, rulemakings, programs, pilot projects, demonstrations, information sharing, contracts, and other activities, to ensure that the use of PII is limited to those uses described in the Privacy Compliance Documentation;

6.10.5 Oversee systems and programs that maintain PII, whether in electronic or paper form, and report any suspected or confirmed Privacy Incidents to the appropriate party in accordance with DHS and CBP procedures for handling Privacy Incidents in Section 9 of this Directive; and

6.10.6 Establish administrative, technical, and physical controls for storing and safeguarding PII consistent with DHS and CBP privacy, security, and records management requirements to ensure the protection of PII from unauthorized access, disclosure, or destruction.

6.10.7 Ensure that personnel are not provided access to CBP systems, programs, or tools containing PII without a fully adjudicated Background Investigation (BI).[15]

6.11 Contracting Officers and Contracting Officers' Representatives will:

6.11.1 Ensure that all contract personnel supporting CBP operations complete the required Privacy Awareness training, review and acknowledge necessary rules of behavior, and complete any system or access-specific training related to privacy;

6.11.2 Coordinate with the Privacy Office to ensure that all contractor-operated systems include necessary safeguards for PII and that all necessary Privacy Compliance documentation sufficiently describes the functionality of the system and the uses of information contained within it;

6.11.3 Notify the CBP Security Operations Center (CBP-SOC) at (703) 921-6507 and the CBP Privacy Office at PRIVACYINCIDENTS@CBP.DHS.GOV immediately upon becoming aware of a privacy incident involving a contractor/subcontractor owned/managed system involving CBP data.

[15] The requirements and processes associated with the completion of Background Investigations (BI) at CBP are outlined in the CBP Personnel Security Handbook (HB 1400-07A), *available at* http://cbpnet.cbp.dhs.gov/IA/Documents/HB%201400-07A.pdf#search=system%20access%2C%20background%20investigation.

6.11.4 Support the Privacy Office's response and remediation of contractor-involved Privacy Incidents through the provision of documentation or other support as identified by the Privacy Office.

7. PRIVACY COMPLIANCE PROCEDURES

7.1 CBP's Privacy and Diversity Office will provide training to all Privacy Liaisons in order to enable them to identify projects or activities with privacy issues early in the development process.

7.2 Each Business Owner who is proposing, developing, implementing, or changing IT systems, technologies, rulemakings, programs, pilot projects, demonstrations, information sharing, contracts, and other activities that may involve the use of PII will include either their in-house Privacy Liaison or a CBP Privacy Analyst in early discussions of such activities to facilitate the determination of the need for Privacy Compliance Documentation.

7.3 Privacy Liaisons must alert their designated CBP Privacy Analysts (formally or informally) about the development or expansion of IT systems, technologies, rulemakings, programs, pilot projects, demonstrations, information sharing, contracts, and other activities, as well as any possible privacy issues.

7.4 The Business Owners of the IT systems, technologies, rulemakings, programs, pilot projects, demonstrations, information sharing, contracts, and other activities are responsible for contacting a Privacy Analyst, through or in coordination with their Privacy Liaison, so that the Privacy Analyst can provide privacy guidance during the development of the system, project, activity, or operation.

7.5 Business Owners and Project Managers of IT systems, technologies, rulemakings, programs, pilot projects, demonstrations, information sharing, contracts, and other activities involving a change in the use of PII shall contact the CBP Privacy Office for assistance.

7.6 The Business Owners, working with a Privacy Analyst, will prepare a PTA to determine the required level of privacy compliance:

7.6.1 The Business Owner will submit completed PTAs to the CBP Privacy Office through their assigned Privacy Analyst;

7.6.2 If the Business Owner has not been assigned a Privacy Analyst, they will submit completed PTAs to PRIVACY.CBP@CBP.DHS.GOV; and

7.6.3 All PTAs must identify the lead Business Owner, as well as the lead Project Manager, as applicable. PTAs without these points of contact will be rejected.

7.7 CBP's Privacy Office will review the PTA, resolve any questions or issues, and transmit the PTA to the DHS Privacy Office. No submission of new systems shall be made to OMB under the "OMB 300" review process before the PTA relating to such system has been cleared by CBP's Privacy and Diversity Office and adjudicated by the DHS Privacy Office.

7.8 The DHS Privacy Office will use the PTA to determine whether the program or system is privacy sensitive. Additionally, the PTA notes if a PIA and/or SORN is required.

7.9 Following the DHS Privacy Office's adjudication of the PTA and a determination of the need for further Privacy Compliance Documentation, CBP's Privacy Officer will direct the Privacy Liaison and Privacy Analyst to prepare the necessary compliance documents for review by the CBP Privacy Officer.

7.10 CBP's Privacy and Diversity Office will use the drafting of the Privacy Compliance Documentation to ensure that the proper privacy compliance measures are followed and incorporated into the development of, or change to, any automated system, project, or operation that collects, maintains, or uses PII, or where there is a change in statutory or regulatory requirements pertaining to PII.

7.11 Upon completion of the drafting of the Privacy Compliance Documentation, CBP's Privacy Officer should provide drafts to the Office of Chief Counsel for a legal sufficiency review.

7.12 Following the Office of Chief Counsel's legal sufficiency review, when appropriate, and formal clearance by the Business Owner's Office and other CBP stakeholders, the final compliance documents (e.g., PTA, PIA, and/or SORN) will be transmitted electronically by CBP's Privacy Office to the DHS Privacy Office for review and approval.

7.13 No CBP personnel may begin collecting or using PII through an automated system, project, operation, pilot, or regulatory change without first completing all of the proper Privacy Compliance Documentation:

7.13.1 No Authority to Operate (ATO) nor Authority to Test (ATT) may be granted to systems that lack properly adjudicated Privacy Compliance Documentation.

7.13.2 For programs in Ongoing Authorization (OA), all proper Privacy Compliance Documentation must be current and complete in order to maintain OA status.

7.13.2.1 For programs entering OA, all compliance documentation must have been completed within the past year.

7.14 Where PII is being collected, maintained, used, or disseminated through IT systems, technologies, rulemakings, programs, pilot projects, demonstrations, information sharing, contracts, and other activities, before the proper privacy compliance documents are completed, CBP's Privacy Officer, in conjunction with the DHS Privacy Office, will make a determination as to whether the IT systems, technologies, rulemakings, programs, pilot projects, demonstrations, information sharing, contracts, and other activities, should be shut down or other corrective actions should be taken in accordance with DHS Directive 047-01 and Instruction 047-01-001.

7.15 As appropriate, CBP's Privacy and Diversity Office will conduct a review of IT systems, technologies, rulemakings, programs, pilot projects, demonstrations, information sharing, contracts, and other activities, to ensure that it conforms to the Privacy Compliance Documentation.

8. INFORMATION SHARING PROCEDURES

8.1 Sharing of PII within DHS pursuant to the One-DHS Memorandum does not require a written agreement between CBP and the other component(s) of DHS. However, where information is shared with another component of DHS as part of a routine or automated process, the Business Owner shall ensure that the request and intended use of the information are compliant with applicable DHS privacy policies by submitting a PTA, detailing the component access, through the procedures in Section 7.

8.2 All domestic bulk sharing initiatives with entities outside DHS require an ISAA:[16]

8.2.1 All requests for ISAAs must comply with procedures established by this Directive in conformance with the DHS ISSGB Charter and overseen by the ISCC;

8.2.2 The party seeking an ISAA is required to prepare all relevant portions of the DARP Questionnaire or draft the ISAA with all the necessary information as identified in the DARP Questionnaire for submission to the ISAO;

8.2.3 The ISAO identifies a business owner for the ISAA who completes the CBP portions of the DARP Questionnaire or reviews the draft ISAA;

[16] Coordination with the DARC is only required when an ISAA associated with a bulk data transfer involves the collection or dissemination of large quantities of intelligence or information, a significant portion of which is not reasonably likely to have any ultimate intelligence or operational value to the recipient, but which is provided to the data recipient for the recipient to identify information of intelligence or operational value within it. See Footnote 2.

8.2.4 The ISAO supports CBP stakeholders in the drafting of the ISAAs based upon the equities identified in the DARP Questionnaire and reviews the draft ISAAs;

8.2.4.1 In filling out a DARP Questionnaire, both parties to the ISAA must identify all relevant stakeholders, the information subject to the exchange, the authorities permitting the exchange, intended uses of the information, and any policy implications of the information exchange.

8.2.5 The ISAO circulates the component-cleared ISAA through the ISCC, if required; or if the One-DHS Policy is not implicated, then the ISAO circulates the draft to the DHS Privacy Office and the Office for Civil Rights and Civil Liberties for oversight review; and

8.2.6 The ISAO is responsible for presenting ISCC or DHS-cleared ISAAs to CBP for acceptance and signature by an appropriate CBP authority.

8.3 All domestic discretionary distribution or ad hoc sharing of CBP records for Law Enforcement purposes must be in accordance with CBP Directive No. 4320-033 on the Sharing of Information for Law Enforcement and Security Purposes.

8.4 For any ad hoc sharing of uncertified CBP records containing PII with foreign authorities, that is not covered by an ISAA, a Delegation of Authority, or intended for use in a judicial proceeding, CBP personnel must coordinate with the CBP Privacy Office at PRIVACY.CBP@CBP.DHS.GOV, as well as the record owner prior to making a disclosure. All discretionary distribution or ad hoc sharing of CBP records with foreign authorities must also be in accordance with CBP Directive No. 4320-025A, Disclosure of Official Information to Foreign Authorities, including personnel seeking the assistance of the Office of Chief Counsel when required by that Directive:

8.4.1 CBP's Privacy Officer shall evaluate the requested disclosure and as appropriate, provide guidance and support to the CBP office and/or personnel supporting the request.

8.5 Requests to disclose CBP records or information containing PII through press releases, articles, social media posts, or in response to media inquiries, may only occur with the review and approval of the CBP Privacy Office (cbp-privacymediareleases@cbp.dhs.gov):

8.5.1 The CBP Privacy Office will assess whether the public interest in disclosure outweighs the privacy interests of the individual to the extent the information would shed light on CBP's performance of its duties and whether there are any applicable prohibitions on release of the information; and

8.5.2 The CBP Privacy Office will coordinate any requests to disclose PII belonging to U.S. persons to the media with the DHS Privacy Officer and the DHS General Counsel.

8.6 Any CBP Office or personnel responsible for sharing PII from a System of Records with a party outside of DHS must confirm that an automated (i.e., system generated) or "hard" copy (i.e., paper or electronic version) DHS-191, Privacy Act Disclosure Record (available from "FORMS" on CBPnet), or other form or process specifically authorized by the CBP Privacy Officer, is prepared to document the sharing of the information. The original DHS-191 or record of disclosure must be retained by the CBP Office providing the information for a period of five years, and a copy must be submitted to the CBP Privacy and Diversity Office at PRIVACY.CBP@CBP.DHS.GOV.

9. PRIVACY INCIDENT HANDLING AND RESPONSE

9.1 In accordance with the DHS Privacy Incident Handling Guidance (PIHG), CBP's Privacy Office will issue guidance to the workforce designed to assist all CBP personnel in responding to suspected or confirmed Privacy Incidents:

9.1.1 The PIHG assigns to all CBP personnel the responsibility to immediately report any suspected or confirmed Privacy Incident to their supervisor, the CBP Privacy and Diversity Office at PRIVACYINCIDENTS@CBP.DHS.GOV, or the CBP CBP-SOC at (703) 921-6507 for review, investigation, and remediation, as necessary; and

9.1.2 The Privacy Incident guidance will provide instruction and best practices on the management of PII and how to safeguard PII. Guidance could include Factsheets, electronic communications via email, FAQs and other guidance documents to provide workflow and reminders for CBP personnel to aid in meeting their respective responsibilities in responding to privacy incidents and safeguarding PII.

9.2 The CBP Privacy Office will coordinate the response to all Privacy Incidents, including ensuring the involvement of key personnel within the Office of Chief Counsel, the Office of Information and Technology, the Office of Professional Responsibility, and the Office of the Commissioner, as necessary:

9.2.1 For incidents involving contract personnel or contractor operated systems, the CBP Privacy Office will also coordinate with personnel from the Office of Acquisition, the Contracting Officer, and relevant program personnel as necessary; and

9.2.1.1 The CBP Privacy Office will coordinate the review of relevant contract documents, ISAAs, non-disclosure agreements, training records, rules of behavior documents, etc.

9.2.2 The CBP Privacy Office will coordinate with the DHS Privacy Office to determine whether an incident should be classified as Major, resulting in the initiation of the departmental Breach Response Team (BRT).

9.3 The CBP Privacy Office will develop a response and remediation plan that, in coordination with the office within which the incident occurred, will be implemented to mitigate the impact of the breach and ensure to the extent possible that similar incidents will not occur in the future:

9.3.1 All personnel will comply with remediation requirements identified and assigned by the CBP Privacy Office in response to a Privacy Incident, including the provision of training and any other remedial measures or obligations deemed necessary by the CBP Privacy Officer; and

9.3.2 The Office determined to be responsible for the incident will bear the costs associated with all response and remediation requirements, including the provision of notification to affected individuals, as well as identity protection and credit monitoring, if deemed necessary.

10. PRIVACY TRAINING REQUIREMENTS

10.1 All CBP personnel must complete privacy training in order to access or use PII as part of their official duties. Training includes:

10.1.1 Annual completion of "Privacy at DHS: Protecting Personal Information" in the DHS Performance and Learning Management System (PALMS TRAEN Course ID: G0597020-31) or successor training course;

10.1.2 System or program-specific training in order to access or use PII in that system or as part of that program. For example, users of TECS must complete the "TECS Privacy and Security Awareness" course annually in order to maintain access to TECS; and

10.1.3 Remedial or refresher training as required in response to a Privacy Incident.

11. TREATMENT OF VESSEL MANIFEST INFORMATION

11.1 In accordance with 19 CFR 103.31, which implements the requirements of 19 U.S.C. 1431(c), , CBP provides confidential treatment under certain circumstances for the name and address of importers, consignees, and shippers (foreign suppliers) on inward vessel manifests, and for the name and address of shippers (exporters) on

outward vessel manifests. Note that the confidential treatment of such information only applies to public disclosure of manifest information and does not impact internal use of this information or use for law enforcement purposes.

11.2 Requests under 19 C.F.R. § 103.31(d) for confidential treatment of manifest information for shipments of goods received by sea (vessel) are received from the public by mail, fax, email at vesselmanifestconfidentiality@cbp.dhs.gov, or other electronic means (such as submission through CBP's public website, www.CBP.gov) and shall be processed by the Office of Trade (OT), Trade Transformation Office, through the ACE/Automated Manifest System (Inward) and the ACE/Automated Export System (Outward).

11.3 Availability of vessel manifest information, as required in 19 CFR 103.31(e), is managed by the Office of Finance, Revenue Division (receipts of payment), and the Office of Information and Technology, Cargo Systems Program Directorate (dissemination of information).

11.4 Coordination of outreach and response to inquiries from representatives of the press is provided by the Office of Trade Relations, Office of the Commissioner:

11.4.1 The Trade Transformation Office, Office of Trade, will assess and determine whether to grant or deny requests from representatives of the press seeking accreditation and access to import and/or export vessel manifest information pursuant to 19 C.F.R. 103.31(a). With regard to vessel manifest information maintained at port locations, the Trade Transformation Office will coordinate with the Office of Field Operations;

11.4.2 The Regulations and Rulings Directorate, Office of Trade, will assess and determine whether to grant or deny administrative appeals of adverse determinations made by the Trade Transformation Office regarding a representative of the press' request for accreditation and access to vessel manifest information pursuant to 19 C.F.R. 103.31(a); and

11.4.3 The Trade Transformation Office, Office of Trade, will facilitate access to vessel manifest information for accredited representatives of the press.

11.5 Inquiries and complaints relating to the publication or non-publication of information, from shippers, importers, consignees, other members of the trade or the public, are coordinated by the Office of Trade Relations, Office of the Commissioner.

12. NO PRIVATE RIGHT CREATED

This Directive is an internal policy statement of CBP and does not create nor confer any rights, privileges, or benefits for any person or entity. United States v. Caceres, 440 U.S. 741 (1979).

Chris Magnus

Commissioner

U.S. Customs and Border Protection